UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE INGENIERÍA
CARRERA DE INGENIERÍA ELECTRÓNICA
INSTITUTO DE ELECTRÓNICA APLICADA
POSTGRADO CARRERA DE INGENIERÍA ELECTRÓNICA
"Magister Scientiarum en Ingeniería en Redes de Comunicación"

TESIS DE MAESTRÍA

"DESARROLLO DE UN MODELO DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA NB/ISO/IEC 27001 APLICADO AL ÁREA DE TI EN EMPRESAS CORREDORAS DE SEGUROS Y REASEGUROS"

Tesis de Grado presentada para optar al título de
"Maestría de Ingeniería en Ingeniería en Redes de Comunicación"

AUTOR: ING. CELIA CARMEN POMA MOYA
TUTOR: M. Sc. ING. CESAR LOZANO MANTILLA

LA PAZ – BOLIVIA

2020

UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE INGENIERIA

LA FACULTAD DE INGENIERIA DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS AUTORIZA EL USO DE LA INFORMACIÓN CONTENIDA EN ESTE DOCUMENTO SI LOS PROPÓSITOS SON ESTRICTAMENTE ACADÉMICOS.

LICENCIA DE USO

El usuario está autorizado a:

a) Visualizar el documento mediante el uso de un ordenador o dispositivo móvil.
b) Copiar, almacenar o imprimir si ha de ser de uso exclusivamente personal y privado.
c) Copiar textualmente parte(s) de su contenido mencionando la fuente y/o haciendo la cita o referencia correspondiente en apego a las normas de redacción e investigación.

El usuario no puede publicar, distribuir o realizar emisión o exhibición alguna de este material, sin la autorización correspondiente.

ÍNDICE GENERAL

CAPÍTULO 3

CAPÍTULO 4

CAPÍTULO 5

CAPÍTULO 7

DEDICATORIA

A Dios, por darme la vida y estar siempre conmigo, guiando mí camino.

A mi esposo José Alberto por su amor y apoyo incondicional, que me han permitido llegar a cumplir un sueño más.

A mis hijos Josue Victor y Luciana Daffne por su cariño y comprensión, por ser mi fuerza para seguir adelante.

A mis padres Victor y Florencia por su apoyo constante, por llenar mi vida con sus valiosos consejos.

AGRADECIMIENTO

Agradecer a Dios, por ser el guía, el apoyo y fortaleza en aquellos momentos de dificultad y de debilidad.

Agradecer al M. Sc. Ing. Wilber Flores por el apoyo, a mi tutor M. Sc. Ing. Cesar Lozano por la motivación y acertadas recomendaciones que me oriento a culminar la tesis, a los tribunales M. Sc. Ing. Roberto Zambrana y M. Sc. Ing. Javier Sanabria por haberme encaminado con sus consejos y correcciones, también agradecer a todos los Gerentes y personal de Tecnologías de la Información de las corredoras de Seguros y Reaseguros por su valioso aporte para desarrollar el presente estudio.

ABSTRACT

In this study, an Information Security Management System model was developed based on the NB/ISO/IEC 27001 Standard, for which, in the first instance, the environment and context in which Bolivia is located was analyzed, considering the situation of the countries with which the border is shared, which are: Argentina, Brazil, Chile, Paraguay and Peru, Colombia was also considered, for its experience in the area of Information Security. The following indicators were analyzed: Technology, Education and Cyber Security Mindset, results have been obtained which indicate that at a general level in all the countries mentioned there is a deficiency and lack of programs in the Education of society for the safe handling of information.

The number of ISO 27001 certifications that the aforementioned countries have has also been seen, of which it can be mentioned that Brazil has 170 certifications and Colombia 148 certifications corresponding to the year 2017 being the countries that have the most certifications, Bolivia would have seven certifications, and Paraguay with 2 certifications. In this regard, accreditation organizations and certifying institutions have been identified in the seven countries, including Bolivia.

In the Bolivian environment, two sectors were identified: the public and the private, the private sector being the one who has made the most progress on the issue of information security. There is no institution dedicated exclusively to the tasks of Information Security Management, just in 2015, in Bolivia entities such as AGETIC and CTIC - EPB were created, that among its functions is to generate guidelines on the subject of information security. While in the financial sector regulated by the ASFI, already in its circulars of the year 2003 the culture of computer security is mentioned, currently the latest ASFI 505/2017 circular is based on the ISO 27000 family of standards and the APS in its 2016 circulars already mentions the NB/ISO/IEC 27001 standard.

In Chapter 4, with the results of the questionnaire consisting of 61 questions, answered by the Information Technology and Management staff, through a personal interview,

Information Security controls used by Insurance and Reinsurance Brokers have been identified. In Chapter 5, the fourteen controls of the NB/ISO/IEC 27002 standard have been studied and analyzed aligned to the NB/ISO/IEC 27001 standard, the form of application was analyzed and as a contribution, guidelines for the development of policies, procedures, processes and records have been prepared, that can contribute to the application of the controls, in the area of Information Technology or Systems area.

In Chapter 6, the Risk Management Process in Information security was applied, developing the activities indicated in the NB/ISO/IEC 27005 standard, supported by Magerit v.03 a combination of both was used to generate the risk matrix, where it has been possible to identify the information assets, identify threats, identify existing controls, identify vulnerabilities and identify consequences. The result of the Risk Management process has justified the need to implement the controls, prioritizing those that can mitigate high risks. In this sense, a proposal was developed to carry out a treatment plan in order to seek to reduce the High-level risks.

Finally, there is the Analysis of Results, the conclusions and recommendations, which synthesize the results of the study.

RESUMEN

En el presente estudio se desarrolló un modelo de Sistema de Gestión de Seguridad de la Información basado en la Norma NB/ISO/IEC 27001, para lo cual en primera instancia se analizó el entorno y contexto en el cual está Bolivia, considerando la situación de los países con los cuales se comparte frontera, que son: Argentina, Brasil, Chile, Paraguay y Perú, también se consideró a Colombia, por su experiencia en el área de Seguridad de la Información. Se analizaron los siguientes indicadores: Tecnología, Educación y Mentalidad de seguridad cibernética, se han obtenido resultados los cuales indican que a nivel general en todos los países citados existe deficiencia y carencia de programas en la Educación de la sociedad para el manejo seguro de la información.

También se ha visto la cantidad de certificaciones ISO 27001 que tienen los países citados, del cual se puede mencionar que Brasil posee 170 certificaciones y Colombia 148 certificaciones correspondiente al año 2017, siendo los países que más certificaciones poseen, Bolivia contaría con 7 certificaciones, y Paraguay con 2 certificaciones. Al respecto, se han identificado las organizaciones de acreditación y las instituciones certificadoras en los siete países incluido Bolivia.

En el entorno de Bolivia se identificaron dos sectores el público y el privado, siendo el sector privado quien más avance ha tenido en el tema de seguridad de la información. No se cuenta con una institución dedicada exclusivamente a las tareas de Gestión de Seguridad de la Información, recién en el año 2015, en Bolivia se crean entidades como el AGETIC y el CTIC – EPB, que entre sus funciones está generar lineamientos en el tema de seguridad de la información. Mientras que en el sector financiero regulado por el ASFI, ya en sus circulares del año 2003 se menciona la cultura de seguridad informática, actualmente la última circular ASFI 505/2017 está fundamentada en la familia de normas ISO 27000 y la APS en sus circulares del año 2016 ya menciona a la norma NB/ISO/IEC 27001.

En el Capítulo 4, con los resultados del cuestionario que consta de 61 preguntas, respondido por el personal de Tecnologías de Información y Gerencia, mediante una entrevista personal, se han identificado los controles de Seguridad de la Información que utilizan las empresas Corredoras de Seguros y Reaseguros. En el Capítulo 5, se ha estudiado y analizado los catorce controles, de la norma NB/ISO/IEC 27002 alineados a la norma NB/ISO/IEC 27001, se analizó la forma de aplicación y como aporte se han elaborado guías de elaboración de políticas, procedimientos, procesos y registros, que puedan contribuir a la aplicación de los controles, en el área de Tecnologías de Información o área de Sistemas.

En el Capítulo 6, se aplicó el Proceso de Gestión del Riesgo en la seguridad de la Información, desarrollando las actividades señaladas en la norma NB/ISO/IEC 27005, apoyado en Magerit v.03. Una combinación de ambas fue utilizada para generar la matriz de riesgo, donde se ha podido identificar los activos de información, identificar las amenazas, identificar los controles existentes, identificar las vulnerabilidades e identificar las consecuencias. El resultado del proceso de Gestión del Riesgo ha permitido justificar la necesidad de implementar los controles, dando prioridad a aquellos que pueden mitigar riesgos altos. En este sentido, se elaboró una propuesta para realizar un plan de tratamiento con el fin de buscar reducir los riesgos de nivel Alto.

Finalmente se presenta el Análisis de Resultados, las conclusiones y recomendaciones, que sintetizan los resultados del estudio.

Palabras clave: NB/ISO/IEC 27001. Certificación. Seguridad.

INDICE DE TABLAS

INDICE DE FIGURAS

LISTA DE ACRÓNIMOS

ADSIB Agencia para el Desarrollo de la Sociedad de la Información para Bolivia

AENOR Asociación Española de Normalización y Certificación

AGETIC Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación

ALC América Latina y el Caribe

AMN Asociación Mercosur de Normalización

ASFI Autoridad de Supervisión del Sistema Financiero

APS Autoridad de Fiscalización y Control de Pensiones y Seguros

API Application Programming Interface

BID Banco Interamericano de Desarrollo

CGII Centro de Gestión de Incidentes Informáticos

CGCRE Coordinación General de Acreditación de Inmetro

CMM Modelo de Madurez de Capacidad de Seguridad Cibernética

CONMETRO Consejo Nacional de Metrología, Normalización y Calidad Industrial

CONACYT Consejo Nacional de Ciencia y Tecnología

COPANT Comisión Panamericana de Normas Técnicas

COPLUTIC Comité Plurinacional de Tecnologías de Información y Comunicación

COSTETIC Consejo Sectorial de Telecomunicaciones y Tecnologías de Información y Comunicación

CPD Centro de Procesamiento de Datos

DS Decreto Supremo

DES Estándar de Cifrado de Datos

CSIRT Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT, por sus siglas en Inglés)

EH Encuesta de Hogares

GCSCC Centro Global de Capacidad sobre Seguridad Cibernética

IAF Foro Internacional de Acreditación

IAAC Cooperación Inter Americana de Acreditación

IBMETRO Instituto Boliviano de Metrología

IBNORCA Instituto Boliviano de Normalización y Calidad

IKEv2 protocolo Internet Key Exchange versión 2

ILAC Cooperación Internacional de Acreditación de Laboratorios

IPSec Internet Protocol Security

INE Instituto Nacional de Estadísticas

INN Instituto Nacional de Normalización

INACAL Instituto Nacional de Calidad

INTN Instituto Nacional de Tecnología, Normalización y Metrología

ITU Unión Internacional de Telecomunicaciones

L2TP Layer 2 Tunneling Protocol

MPPE Cifrado punto a punto de Microsoft

MAE Máxima Autoridad Ejecutiva

NIST National Institute of Standards and Technology

OAA Organismo Argentino de Acreditación

OCDE Organización para la Cooperación y el Desarrollo Económico

OEA Organización de Estados Americanos

OMC Organización Mundial del Comercio

ONA Organismo Nacional de Acreditación

ONAC Organismo Nacional de Acreditación de Colombia

ONC Organismo Nacional de Certificación

OWASP Open Web Application Security Project

PIB Producto Interno Bruto

PPTP Point to Point Tunneling Protocol

RSA Rivest, Shamir y Adleman

SSTP Secure Socker Tunneling Protocol

SSL Secure Sockets Layer

VPN Virtual Private Network

CAPITULO 1

1. INTRODUCCIÓN

Existen muchos estándares orientados a la gestión de seguridad, entre los cuales se encuentra la norma ISO 27001, que ha sido adoptada por muchos países de Sudamérica.

La gestión de seguridad de la Información, es un tema al que se le debe prestar atención, ya que la dependencia de las TIC (Tecnologías de la Información y las Comunicaciones) para el desarrollo de las actividades, es tal que una empresa al no poder contar con estas en un momento determinado pudiera provocar un verdadero desastre, causando pérdidas económicas y quedando con una mala imagen. Por este motivo y debido a la existencia de riesgos, garantizar la seguridad de la información mediante una buena gestión, se ha convertido en un aspecto importante que debe ser tomado en cuenta por toda empresa, en este caso específico Corredores de Seguros y Reaseguros.

Con el desarrollo del modelo de un SGSI en la unidad de Tecnologías de Información de empresas Corredores de Seguros y Reaseguros, se generará una herramienta que ayudará a mejorar o controlar la seguridad de la información cumpliendo con normas de calidad, en términos de las características de localización, activos y tecnología, apoyado en los controles de seguridad que pueden ser aplicables según la norma NB/ISO/IEC 27001.

1.1 DESCRIPCIÓN DEL PROBLEMA

El crecimiento acelerado de la tecnología, para crear, procesar y almacenar información, ha generado beneficios, sin embargo también ha generado problemas de vulnerabilidad, riesgos e inseguridad así como fraudes informáticos, virus informático y ataques de intrusión o denegación de servicios.

Una de las principales causas por las que se acentúan los problemas es la implementación de tecnología, que no sigue las buenas prácticas de seguridad,

recomendadas por las normas, ya sea por falta de conocimiento o por factores económicos a los que está expuesta la unidad de Tecnologías de Información.

En el año 2010, la sección de seguros fue transferida a la Dirección de Supervisión de Seguros de la Autoridad de Supervisión del Sistema Financiero (ASFI). Es así que para realizar los trabajos de Auditoria Externa en el área de Tecnologías de Información, se consideró como referencia la Circular ASFI/193/2013 (16 de septiembre de 2013), que trata de la "Modificación del reglamento de requisitos mínimos de seguridad informática para la administración de sistemas de información y tecnologías relacionadas". Como primera modificación señala que la denominación de "Reglamento de Requisitos mínimos de seguridad informática para la administración de sistemas de Información y Tecnologías relacionadas" cambia por "Reglamento para la Gestión de Seguridad de la Información".

En la Resolución ASFI No 604/ 2013 (16 de septiembre de 2013) considera "Que, a fin de compatibilizar y actualizar criterios técnicos insertos en el Reglamento sobre Requisitos Mínimos de Seguridad Informática para la Administración de Sistemas de Información y Tecnologías Relacionadas" corresponde establecer los lineamientos con el contenido del estándar ISO/IEC 27002 .

Por tanto, al realizar las auditorías externas, en el ámbito de Tecnologías de la Información en las corredoras de Seguros y Reaseguros, se tomaron como referencia las circulares de la ASFI, como resultado se pudo evidenciar, que las corredoras, no cumplían con los controles mínimos de seguridad.

Teniendo como referencia, actualmente la circular ASFI 505/2017 emitido el 4 de diciembre de 2017, está circular sigue los lineamientos de la norma NB/ISO/IEC 27001.

En el año 2011, la sección de seguros se volvió a transferir a la Autoridad de Fiscalización y Control de Pensiones y Seguros -APS-. Y ya en el año 2017 con las

circulares APS/DS/JCF/ 153 -2017 y APS/DS/JCF 154-2017, del 6 de noviembre de 2017 que trata sobre el Alcance Mínimo para la realización de Auditorías Externas – Gestión 2017, en el numeral 5 ya se hace mención a la Evaluación en el ámbito de Tecnologías de Información y a la norma NB/ISO/IEC 27001, respectivamente.

En este contexto los entes reguladores y fiscalizadores, están adoptando normas relacionadas a la Seguridad de la Información y aplicándolos. Es así que ASFI recibió certificación ISO/IEC 27001:2013 de seguridad de la información (Ministerio de Economía y Finanzas Públicas, Noticias del Ministerio, 14 diciembre 2018), calificación que reconoce la confidencialidad en la información que maneja la entidad pública.

Extraemos el texto del ARTÍCULO 4º TECNOLOGÍA DE LA INFORMACIÓN de la resolución administrativa APS/DJ/DS/ Nº39 – 2016 (12 de enero de 2016), que dice: "La firma de Auditoria Externa a través de personal calificado, debe evaluar y emitir opinión de acuerdo a la norma NB-ISO-IEC 27001" sobre si los controles de los sistemas informáticos y de procesamiento de datos adoptados y / o desarrollados por la entidad cumplen mínimamente con los siguientes incisos de la citada norma:

- ✓ Política de Seguridad
- ✓ Aspectos Organizativos
- ✓ Física y Ambiental
- ✓ Comunicaciones y Operaciones
- ✓ Control Accesos
- ✓ Adquisición, desarrollo y mantenimiento de los sistemas de Información
- ✓ Gestión de Incidentes
- ✓ Gestión Continuidad del Negocio

Por este motivo es que las empresas Corredores de Seguros y Reaseguros, en un futuro próximo deberán prepararse para cumplir los controles establecidos en la norma NB/ISO/IEC 27001, sin embargo el principal problema es que aún desconocen la norma y más aún los beneficios que una empresa podría alcanzar siguiendo los parámetros de la norma.

El principal problema está centrado en el personal, a todo nivel, desde la alta dirección, personal de TI (Tecnologías de Información) y los usuarios finales, que no tienen conocimiento sobre la seguridad de la información y cuando se presentan incidentes de seguridad de la información los resuelven sin seguir procedimientos adecuados, por lo que siempre están presentes los problemas.

Se puede indicar que las empresas Corredoras de Seguros y Reaseguros, generalmente no consideran al representante del área de TI, en reuniones de alta dirección, donde se toman decisiones importantes en el aspecto de presupuestos para proyectos. Siendo que el área de TI, muchas veces nombrada como área de Sistemas, se encuentra en el último nivel del organigrama e incluso en algunas instancias ni siquiera forma parte del organigrama.

Es común que una sola persona del área de TI realice muchos trabajos técnicos, lo cual absorbe tiempo, motivo por el que se dificulta la generación de documentación pertinente al trabajo que realiza.

Puesto que en las empresas Corredores de Seguros y Reaseguros, no han considerado aún la conformación de un área de TI, no se cuentan con especialistas o con un plan de organización para los temas de seguridad de la información.

En la tesis, se desarrollará un modelo de un Sistema de Gestión de Seguridad de la Información, el cual abarca la problemática descrita. Invadidos por el desarrollo de la tecnología, actualmente es de vital importancia conocer las normas que se utilizan para obtener parámetros aceptables en el manejo seguro de la información.

El acceso y conocimiento sobre la norma NB/ISO/IEC 27001, es un limitante, con el modelo que se desarrollará, en el entorno de las empresas corredores de Seguros y

Reaseguros, se apoyará al área de TI, con un Sistema de Gestión de Seguridad de la Información que pueda ser implementado eficientemente, con énfasis en los controles de Seguridad de las Comunicaciones, que está relacionado con la Gestión de Seguridad de Red y la Transferencia de Información.

Para describir el problema esquemáticamente, se utiliza el diagrama de Ishikawa, que es un diagrama de Causa y Efecto que representa varios elementos (causas) de un sistema que pueden contribuir a un problema (efecto). Fue desarrollado en 1943 por el Profesor Kaoru Ishikawa en Tokio. (Federación Latinoamericana para la Calidad, s.f.).

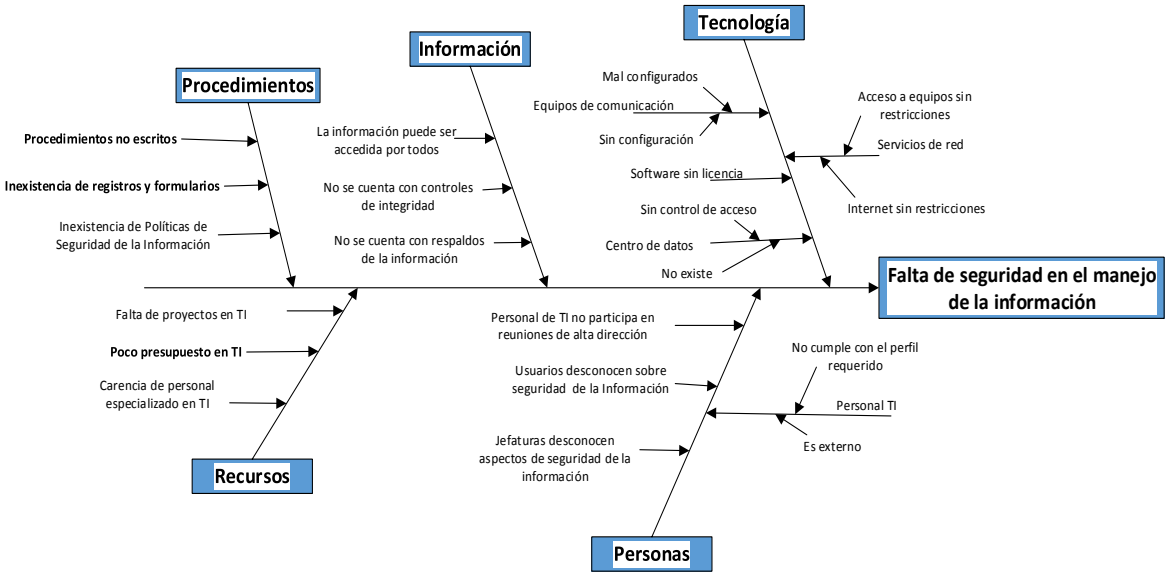


Figura 1.1.Diagrama de Ishikawa Causa efecto. Descripción del problema
Fuente: Elaboración propia

1.2 JUSTIFICACIÓN

Un Sistema de Gestión de Seguridad de la Información basado en la norma NB/ISO/IEC 27001, provee las condiciones necesarias para resguardar la integridad, confidencialidad y disponibilidad de los activos de información que posee una empresa corredora de Seguros y Reaseguros.

Una de las razones principales para implementar tecnologías de información, que tuvieron, las empresas corredoras de Seguros y Reaseguros de Bolivia, fue el de cumplir con los requerimientos de las circulares del Ente Regulador que es la APS. Sin

embargo en la implementación de la tecnología no se consideró el tema de seguridad de la información.

En el contexto de las empresas privadas, quienes primero afrontaron el tema de Seguridad de la Información fueron las Entidades Financieras, hoy en día mediante la APS, las corredoras de Seguros y Reaseguros, deben prepararse para abordar los requerimientos de Seguridad de la Información en base a la norma NB/ISO/IEC 27001:2013.

Por este motivo se requiere realizar un estudio de la mencionada norma, que pueda identificar los controles necesarios y aplicables, a las Corredoras de Seguros y Reaseguros, específicamente a las actividades relacionadas con Tecnologías de la Información.

El análisis de los resultados del estudio, también permitirá preparar a la Empresa Corredora para procesos de evaluación, auditoría o acreditación, tomando en cuenta que es un paso inicial para una certificación. En Bolivia, IBNORCA tiene la atribución de otorgar la certificación NB/ISO/IEC 27001, a las empresas que cumplan con los requerimientos indicados por la norma mencionada.

El desarrollo del modelo Sistema de Gestión de Seguridad de la Información (SGSI) también permite brindar los lineamientos que se deberían seguir para elegir una tecnología adecuada, de acuerdo a las características de la Corredora de Seguros y Reaseguros.

Entre la información generada por un SGSI, se puede mencionar registros y formularios que ayudan a establecer los criterios técnicos más relevantes para la selección de determinado equipo. Como ser los equipos de infraestructura de redes, que soporta los servicios de: Internet, red interna, correo electrónico, acceso a servidores locales, acceso a servidores remotos entre otros.

En el área de TI, el modelo de un SGSI, brinda apoyo en la gestión de: Redes de Comunicación, Parámetros de monitorización en la red, Respaldos de Información, Seguridad en el CPD (Centro de Procesamiento de Datos), administración de accesos

a diferentes servicios, generación de documentación, registros, formularios, procedimientos y procesos entre otros.

1.3 OBJETIVO GENERAL

Desarrollar un modelo de Sistema de Gestión de Seguridad de la Información, basado en la norma NB/ISO/IEC 27001:2013 aplicado al área de Tecnologías de Información de las Empresas Corredoras de Seguros y Reaseguros que operan en la ciudad de La Paz.

1.4 OBJETIVOS ESPECÍFICOS

- Analizar el entorno respecto a Gestión de Seguridad de la Información en nuestro País y Países vecinos.
- Identificar mediante la investigación los controles de seguridad de Información, que aplican las empresas Corredores de Seguros y Reaseguros.
- Elaborar guías de procedimientos, procesos, registros y políticas para la aplicabilidad de controles de la norma NB/ISO/IEC 27001:2013 en las empresas Corredores de Seguros y Reaseguros.
- Elaborar un modelo de la matriz de Gestión de Riesgo en la Seguridad de la Información.

1.5 ALCANCES

El presente proyecto, permitirá el desarrollo de un modelo de Sistema de Gestión de Seguridad de la Información basado en la norma NB/ISO/IEC 27001 aplicado al área de TI en Empresas Corredores de Seguros y Reaseguros, ubicadas geográficamente en la ciudad de La Paz.

Se recabará información respecto a los indicadores relacionados con la Seguridad de la Información así también las certificaciones en la norma ISO/IEC 27001, en Bolivia y en los países vecinos ubicados en Sudamérica, de esta manera comprender y reconocer el entorno en el cual se encuentra Bolivia en temas de Seguridad de la Información.

Se utilizará como herramienta de investigación, el cuestionario mediante entrevistas personales dirigidas al personal de Tecnologías de Información de las empresas corredoras de Seguros y Reaseguros, para conocer los controles de seguridad que aplica el área de TI actualmente, respecto a Gestión de Seguridad de la Información.

Se determinarán mediante análisis, los controles que pueden ser aplicables, en base al Anexo A de la Norma NB/ISO/IEC 27001:2013, que están directamente alineados con la norma ISO/IEC 27002.

Se realizará el proceso de Gestión del Riesgo en la seguridad de la Información, para elaborar el modelo de la matriz de Gestión de Riesgo en la Seguridad de la Información, basado en los lineamientos de la norma NB/ISO/IEC 27005, cuyo resultado sustentará la elección de controles.

1.6 LIMITACIONES

Se cuenta con un total de 39 empresas corredoras de Seguros y Reaseguros que operan en Bolivia, regulados por la APS, de los cuales 23 tienen sus oficinas principales en la Ciudad de La Paz, lo que representa al 59 % de corredoras de Seguros y Reaseguros.

Por lo expuesto, será una limitante el análisis del Universo de Corredoras de Seguros y Reaseguros, por lo que se realizó el estudio con 20 empresas a las que se pudo acceder con una entrevista personal, representando el 87% de un total de 23 empresas corredoras de seguros y reaseguros que operan en la Ciudad de La Paz.

Los aspectos que conforman la confidencialidad de la información de las Empresas Corredoras de Seguros y Reaseguros, no serán expuestos, sin embargo los resultados alcanzados serán presentados en porcentajes que determinaran criterios de interpretación de los controles de seguridad de la información, para desarrollar el modelo SGSI.

Los resultados presentados, y las consideraciones que se tomen, no significan que las empresas cumplan con todos los controles de seguridad de la información que está mencionado en la norma NB/ISO/IEC 27001.

En las normas de sistemas de gestión ISO basado en el proceso Planificar, Hacer, Verificar y Actuar, el presente estudio alcanza a la parte de Planificar, y se dan las guías de políticas, procedimientos, procesos y registros para poder Hacer.

CAPITULO 2

2. MARCO TEÓRICO

2.1 ISO E IEC

ISO (Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional) forman el sistema especializado para la normalización mundial. Los organismos nacionales miembros de ISO e IEC participan en el desarrollo de las Normas Internacionales por medio de comités técnicos establecidos por la organización respectiva, para atender campos particulares de la actividad técnica. Los comités técnicos de ISO e IEC colaboran en campos de interés mutuo. Otras organizaciones internacionales, públicas y privadas, en coordinación con ISO e IEC, también participan en el trabajo. (ISO, 2015)

Las normas internacionales para los sistemas de gestión proporcionan un modelo a seguir en la creación y operación de un sistemas de gestión. Este modelo incorpora los elementos sobre los que expertos en la materia han llegado a un consenso internacional como estado del arte. ISO/IEC JTC 1 SC 27 mantiene un comité de expertos dedicado a la elaboración de normas internacionales de sistemas de gestión para la seguridad de la Información, también conocida como la familia de normas de Sistemas de Gestión de Seguridad de la Información (SGSI).

2.2 NORMA BOLIVIANA NB/ISO/IEC 27000

La elaboración de la Norma Boliviana NB/ISO/IEC 27000:2010 “TECNOLOGÍA DE LA INFORMACIÓN – TÉCNICAS DE SEGURIDAD – SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN – VISIÓN GENERAL Y VOCABULARIO correspondiente a la norma ISO/IEC 27000: 2009 es idéntica a la norma ISO/IEC 27000:2009 “Information technology – Security techniques – Information Security management systems – Overview and vocabulary”

Está norma ofrece una visión general de los sistemas de gestión de seguridad de la información, que son objeto de la familia de normas de SGSI y define los términos relacionados.

2.2.1 FAMILIA DE NORMAS DE SGSI

Mediante el uso de la familia de normas de SGSI, las organizaciones pueden desarrollar y aplicar un marco para la gestión de la seguridad de sus activos de información y prepararse para una evaluación independiente de sus SGSI aplicada a la protección de la información.

La familia de normas de SGSI 1 tiene como objetivo ayudar a las organizaciones de todos los tipos y tamaños a implementar y operar un SGSI. La familia de normas de SGSI consta de las siguientes normas internacionales, bajo el título general Tecnología de la Información – Técnicas de Seguridad que indican que estas normas fueron preparadas por el comité técnico conjunto ISO/IEC JTC 1, Tecnologías de la Información, Subcomité SC 27, Técnicas de seguridad de TI.

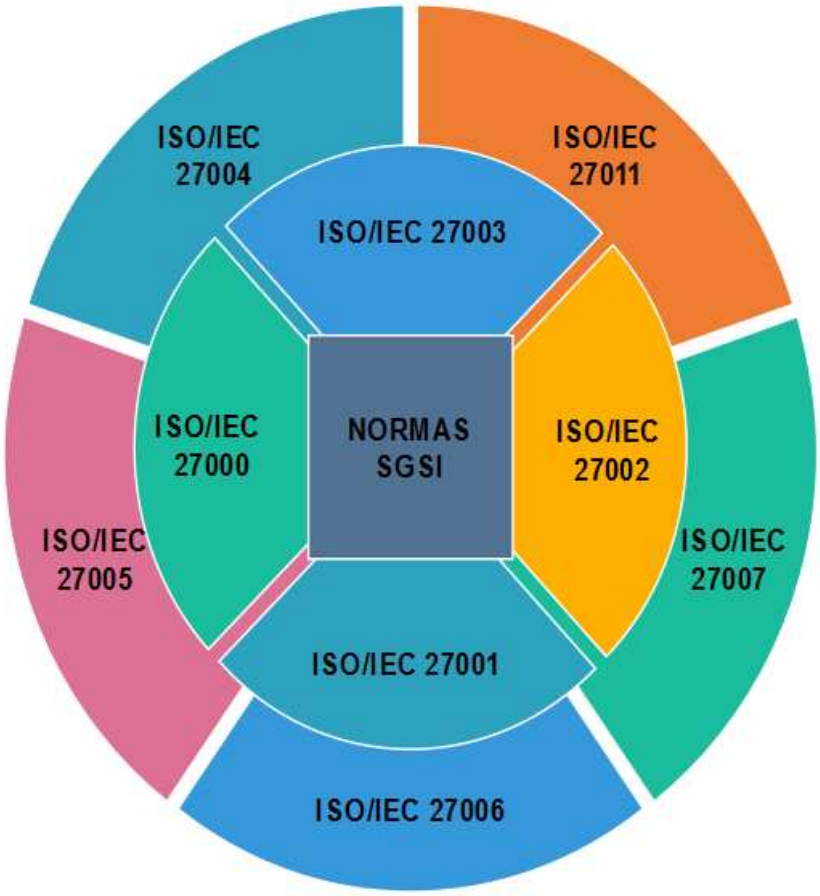


Figura 2.1 Familia de normas SGSI
Fuente: Elaboración propia en base a NB/ISO/IEC 27000:2010

Donde:

ISO/IEC 27000 Sistemas de Gestión de la seguridad de la información – Visión General y Vocabulario

ISO/IEC 27001:2005 Sistemas de Gestión de la seguridad de la información - Requisitos

ISO/IEC 27002:2005 Código de buenas prácticas para la gestión de la seguridad de la información

ISO/IEC 27003 Guía de implementación de sistemas de gestión de la seguridad de la información

ISO/IEC 27004 Gestión de la seguridad de la información - Métricas

ISO/IEC 27005: 2008 Gestión del riesgo de seguridad de la Información

ISO/IEC 27006:2007 Requisitos para los organismos que realizan la auditoria y certificación de sistemas de gestión de la seguridad de la información

ISO/IEC 27007 Directrices para la auditoria de los sistemas de gestión de la seguridad de la información

ISO/IEC 27011 Directrices para la gestión de la seguridad de la información en organizaciones de telecomunicaciones basadas en ISO/IEC 27002

2.2.2 SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Un Sistema de Gestión de la Seguridad de la Información (SGSI) proporciona un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de la protección de los activos de información para alcanzar los objetivos del negocio sobre la base de una evaluación del riesgo y los niveles de aceptación del riesgo de la organización para tratar y gestionar los riesgos de manera eficaz. El análisis de los requisitos para la protección de los activos de información y la aplicación de controles adecuados para garantizar la protección de estos activos de información según corresponda, contribuyen a la implementación exitosa de un SGSI. Los siguientes principios fundamentales también contribuyen a la implementación exitosa de un SGSI:

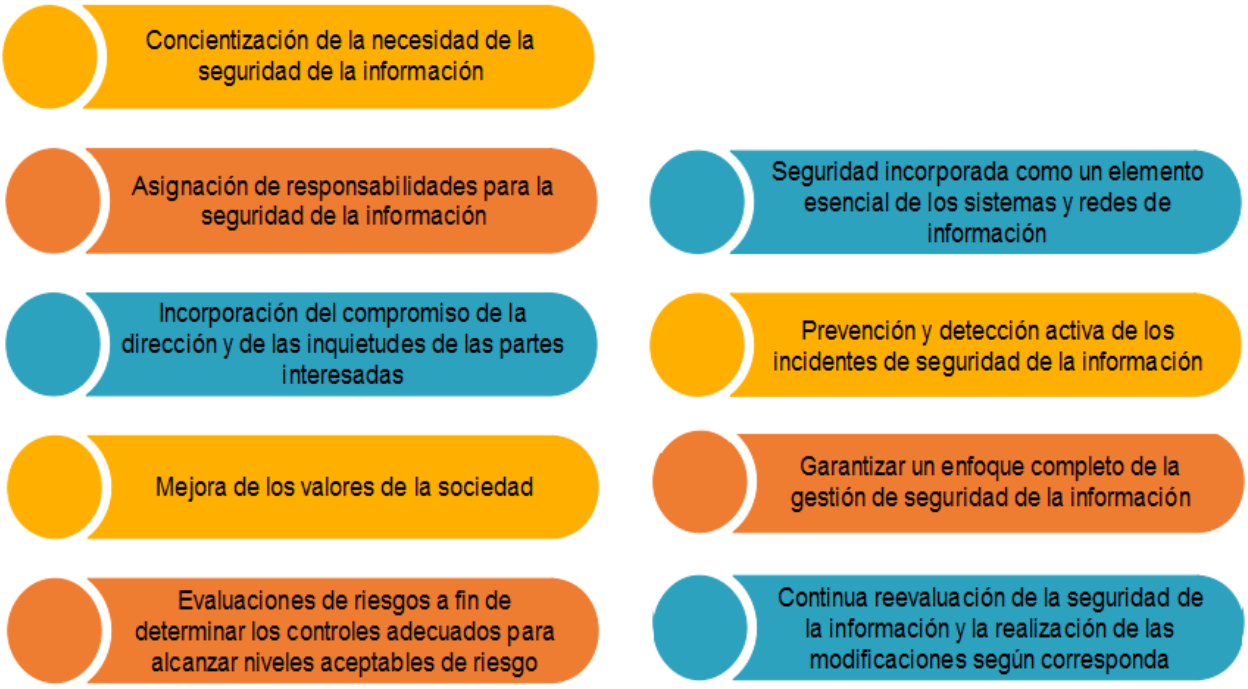


Figura 2.2 Principios fundamentales para la implementación de un SGSI

Fuente: Elaboración propia basado en NB/ISO/IEC 27000:2010

2.2.3 INFORMACIÓN

La información es un activo que, al igual que otros importantes activos del negocio, es esencial para el negocio de la organización y en consecuencia, necesita ser debidamente protegida. La información puede ser almacenada en muchas formas, incluyendo: formato digital (por ejemplo, archivos de datos almacenados en medios ópticos o electrónicos), medio material (por ejemplo, en papel), así como información no representada, en forma de conocimiento de los empleados. La información puede ser transmitida por diversos medios, entre ellos: mensajería, comunicación verbal o electrónica. Cualquiera sea la forma que la información adopte a los medios por los cuales la información se transmita, siempre necesita una protección adecuada.

La información de una organización depende de las tecnologías de la información y las comunicaciones. Estas tecnologías son un elemento esencial en cualquier organización y facilitan la creación, transformación, almacenamiento, transmisión, protección y destrucción de información. Cuando el alcance de los ambientes de negocio interconectados globalmente se expande, lo hace la obligación de proteger la

información ya que está información está ahora expuesta a una variedad más amplia de amenazas y vulnerabilidades.

2.2.4 SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información comprende tres dimensiones principales:

Figura 2.3 Dimensiones de la seguridad de la Información
Fuente: Elaboración propia basado en NB/ISO/IEC 27000:2010

Con el fin de garantizar el éxito sostenido del negocio y la continuidad, así como la minimización de los impactos, la seguridad de la información consiste en la aplicación y gestión de las medidas de seguridad adecuadas que implica la consideración de una amplia gama de amenazas.

La seguridad de la Información se logra mediante la implementación de un conjunto aplicable de controles, seleccionados a través del proceso de gestión del riesgo elegido y gestionado utilizando un SGSI, incluyendo políticas, procesos, procedimientos, estructuras organizacionales, software y hardware para proteger los activos de información identificados. Estos controles necesitan ser especificados, implementados, monitorizados, revisados y mejorados cuando sea necesario, para asegurar el logro de los objetivos de seguridad y del negocio. Se espera que los controles de seguridad relevantes sean integrados sin inconvenientes en los procesos de negocio de la organización.

2.2.5 GESTIÓN

La gestión incluye actividades para dirigir, controlar y mejorar continuamente la organización dentro de las estructuras adecuadas. Las actividades de gestión incluyen el acto, la forma o práctica de organizar, manejar, dirigir, supervisar y controlar los recursos. Las estructuras de gestión van desde una persona en una pequeña organización a jerarquías de gestión consistentes de muchas personas en grandes organizaciones.

En términos de un Sistema de Gestión de Seguridad de la Información (SGSI), la gestión implica la supervisión y toma de decisiones necesarias para alcanzar los objetivos empresariales a través de la protección de los activos de información de la organización. La gestión de la seguridad de la información se expresa a través de la formulación y el uso de políticas de seguridad de la información, normas, procedimientos y directrices, que luego se aplican a lo largo de toda la organización por todos los individuos asociados con la organización.

2.2.6 SISTEMA DE GESTIÓN

Un Sistema de Gestión utiliza un esquema de recursos para lograr los objetivos de una organización. El sistema de gestión incluye la estructura organizacional, políticas, actividades de planificación, responsabilidades, prácticas, procedimientos, procesos y recursos.

En términos de seguridad de la información, un sistema de gestión permite a una organización:

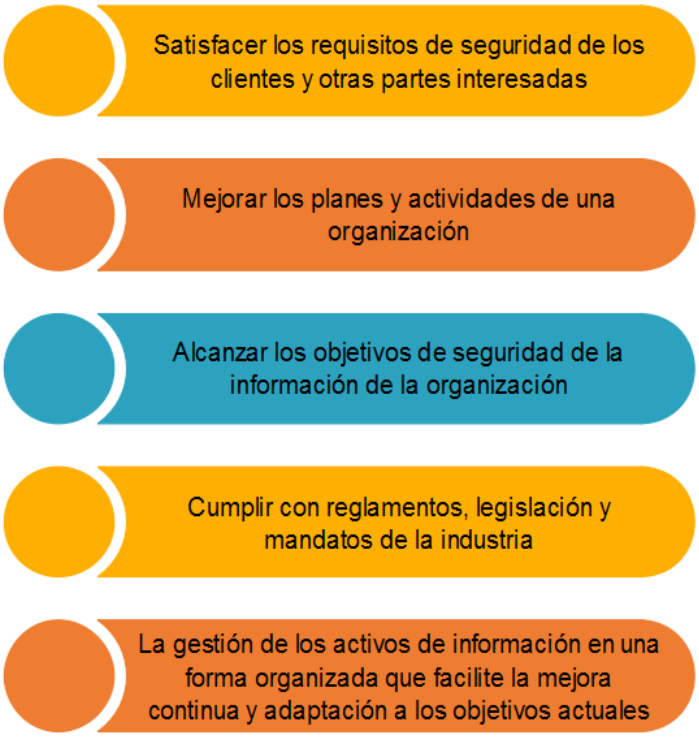


Figura 2.4 Beneficios de un sistema de Gestión

Fuente: Elaboración propia basado en NB/ISO/IEC 27000:2010

2.2.7 ENFOQUE DE PROCESO

Las organizaciones necesitan identificar y gestionar numerosas actividades para poder funcionar de manera eficaz y eficiente. Es necesario gestionar toda la actividad que utilice recursos para permitir la transformación de insumos en productos mediante un conjunto de actividades interrelacionadas o que interactúan – esto es también conocido como un proceso. La salida de un proceso puede directament formar parte de la entrada de otro proceso y, generalmente, está transformación se lleva a cabo bajo condiciones planificadas y controladas. La aplicación de un sistema de procesos dentro de una organización, junto con la identificación e interacciones de estos procesos y su gestión, se puede denominar como un “enfoque de proceso”.

El enfoque de procesos para el Sistema de Gestión de la Seguridad de la Información (SGSI) presentado por la familia de normas de SGSI está basado en el principio de funcionamiento aprobado en las normas de sistemas de gestión ISO comúnmente

conocido como el proceso Planificar – Hacer – Verificar – Actuar (PHVA, del inglés PDCA).

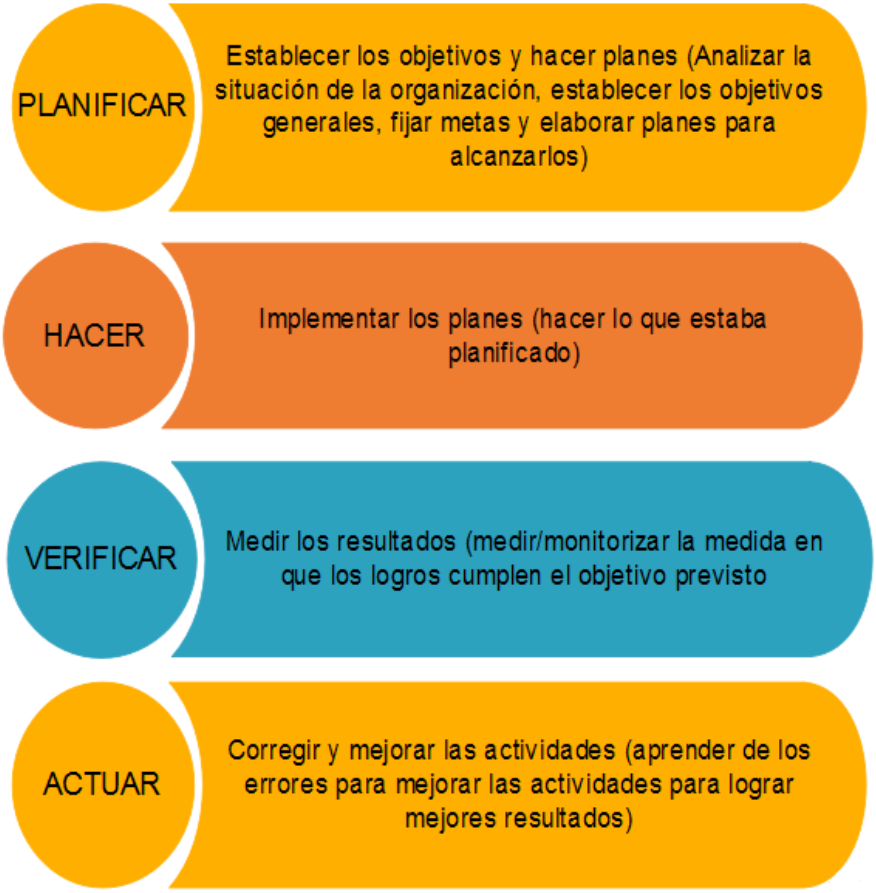


Figura 2.5 Ciclo Planificar – Hacer – Verificar - Actuar

Fuente: Elaboración propia basado en NB/ISO/IEC 27000:2010

2.3 ISO/IEC 27001

Publicada el 15 de Octubre de 2005, revisada el 25 de Septiembre de 2013. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSIs de las organizaciones. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la

implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.

2.4 NORMA BOLIVIANA NB/ISO/IEC 27001:2013 TECNOLOGÍAS DE LA INFORMACIÓN – TÉCNICAS DE SEGURIDAD – SISTEMAS DE GESTIÓN DE SEGURIDAD – REQUISITOS

Está norma es idéntica a la norma ISO/IEC 27001:2013 “Information technology – Security Techniques – Information Security management Systems - Requirements”

Esta norma ha sido preparada para proporcionar los requisitos para establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información.

El establecimiento e implementación de un sistema de gestión de seguridad de la información de la organización está influenciada por las necesidades y objetivos de la organización, los requisitos de seguridad, los procesos organizacionales utilizados, el tamaño y la estructura de la organización.

El sistema de gestión de seguridad de la información conserva la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgo y entrega confianza a las partes interesadas cuyos riesgos son gestionados de manera adecuada.

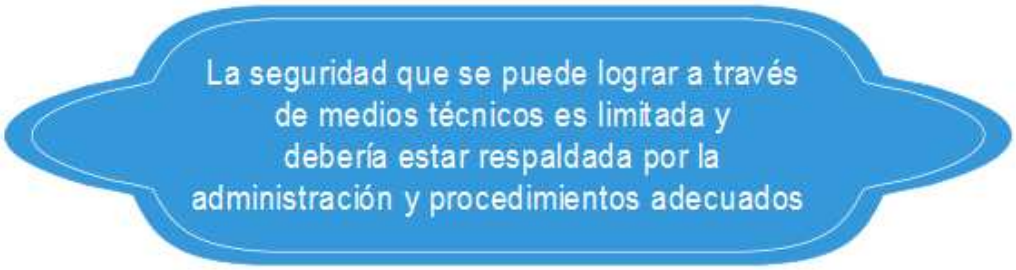
Es importante que el sistema de gestión de seguridad de la información sea parte de y este integrado a los procesos de la organización y a la estructura de gestión general y que la seguridad de la información sea considerada en el diseño de procesos, sistemas de información y controles. Se espera que la implementación del sistema de gestión de la seguridad de la información sea escalada de acuerdo a las necesidades de la organización. (NB/ISO/IEC 27001, 2013)

El Anexo A trata de los Objetivos de control de referencia y controles que están alineados con los enumerados en ISO/IEC 27002.

2.5 NB/ISO/IEC 27002:2014 TECNOLOGÍAS DE LA INFORMACIÓN – TÉCNICAS DE SEGURIDAD – CÓDIGO DE PRÁCTICAS PARA LOS CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

Está norma está diseñada para que las organizaciones la utilicen como referencia al seleccionar los controles dentro del proceso para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en base a ISO/IEC 27001 o como un documento de orientación para las organizaciones que implementen controles de seguridad de información de aceptación común.

Los activos están sujetos tanto a amenazas deliberadas como accidentales, mientras que los procesos, sistemas, redes y personas relacionadas poseen vulnerabilidades inherentes. Los cambios en los procesos y sistemas comerciales u otros cambios externos (como las nuevas leyes y normativas) pueden generar nuevos riesgos para la seguridad de la información. Por lo tanto, dada la multitud de formas en que las amenazas se pueden aprovechar de las vulnerabilidades para dañar a la organización, los riesgos en la seguridad de la información siempre están presentes. La seguridad eficaz en la información reduce estos riesgos al proteger a la organización contra las amenazas y vulnerabilidades y luego reduce el impacto en sus activos.



La identificación de los controles que se deberían poner en vigencia requiere de una planificación minuciosa y detallada. Los controles se pueden seleccionar a partir de esta norma o de otros conjuntos de controles, o bien se pueden diseñar nuevos controles para cumplir con las necesidades específicas según sea necesario.

Esta norma contiene 14 cláusulas de control de seguridad que en conjunto contienen un total de 35 categorías de seguridad principales y 114 controles.

Las 14 cláusulas de control son:

- Primer Control. Políticas de Seguridad de la Información
- Segundo Control. Organización de la seguridad de la Información
- Tercer Control. Seguridad de recursos humanos
- Cuarto Control. Administración de Activos
- Quinto Control. Control de acceso
- Sexto Control. Criptografía
- Séptimo Control. Seguridad física y del Ambiente
- Octavo Control. Seguridad de las operaciones
- Noveno Control. Seguridad de las comunicaciones
- Décimo Control. Adquisición, desarrollo y mantenimiento del sistemas
- Décimo Primer Control. Relaciones con los proveedores
- Décimo Segundo Control. Administración de incidentes de seguridad de la información
- Décimo Tercer. Aspectos de seguridad de la información de la administración de la continuidad comercial
- Décimo Cuarto. Cumplimiento

El orden de los controles en esta norma no implica su importancia.

2.6 ANÁLISIS DE RIESGO

El análisis de riesgos es una herramienta (imprescindible) de gestión. Por hacer o dejar de hacer un análisis de riesgos no se está ni más ni menos seguro: simplemente, se sabe dónde se está. A partir de este conocimiento podemos tomar decisiones de tratamiento y ejecutarlas.

El análisis de riesgos es una aproximación metódica que nos permite determinar el riesgo siguiendo unos pasos:

1. Determinar los activos relevantes para la organización,

2. Valorar dichos activos en función del coste que supondría para la organización recuperarse de un fallo de disponibilidad, integridad, confidencialidad o autenticidad

3. Determinar a qué amenazas están expuestos aquellos activos.

4. Valorar la vulnerabilidad de los activos a las amenazas potenciales.

5. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.

6. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectación de materialización) de la amenaza.

Es típico ver cómo los servicios dependen de los datos y de los aplicativos, propios o adquiridos. Todos a su vez dependen del equipamiento, hardware y comunicaciones que, a su vez, dependen de los locales que los acogen y de las personas que los operan. (Mañas, 2004, p.4)

Actualmente, existen varias metodologías para realizar el análisis de riesgos, las cuáles están fundamentadas en tres variables esenciales (Activos, las amenazas y las vulnerabilidades) que se identifican y se relacionan entre sí para determinar los riesgos, entre las metodologías más utilizadas se tienen Magerit, Octave y Mehari, todas cumplen con el mismo objetivo, su diferencia se determina en la forma de presentación de los resultados.

2.7 ISO 27005

Proporciona directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información)

Esta norma establece los principios para el uso eficaz, eficiente y aceptable de las tecnologías de la información. Garantizando que sus organizaciones siguen estos principios ayudará a los directores a equilibrar riesgos y oportunidades derivados del uso de las TI.

2.8 ISO/IEC 17021-1:2015. EVALUACIÓN DE LA CONFORMIDAD — REQUISITOS PARA LOS ORGANISMOS QUE REALIZAN LA AUDITORÍA Y LA CERTIFICACIÓN DE SISTEMAS DE GESTIÓN — PARTE 1: REQUISITOS.

En el campo de la evaluación de la conformidad, el Comité de ISO para la evaluación de la conformidad (CASCO Committee on Conformity Assessment) es responsable del desarrollo de Normas y Guías Internacionales.

En la parte 1 de las Directivas ISO/IEC se describen los procedimientos utilizados para desarrollar esta norma y para su mantenimiento posterior. En particular debería tomarse nota de los diferentes criterios de aprobación necesarios para los distintos tipos de documentos ISO.

Cualquier nombre comercial utilizado en esta norma es información a la atención de los usuarios y no constituyen una recomendación.

La Norma ISO/IEC 17021-1 ha sido preparada por el Comité de ISO para la evaluación de la conformidad (CASCO). El proyecto fue sometido a votación de los organismos nacionales de ISO y de IEC y fue aprobado por las dos organizaciones.

Esta primera edición de la Norma ISO/IEC 17021-1 anula y sustituye a la Norma ISO/IEC 17021:2011, que ha sido revisada técnicamente.

La Norma ISO/IEC 17021 consiste en las siguientes partes, bajo el título general Evaluación de la conformidad. Requisitos para los organismos que realizan la auditoría y la certificación de sistemas de gestión:

— Parte 1: Requisitos

— Parte 2: Requisitos de competencia para la auditoría y la certificación de sistemas de gestión ambiental [Especificación Técnica]

— Parte 3: Requisitos de competencia para la auditoría y la certificación de sistemas de gestión de la calidad [Especificación Técnica]

— Parte 4: Requisitos de competencia para la auditoría y la certificación de sistemas de gestión de la sostenibilidad de eventos [Especificación Técnica]

— Parte 5: Requisitos de competencia para la auditoría y la certificación de sistemas de gestión de activos [Especificación Técnica]

— Parte 6: Requisitos de competencia para la auditoría y la certificación de sistemas de gestión de la continuidad del negocio [Especificación Técnica]

— Parte 7: Requisitos de competencia para la auditoría y certificación de sistemas de gestión de la seguridad vial [Especificación Técnica]

Prólogo de la versión en español

Esta Norma Internacional ha sido traducida por el Grupo de Trabajo Spanish Translation Task Force (STTF) del Comité Técnico ISO/CASCO, Comité para la evaluación de la conformidad, en el que participan representantes de los organismos nacionales de normalización y representantes del sector empresarial de los siguientes países:

Argentina, Bolivia, Chile, Colombia, Costa Rica, Cuba, Ecuador, España, Estados Unidos de América, Honduras, México, Panamá, Perú, República Dominicana y Uruguay.

Igualmente, en el citado Grupo de Trabajo participan representantes de COPANT (Comisión Panamericana de Normas Técnicas) e INLAC (Instituto Latinoamericano de la Calidad).

Esta traducción es parte del resultado del trabajo que el Grupo ISO/CASCO viene desarrollando desde su creación en el año 2002 para lograr la unificación de la terminología en lengua española en el ámbito de la evaluación de la conformidad.

Introducción de la norma ISO/IEC 17021

La certificación de un sistema de gestión, tal como un sistema de gestión ambiental, de la calidad, o de seguridad de la información de una organización, es una de las formas de asegurar que la organización ha implementado un sistema para la gestión de los aspectos pertinentes de sus actividades, productos y servicios, en línea con la política de la organización y con los requisitos de la Norma Internacional de sistema de gestión respectiva.

Esta parte de la Norma ISO/IEC 17021 especifica requisitos para los organismos que realizan auditoría y certificación de sistemas de gestión. Presenta requisitos genéricos para tales organismos que llevan a cabo auditorías y certificaciones en el campo de sistemas de gestión de la calidad, ambiental y otros tipos de sistemas de gestión. Dichos organismos se conocen como organismos de certificación. El cumplimiento de estos requisitos tiene por finalidad asegurar que los organismos de certificación realicen la certificación de los sistemas de gestión de manera competente, coherente e imparcial, facilitando así el reconocimiento de dichos organismos y la aceptación de sus certificaciones en el ámbito nacional e internacional. Esta parte de la Norma ISO/IEC 17021 sirve como base para facilitar el reconocimiento de la certificación de los sistemas de gestión para los intereses del comercio internacional.

La certificación de un sistema de gestión proporciona una demostración independiente de que el sistema de gestión de la organización:

a) es conforme con los requisitos especificados;

b) es capaz de lograr coherentemente su política y objetivos declarados; y

c) está implementado de manera eficaz.

Por lo tanto, la evaluación de la conformidad, como es el caso de la certificación de un sistema de gestión, aporta valor a la organización, a sus clientes y a sus partes interesadas.

Las actividades de certificación son las actividades individuales que conforman el proceso entero de certificación desde la revisión de la solicitud hasta la terminación de la certificación.

Las actividades de certificación involucran la auditoría del sistema de gestión de una organización. La forma de atestación de la conformidad de un sistema de gestión de una organización con una norma específica de sistemas de gestión u otros requisitos normativos generalmente es un documento de certificación o un certificado.

Esta parte de la Norma ISO/IEC 17021 es aplicable a la auditoría y certificación de todo tipo de sistema de gestión. Se reconoce que algunos requisitos, en especial aquellos relacionados con la competencia de los auditores, se pueden complementar con criterios adicionales a fin de satisfacer las expectativas de las partes interesadas.

En esta parte de la Norma ISO/IEC 17021 se emplean las siguientes formas verbales:

— “debe” indica un requisito;

— “debería” indica una recomendación;

— “puede” indica un permiso, una posibilidad o capacidad;

En las Directivas de ISO/IEC, Parte 2, se pueden encontrar detalles adicionales.

Objeto y campo de aplicación

Esta parte de la Norma ISO/IEC 17021 contiene principios y requisitos relativos a la competencia, coherencia e imparcialidad de los organismos que realizan auditoría y certificación de todo tipo de sistemas de gestión.

No es necesario que los organismos de certificación que operan de acuerdo con esta parte de la Norma ISO/IEC 17021 ofrezcan todos los tipos de certificación de sistemas de gestión.

La certificación de sistemas de gestión es una actividad de evaluación de la conformidad de tercera parte y los organismos que realizan esta actividad son, por lo tanto, organismos de evaluación de la conformidad de tercera parte.

NOTA 1 Ejemplos de sistemas de gestión incluyen sistemas de gestión ambiental, sistemas de gestión de la calidad y sistemas de gestión de seguridad de la información.

NOTA 2 En esta parte de la Norma ISO/IEC 17021, la certificación de sistemas de gestión se denomina “certificación” y los organismos que realizan la evaluación de la conformidad de tercera parte se denominan “organismos de certificación”.

NOTA 3 Un organismo de certificación puede ser gubernamental o no gubernamental, con o sin autoridad de reglamentación.

NOTA 4 Esta parte de la Norma ISO/IEC 17021 puede utilizarse como documento de criterios para la acreditación, la evaluación entre pares u otros procesos de auditoría.

Referencias normativas

Los siguientes documentos referenciados, en parte o completos, son indispensables para la aplicación de esta norma. Para las referencias con fecha sólo se aplica la edición citada. Para las referencias sin fecha, se aplica la última edición del documento indicado (incluyendo cualquier modificación).

ISO 9000, Sistemas de gestión de la calidad — Fundamentos y vocabulario

ISO/IEC 17000, Evaluación de la conformidad — Vocabulario y principios generales

2.9 ISO SURVEY 2018

La Organización Internacional de Estandarización (ISO), lleva a cabo una encuesta anual que tiene como propósito averiguar el progreso de los sistemas de gestión ISO a nivel mundial. La encuesta que realiza y publica se la conoce como ISO Survey y

presenta los datos del número de certificados que hay de los diversos sistemas de gestión del mundo. En la siguiente tabla se puede observar el detalle de certificados válidos hasta el año 2018.

	Total valid certificates
ISO 9001:2015	878 664
ISO 14001:2015	307 059
ISO IEC 27001:2013	31 910
ISO 22000:2005&2018	32 120
ISO 45001:2018	11 952
ISO 13485:2003&2016	19 472
ISO 50001:2011	18 059
ISO 20000-1:2011	5 308
ISO 22301:2012	1 506
ISO 28000:2007	617
ISO 39001:2012	547
ISO 37001:2016	389

Tabla 2.1 Certificaciones ISO a nivel mundial

Fuente: ISO survey 2018

Se puede apreciar que la certificación ISO 9001: 2015 (Sistema de Gestión de Calidad con la última actualización del año 2015) es la más difundida a nivel mundial seguida de la ISO/14001:2015 (Sistema de Gestión ambiental con la última actualización del año 2015) y en tercer lugar ISO/IEC 27001: 2013 (Gestión de la seguridad de la Información con la última actualización del año 2013).

El número de certificaciones fluctúa de un año al otro, ya que se tiene un período de validez y para continuar con la certificación debe ser renovado, está información es un parámetro válido, en el cual se puede observar la cantidad de certificaciones a nivel mundial.

Suele existir confusión entre el uso de términos respecto a organismos de certificación y acreditación, es importante señalar las definiciones correspondientes, que a continuación se mencionan.

2.10 CERTIFICACIÓN DE SISTEMAS DE GESTIÓN

CTMA Consultores (2018) indica:

Las entidades certificadoras son las encargadas de realizar las gestiones y auditorías necesarias para determinar si se puede otorgar el certificado ISO correspondiente. Estas compañías que expiden los certificados ISO, deben estar debidamente acreditadas para el ejercicio de su labor. Son entidades totalmente imparciales e independientes.

INACAL (2016) indica:

Con la acreditación de Sistemas de Gestión una organización demuestra que cumple el estándar internacional, y es capaz de evaluar y certificar los sistemas de gestión en el alcance acreditado. Los organismos de certificación de sistemas de Gestión verifican que una Entidad cumpla con todos los requerimientos de una norma técnica.

La certificación de sistemas de gestión es una actividad de evaluación de la conformidad de tercera parte (por ejemplo: Sistemas de gestión ambiental, de la calidad, de seguridad de la información, etc).

2.11 ACREDITACIÓN DE ORGANISMOS DE CERTIFICACIÓN

Acreditación significa aplicar normas reconocidas internacionalmente, en este caso normas ISO, la cual certifica que se opera según los más altos niveles de calidad, aportando una garantía mayor acerca de los certificados emitidos, que poseen crédito e imparcialidad, de esta manera se otorga confianza a las instituciones que buscan certificarse, por una organización acreditada.

Para el Organismo Argentino de Acreditación (OAA) la definición de acreditación se da a continuación:

La acreditación es el reconocimiento formal de competencia e imparcialidad a laboratorios, proveedores de ensayos de aptitud, productores de materiales de referencia, organismos de certificación y/o de inspección. Se realiza mediante una

evaluación independiente en base a requisitos normativos internacionales, de acuerdo al esquema se utilizan diferentes normas reconocidas. (OAA. s.f.)

Los organismos se pueden acreditar, para certificar productos, personas y sistemas de gestión.

Como factor común todas las organizaciones de acreditación en sistemas de Gestión aplican como requisito el cumplimiento de la Norma ISO/IEC 17021-1:2015 “Evaluación de la Conformidad - Requisitos para los organismos que realizan la Auditoria y la Certificación de Sistemas de Gestión - Parte 1: Requisitos”precedida por NTP si se trata de Norma Peruana, Nch si se trata de Norma Chilena o NB para indicar Norma Boliviana.

En América existen organizaciones e instituciones las cuales promueven la interacción de la acreditación entre Países miembro, una de las principales organizaciones es la Cooperación Interamericana de Acreditación (IAAC).

Es necesario conocer a las organizaciones e instituciones correspondiente a cada País, que pueden acreditar a otras instituciones para otorgar la certificación ISO 27001, está misma norma según se menciona en diferentes regiones es reconocida por las abreviaturas que la anteceden ejemplo NB/ISO/IEC 27001 “NB” hace referencia a la Norma Boliviana, NCh-ISO27000 “NCh” hace referencia a la Norma Chilena y NBR/ISO/IEC 27001 donde “NBR” hace referencia a Norma Brasilera, se aclara que la familia de la Norma ISO 27000 mantiene la correspondencia con cada una de las citadas en cada región.

2.11.1 COOPERACIÓN INTERAMERICANA DE ACREDITACIÓN (IAAC)

La Cooperación InterAmericana de Acreditación es una asociación regional de organismos de acreditación y de otras organizaciones interesadas en la evaluación de la conformidad en América. (IAAC, 2020)

La misión de IAAC es promover la cooperación entre los organismos de acreditación y las partes interesadas en América, enfocada al desarrollo de las estructuras de

evaluación de la conformidad para lograr el mejoramiento de productos, procesos y servicios. (IAAC, 2020)

Entre los principales objetivos de IAAC están:

- ✓ Promover la aceptación regional e internacional de las acreditaciones otorgadas por sus miembros.
- ✓ Promover la aceptación regional e internacional de certificados de conformidad, informes de inspección, resultados de calibración y pruebas, emitidos por los organismos de evaluación de la conformidad acreditados.
- ✓ Desarrollar una infraestructura de acreditación regional y una infraestructura de evaluación de la conformidad eficiente y confiable.
- ✓ Establecer un sistema regional de acuerdos de reconocimiento multi-laterales entre los organismos de acreditación.

Cada país tiene un organismo nacional de acreditación, entre sus funciones está la acreditación de organismos de certificación, a continuación se mencionan los correspondientes a los países vecinos con los que Bolivia comparte frontera territorial: Argentina, Brasil, Chile, Paraguay y Perú, también se hace referencia a Colombia, que es uno de los países con mayor experiencia en temas de Seguridad de la Información.

2.12 ORGANISMOS DE ACREDITACIÓN Y CERTIFICACIÓN EN SISTEMAS DE GESTIÓN

En algunos países no existen organismos acreditados para certificar Sistemas de Gestión de Seguridad de la Información, sin embargo existen organismos acreditados internacionalmente, los cuales ofrecen servicios de certificación para los países de Sudamérica.

En todos los países de estudio, se cuentan con organismos Nacionales de acreditación, los cuales están regidos por decretos y leyes de acuerdo al País respectivo, a continuación se mencionan los organismos de acreditación y certificación.

2.12.1 INSTITUTO BOLIVIANO DE METROLOGÍA (IBMETRO)

El Instituto Boliviano de Metrología (IBMETRO), es una institución pública desconcentrada con relación de dependencia del Ministerio de Desarrollo Productivo y Economía Plural.

“El D.S. 29519 en su Capítulo IV, Artículo 15 (Atribuciones del Instituto Boliviano de Metrología), establece en su inciso e) lo siguiente:

e) Acreditación de los organismos de certificación que operan en el territorio nacional, sean estos nacionales o extranjeros como condición necesaria para que sus certificaciones sean reconocidas a nivel del Estado Boliviano.” (Instituto Boliviano de Metrología, 2018)

Esto representa que en cumplimiento a lo dispuesto por el D.S. 29519, en el Estado Plurinacional de Bolivia, solo son reconocidas las certificaciones de los organismos nacionales o extranjeros, acreditados por IBMETRO.

IBMETRO es la referencia nacional para todas las mediciones, cuenta un sistema Integrado de Gestión de Calidad en base a las normas ISO 9001, ISO/IEC 17025, ISO 17034 e ISO/IEC 17020, así como convenios y reconocimientos internacionales, efectuando trabajos conjuntos y coordinados con nuestros pares a nivel internacional.

Presta servicios de calibración, acreditación y verificación mediante la siguiente dirección técnica:

Acreditación de laboratorios de ensayo, laboratorios de calibración, laboratorios clínicos, organismos de certificación de sistemas de gestión, organismos de certificación de producto y organismos de inspección, además se organizan ensayos de aptitud. (Instituto Boliviano de Metrología, 2018)

La Dirección técnica de Acreditación del Instituto Boliviano de Metrología otorgo al Instituto Boliviano de Normalización y Calidad IBNORCA la acreditación como Organismo de Certificación de Sistemas de Gestión, de acuerdo a la norma ISO/IEC 17021-1:2015 para realizar certificaciones de Sistemas de Gestión. Vigencia de

Acreditación desde 2 de diciembre de 2017 hasta el 1 de diciembre de 2020. (IBNORCA Acreditada, s.f.)

2.12.1.1 INSTITUTO BOLIVIANO DE NORMALIZACIÓN Y CALIDAD (IBNORCA)

En Bolivia IBNORCA es el único representante de la Organización Internacional de Normalización (ISO) y el único organismo acreditado en Certificación de Sistemas de Gestión en el país. La acreditación garantiza y reconoce que IBNORCA tiene las competencias y cumple los requisitos para realizar labores de certificación a las organizaciones, adicionalmente verifica si en IBNORCA se ha implementado un Sistema de Gestión que asegure la imparcialidad, confidencialidad y calidad de sus certificaciones. (IBNORCA s.f.)

2.12.2 INSTITUTO NACIONAL DE NORMALIZACIÓN (INN)

En Chile el Instituto Nacional de Normalización (INN), está constituido como una fundación de derecho privado sin fines de lucro, como un organismo técnico en materias de la Infraestructura de la calidad. Entre una de sus responsabilidades está la elaboración de normas técnicas nacionales (normalización). El Instituto es uno de los veinticinco países fundadores de la International Organization for Standardization (ISO). Organismo del cual es parte de manera ininterrumpida desde su fundación en el año 1947. (INN, 2016)

La INN cuenta con la División Acreditación que tiene como funciones principales: operar los procesos de acreditación, según los reglamentos y procedimientos establecidos; supervisar los organismos de evaluación de conformidad acreditados; coordinarse con organismos gubernamentales para la acreditación en el área reglamentaria; difundir el Sistema Nacional de Acreditación y promover su uso; y actualizar el directorio de organismos de evaluación de la conformidad acreditados. (INN, 2016)

La INN acredita en los siguientes esquemas de acreditación:

- Organismos de certificación de sistemas

- Organismos de certificación de productos
- Organismos de certificación de personas

Solicita a INN, la acreditación como organismo de certificación de sistemas de acuerdo a la norma NCh-ISO 17021/1:2015

Los Organismos que desean acreditarse para otorgar Certificación de Sistemas de Gestión de Seguridad de la Información con la norma NCh-ISO27000, deberán cumplir los requisitos exigidos por el Instituto Nacional de Normalización. (INN, 2016)

2.12.3 INSTITUTO NACIONAL DE CALIDAD (INACAL)

En Perú el Instituto Nacional de Calidad (INACAL) es el ente rector y máxima autoridad técnico-normativa del Sistema Nacional para la Calidad, que tiene por finalidad promover y asegurar el cumplimiento de la Política Nacional para la Calidad con miras al desarrollo y la competitividad de las actividades económicas y la protección del consumidor. (INACAL, 2016)

Son competencias del INACAL la normalización, la acreditación y la metrología, las mismas que ejerce en el ámbito nacional. Realiza sus funciones acorde a lo previsto en el Acuerdo sobre Obstáculos Técnicos al Comercio, de la Organización Mundial del Comercio (OMC), y a los convenios internacionales y de integración sobre la materia de los que Perú es parte. (INACAL, 2016)

INACAL acredita Organismos de certificación de sistemas de gestión bajo el cumplimiento de sus correspondientes Normas Técnicas Internacionales ISO/IEC, las cuales han sido adoptadas como Normas Técnicas Peruanas NTP, como lo es la norma NTP-ISO/IEC 17021.

2.12.4 INSTITUTO NACIONAL DE METROLOGÍA, CALIDAD Y TECNOLOGÍA (INMETRO)

En Brasil el Instituto Nacional de Metrología, Calidad y Tecnología es una agencia federal vinculada al Departamento de Producción especial, Empleo y Competitividad, del Ministerio de Economía. El Instituto actúa como Secretario Ejecutivo del Consejo

Nacional de Metrología, Normalización y Calidad Industrial (Conmetro), inter-colegial, que es el órgano legislativo del Sistema Nacional de Metrología, Normalización y Calidad Industrial (Sinmetro). (Inmetro 2018)

Entre sus competencias está “Estimular el uso de técnicas de gestión de calidad en las empresas brasileñas” y la Acreditación de organismos de evaluación, bajo las normas ISO/IEC 17021 Evaluación de la conformidad. Requisitos para los organismos que realizan la auditoría y la certificación de sistemas de gestión. (Inmetro 2018)

La Coordinación General de Acreditación de Inmetro (Cgcre) es el único organismo de acreditación reconocido por el Gobierno brasileño para acreditar organismos de evaluación de la conformidad.

En Brasil, los organismos de certificación deben estar acreditados por el INMETRO.

Los organismos de certificación acreditados en el área de Sistemas de Gestión de Seguridad de la Información son:

- ✓ FCAV - Fundação Carlos Alberto Vanzolini
- ✓ TÜV Nord Brasil Avaliações da Qualidade EIRELI

2.12.5 INSTITUTO ARGENTINO DE NORMALIZACIÓN Y CERTIFICACIÓN (IRAM)

IRAM ha sido el primer organismo de certificación en ser acreditado por el Organismo Argentino de Acreditación (OAA) que es el representante de la Argentina ante los foros internacionales correspondientes como el IAF (International Accreditation Forum) y la IAAC (Interamerican Accreditation Co-operation)

IRAM está acreditado como Organismo de Certificación de Sistemas de Gestión Conforme a los criterios contenidos en la Norma IRAM-ISO/IEC 17021-1:2016 equivalente a la Norma ISO/IEC 17021-1:2015. (IRAM-ISO-IEC 17021: Evaluación de la conformidad. Requisitos para los organismos que realizan la auditoría y la certificación de sistemas de gestión. Parte 1 – Requisitos).

IRAM es el Instituto Argentino de Normalización y Certificación cuya visión es ser una institución referente en el ámbito nacional, regional e internacional para la mejora de la competitividad, el desarrollo sostenible y la calidad de vida del ciudadano. (IRAM s.f.)

IRAM participa activamente, como representante de la República Argentina, en los procesos de normalización internacional, en ISO e IEC, y en la normalización regional, en COPANT (Comisión Panamericana de Normas Técnicas) y AMN (Asociación Mercosur de Normalización). (IRAM s.f.)

IRAM brinda servicios de certificación de productos, procesos, personas, servicios y sistemas de gestión, tanto a nivel nacional como internacional. Entre los servicios que brinda IRAM está:

- ✓ Certificación bajo IRAM-ISO/IEC 27001 – Requisitos para la gestión de la seguridad de la información

2.12.6 ORGANISMO NACIONAL DE ACREDITACIÓN DE PARAGUAY

El Organismo Nacional de Acreditación (ONA), dependiente del Consejo Nacional de Ciencia y Tecnología (CONACYT), como parte integrante del Sistema Nacional de Calidad es la institución responsable de dirigir y administrar el Sistema Nacional de Acreditación y otorgar la acreditación en Paraguay. Entre sus funciones están el de llevar registro de las instituciones u organismos acreditados en Paraguay, elaborar reglamentos de procedimientos de acreditación, representar al Paraguay ante foros de acreditación regionales e internacionales. Para la acreditación de organismos de certificación, se utiliza la norma ISO/IEC 17021. (CONACYT,s.f.)

Una organización acreditada por la ONA es el Instituto Nacional de Tecnología, Normalización y Metrología (INTN) es una entidad pública, autárquica y descentralizada. Actualmente el INTN ha fortalecido su imagen institucional como una entidad técnica, científica y confiable, mediante los reconocimientos de las competencias técnicas de los laboratorios por organismo competente tanto nacional e internacional. En cuanto a certificación el INTN solamente se menciona la Certificación de Sistemas de Gestión de Calidad ISO 9001:2015 (INTN, 2016)

2.12.7 ORGANISMO NACIONAL DE ACREDITACIÓN DE COLOMBIA (ONAC)

ONAC cumple las actividades de Organismo Nacional de Acreditación de Colombia desde 2008. En dicho año, se suprimió el carácter de actividad pública administrativa de la acreditación y se reconoció plenamente su carácter técnico. (ONAC, s.f.)

El Organismo Nacional de Acreditación de Colombia - ONAC es una corporación sin ánimo de lucro, regida por el derecho privado, constituida en 2007 y que por disposición estatutaria se organizó bajo las leyes colombianas dentro del marco del Código Civil y las normas sobre ciencia y tecnología. (ONAC, s.f.)

ONAC tiene como objeto principal acreditar la competencia técnica de Organismos de Evaluación de la Conformidad, ejercer como autoridad de monitoreo en buenas prácticas de laboratorio de la Organización para la Cooperación y el Desarrollo Económico (OCDE) y desempeñar las funciones de Organismo Nacional de Acreditación de Colombia, conforme con la designación contenida en el capítulo 26 del Decreto 1074 de 2015 y las demás normas que los modifiquen, sustituyan o complementen. (ONAC, s.f.)

ONAC presta servicios de acreditación de acuerdo con los requisitos de la norma ISO/IEC 17011 "Evaluación de la Conformidad Requisitos generales para los organismos de acreditación que realizan la acreditación de organismos de evaluación de la conformidad" y con las políticas, criterios y lineamientos establecidos por la Cooperación Internacional de Acre-ditación de Laboratorios (ILAC), el Foro Internacional de Acreditación (IAF) y la Cooperación Inter Americana de Acreditación (IAAC). (ONAC, s.f.)

COLOMBIA ONAC acredita a los organismos de certificación de sistemas de gestión con requisitos de la norma ISO /IEC 17021 Requisitos para los organismos que realizan la Auditoría y Certificación de Sistemas de Gestión.

En la reunión intermedia de International Accreditation Forum (IAF), llevada a cabo en Frankfurt, Alemania en abril de 2018, IAF otorgó a ONAC el reconocimiento internacional para la acreditación en sistemas de gestión, de tres nuevos campos, en

nivel cinco: ISO 22000, sistemas de gestión de seguridad alimentaria; ISO/IEC 27001, sistemas de gestión en seguridad de la información e ISO 13485, sistemas de gestión de calidad de dispositivos médicos. (ONAC, 2018)

Con este importante logro, ONAC no solo continúa avanzado en su propósito de ofrecer a Colombia una amplia gama de servicios de acreditación con reconocimiento multilateral, sino que se convierte con ello en uno de los cinco países con mayor número de alcances reconocidos mundialmente por IAF en sistemas de gestión. Adicionalmente, como miembros de la Cooperación Inter Americana de Acreditación, con la suscripción de este acuerdo por parte de ONAC, el mismo constituye un reconocimiento también para IAAC como cooperación regional de la acreditación en América. (ONAC, 2018)

Los organismos acreditados en Colombia por el ONAC bajo cumplimiento de los requisitos de la Norma ISO 17021 son:

- ✓ CERTIFICATION QUALITY RESOURCES SAS-SIGLA: CQR SAS
- ✓ GLOBAL COLOMBIA CERTIFICACIÓN S.A.S
- ✓ SGS COLOMBIA S.A.S. – SGS
- ✓ BVQI COLOMBIA LTDA.
- ✓ INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN – ICONTEC

Las cinco empresas mencionadas son capaces de evaluar y certificar los sistemas de Gestión de Seguridad de la información con el alcance de la norma ISO 27001.

La presentación respecto a la existencia de los organismos de acreditación y certificación son algo confusos, lo que se puede extraer es que en cada País existe un organismo de acreditación, que es regido por leyes y decretos propios de cada País, el cual tiene como uno de sus propósitos generales acreditar a organismos en diferentes rubros como ser productos, personas y sistemas, cada uno de estos organismos presenta sus requisitos que deben cumplirse para ser un organismo acreditado de certificación, también se puede consultar sobre las empresas acreditadas.

Para que los requisitos sean uniformes y estandarizados existe el IAAC, que mediante acuerdo y requisitos, permite que una entidad acreditada pueda extender una certificación de un País a otro. El IAAC no es una organización exclusiva a acreditar solo a organizaciones en el tema de sistemas de gestión, su propósito va al campo de toda acreditación, como ser productos, laboratorios, entre otros.

Las Empresas corredoras pueden implementar un Sistema de Gestión de Seguridad de la Información, que trae muchas ventajas, sin necesidad de requerir una certificación ISO 27001, sin embargo para la demostración y reconocimiento ante las partes interesadas, la certificación ISO 27001 acreditada, es el camino para demostrar la conformidad de las exigencias del estándar.

En cada País existen organismos de certificación, los cuales deben obtener acreditación para conferir certificaciones y realizar las auditorias de certificación. En los países en estudio, sólo hay un organismo de acreditación por País.

Los organismos de acreditación tienen acuerdos internacionales para reconocimiento mutuo de acreditaciones y establecer criterios estándar. Con este propósito son reconocidos en América del Sur la IAF (International Accreditation Forum), la IAAC (The InterAmerican Accreditation Cooperation) entre las más sobresalientes.

La debida acreditación y la certificación cumpliendo requisitos de normas ISO son reconocidas a nivel mundial. Si la empresa no está debidamente acreditada, entonces el certificado de certificación emitido puede no tener validez.

En los países de estudio incluido Bolivia existen pocas empresas acreditadas que certifican norma ISO 27001, mediante acuerdos de cooperación que impulsa el IAAC, es que las acreditaciones transfrontera permite que una organización fuera de un País pueda certificar dentro de otro País, cumpliendo requisitos de las normas establecidas.

También se puede indicar que Colombia es un País con mucha experiencia en el campo de certificaciones ISO 27001, es así que mediante ICONTEC otorga la certificación ISO 27001 al INACAL de Perú.

Cuando se requiera de una certificación ISO 27001 en Bolivia, se deberá averiguar si el organismo está acreditado para otorgar una certificación, es así que en el caso de Bolivia el IBMETRO (Instituto Boliviano de Metrología) es la única institución por decreto supremo, que acredita a los organismos de certificación. Siendo un requisito para el Organismo de Certificación de Sistemas de gestión cumplir con los requisitos de la NB/ISO/IEC 17021-1 que ha sido desarrollado en el marco teórico. En este sentido IBNORCA ha sido acreditada para otorgar certificación en los Sistemas de Gestión.

La acreditación es un documento escrito, donde una organización de acreditación superior cumpliendo los requisitos de la norma ISO/IEC 17011 tiene la potestad de acreditar, ONAC de Colombia es una de las organizaciones que puede acreditar a otra organización, aplicando la norma ISO 27001.

Solamente como ejemplo en el caso de Colombia la ONAC ha otorgado la acreditación a ICONTEC, mediante el cumplimiento de los requisitos de la norma ISO 27001, para otorgar certificaciones en Sistemas de Gestión de la Seguridad de la Información aplicando la norma ISO 27001.

La certificación es un documento escrito, donde un tercero acreditado da la conformidad de cumplimiento con los requisitos del estándar ISO 27001.

Son dos extremos que se pueden notar entre los países en estudio, Colombia que cuenta con cinco organizaciones de certificación acreditadas, para certificar la norma ISO 27001, Paraguay no cuenta con institución acreditada localmente para otorgar certificación de la Norma ISO 27001, de acuerdo al detalle de Certificación de Sistemas de Gestión solamente se menciona el Sistemas de Gestión de Calidad ISO 9001:2015.

En el caso de Bolivia, IBNORCA es el único organismo acreditado por IBMETRO para certificar sistemas de gestión.

2.13 CONVENIO DE BUDAPEST

Conocido también como el Convenio sobre la Ciberdelincuencia, que es parte de la serie de tratados Europeos Nº 185, hecho en Budapest el 23 de noviembre de 2001,

extraemos las bases del preámbulo, Convention on Cybercrime, (2001) que indica lo siguiente:

Convencidos de la necesidad de aplicar, con carácter prioritario, una política penal común con objetos de proteger a la sociedad frente a la ciberdelincuencia, en particular mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional.

“Estimando que la lucha efectiva contra la ciberdelincuencia requiere una cooperación internacional reforzada, rápida y eficaz en materia penal”

Convencidos de que el presente Convenio es necesario para prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, garantizando la tipificación como delito de dichos actos, tal como se definen en el presente Convenio, y la asunción de poderes suficientes para luchar eficazmente contra dichos delitos, facilitando su detección, investigación y sanción, tanto a nivel nacional como internacional, y estableciendo disposiciones materiales que permitan una cooperación internacional rápida y fiable.

El convenio consta de 48 artículos, entre los cuales podemos mencionar:

- Artículo 4. Ataques a la Integridad de los Datos
- Artículo 5. Ataques a la integridad de los sistemas
- Artículo 6. Abuso de los dispositivos
- Artículo 19. Registro y confiscación de datos informáticos almacenados
- Artículo 29. Conservación rápida de datos informáticos almacenados

En el artículo 37. Adhesión al Convenio, indica: “A partir de la entrada en vigor del presente Convenio, el comité de Ministros del Consejo de Europa podrá, previa consulta con los Estados contratantes del Convenio y habiendo obtenido su consentimiento unánime, invitar a adherirse al presente Convenio a cualquier Estado

que no sea miembro del Consejo de Europa y que no haya participado en su elaboración...”

Tal como hace referencia, es de vital importancia la ayuda entres estados, para poder afrontar la ciberdelincuencia, ya que el Internet no tiene fronteras, y el convenio de Budapest es una buena referencia, que deber ser analizada.

2.14 HONEYPOT

El honeypot es una estrategia de ciberseguridad dirigida, entre otras cosas, a engañar a los posibles cibercriminales. Ya sea mediante software o a través de la acción humana, el honeypot hace que una empresa simule tener algunas “puertas de entrada” a sus sistemas que no han sido suficientemente protegidas.

La táctica es la siguiente. De manera previa, una empresa decide habilitar una serie de servidores o sistemas cuyo aspecto parezca sensible. Aparentemente, esa empresa se ha dejado varios cabos sin atar y parece vulnerable. Una vez dejada la trampa, la intención es atraer al atacante, que acudirá a la llamada para intentar entrar. Sin embargo, lo que el cibercriminal no sabe es que, lejos de estar encontrando una puerta vulnerable, en realidad está siendo perfectamente controlado y monitorizado por la empresa en cuestión.

De este modo, las empresas obtienen un beneficio triple: en primer lugar, contener posibles ataques verdaderamente peligrosos; en segundo, entretener y desgastar al atacante haciéndole perder el tiempo; y en tercero, analizar sus movimientos para detectar posibles nuevas formas de ataque que se estén llevando a cabo en el sector.

El honeypot es similar al llamado contraespionaje de ciberseguridad, que también opta por colocar señuelos de ciberseguridad que, aparentando ser vulnerables, consigan atraer a los atacantes para engatusarlos y frenar sus ataques a la vez que espían, analizan y monitorizan todos sus movimientos.

El honeypot, en definitiva, es una estrategia que puede resultar muy útil, sobre todo, en el caso de las grandes empresas, ya que suelen almacenar mucha más información

confidencial y, por su propio volumen de actividad, resultan más atractivas para los posibles atacantes.

El uso e implementación de un honeypot en una red hogareña no es ni práctica ni económica. Requiere de buenos conocimientos de informática y en especial de seguridad informática, de equipos y recursos dedicados que no suelen estar al alcance de cualquiera.

Sin embargo pueden usarse a modo de investigación o educativos sistemas honeypot gratuitos, como el comentado PenTBox Security Suite.

2.15 CIBERSEGURIDAD

ITU Ciberseguridad (abril 2008), indica:

Ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización son los dispositivos informáticos conectados, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes:

• Disponibilidad;
• Integridad, que puede incluir la autenticidad y el no repudio;
• Confidencialidad.

El ciberentorno incluye el software que se ejecuta en los dispositivos informáticos, la información almacenada (y transmitida) en estos dispositivos o la información que éstos generan. Las instalaciones y edificios donde residen los dispositivos también forman parte del ciberentorno.

2.16 CRIPTOGRAFÍA

Mendoza T., Julio César (2008), indica que: la criptografía es una palabra que proviene de las palabras griegas Kriptos (ocultar) y graphos (escritura). Literalmente significa “escritura oculta”, es decir mantener seguro los secretos mediante la codificación de los mensajes para hacerlos ilegibles, de tal manera que solo pueda verla aquel receptor que el emisor desea.

En terminología de cifrado:

• El mensaje original recibe el nombre de texto claro.

• El mensaje codificado se denomina texto cifrado.

• El proceso de convertir el texto claro en texto cifrado se denomina cifrado.

• El proceso de recuperar el texto claro a partir del texto cifrado se denomina descifrado.

Una parte importante de la aplicación de los algoritmos criptográficos son las claves. Una clave criptográfica es similar a una llave física que se usa para cerrar o abrir una puerta.

Cada algoritmo criptográfico necesita una clave con la extensión correcta (número correcto de bits). Se puede procesar un algoritmo criptográfico con cualquier clave que tenga la longitud apropiada, pero solo la que tenga el patrón correcto de bits hará que el algoritmo descifre la información cifrada.

El cifrado ayuda a garantizar: confidencialidad, autenticación e integridad.

2.16.1 CIFRADO AES – 256

Techlandia (2001 – 2019) indica que:

El estándar de cifrado avanzado (AES, por sus siglas en inglés) describe una fórmula matemática o algoritmo, para la conversión de datos electrónicos en una forma ininteligible, denominada texto cifrado. El texto cifrado no puede ser leído por cualquier persona que no sea el destinatario. El AES funciona alimentando una clave de cifrado, esencialmente una cadena de dígitos en el algoritmo de cifrado y realizando de una serie de operaciones matemáticas basadas en esa clave de cifrado.

El AES puede ser descrito como un bloque cifrado iterativo y simétrico. El AES utiliza una estructura de bucle para realizar repetidamente reordenamientos de datos, o permutaciones. El bucle reemplaza una unidad de datos con otra para datos de entrada. La rutina de cifrado utiliza la misma clave para cifrar y descifrar los datos, y aplica esa clave a los bloques de datos de longitud fija.

AES es lo que se conoce como un cifrado simétrico por bloques, lo que significa que cifra y descifra los datos en bloques de 128 bits cada uno. Para ello, utiliza una clave criptográfica específica, que es efectivamente un conjunto de protocolos para manipular información. Esta clave puede ser de 128, 192 o 256 bits de tamaño.

2.17 SISTEMA DE ALMACENAMIENTO DE DATOS DIGITALES

Según indica *Salvador E. Vásquez Moctezuma (julio, 2015):*

El ser humano en cada época se ha encontrado en la necesidad de mejorar sus mecanismos de almacenamiento a causa del incremento del número de datos producidos y los retos que surgen por el manejo de información. El desarrollo tecnológico ha permitido que los centros de datos dedicados al almacenamiento estén estructurados de una o varias combinaciones de las siguientes cuatro formas: DAS, NAS, SAN y almacenamiento en la nube.

2.17.1 Almacenamiento de Conexión Directa (DAS)

Direct Attached Storage o DAS es una de las formas más sencillas y tradicionales del almacenamiento de conexión directa, donde las unidades de disco se encuentran conectadas directamente con los servidores o host.

De acuerdo con (*Salvador E. Vásquez Moctezuma (2015), que cita a* Zhao (2006)) las conexiones en DAS tienen muchas ventajas, tales como: su instalación es fácil; el software es poco complejo; el costo en mantenimiento es bajo; la tecnología presenta madurez técnica, buena compatibilidad y, relativamente, es de menor gasto.

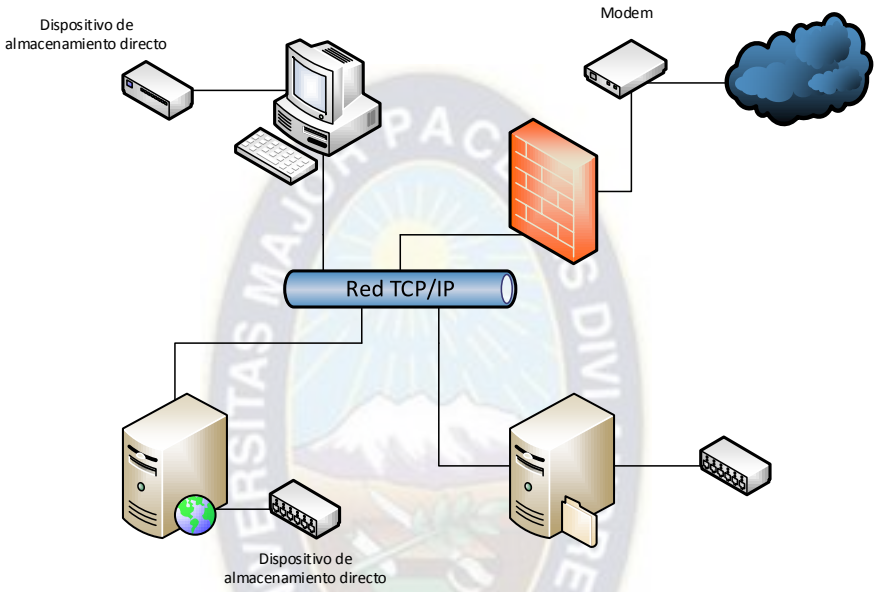


Figura 2.6 Almacenamiento de Conexión Directa DAS

Fuente: Elaboración propia

Se convierte en la elección previa para las pequeñas unidades de información, debido a que cuentan con menos recursos financieros. Principalmente es utilizado en las computadoras personales y pequeños servidores, que soportan solo aplicaciones que requieren capacidades bajas de almacenamiento.

2.17.2 Almacenamiento conectado en red (NAS)

El Almacenamiento Conectado en Red o NAS (del acrónimo inglés Network Attached Storage) es un dispositivo que se conecta a la red y provee un almacén de datos que permite a varios hosts acceder al mismo lugar de almacenamiento a través de una red IP. Este dispositivo se encuentra en la red LAN; por lo tanto NAS depende de ciertas características de LAN.

El sistema NAS, tiene ventajas tales como facilidad en la instalación, complementos o extensiones (plugs), flexibilidad de conexión, fácil mantenimiento, seguridad de autenticación, administración de espacio en disco y escalabilidad. NAS es una opción ideal para organizaciones pequeñas y medianas que buscan, de una manera simple y rentable, lograr el acceso de datos rápido en nivel de archivo para varios usuarios.

En la siguiente figura 2.7, se puede observar una red, en la cual se conecta un dispositivo NAS a la red.

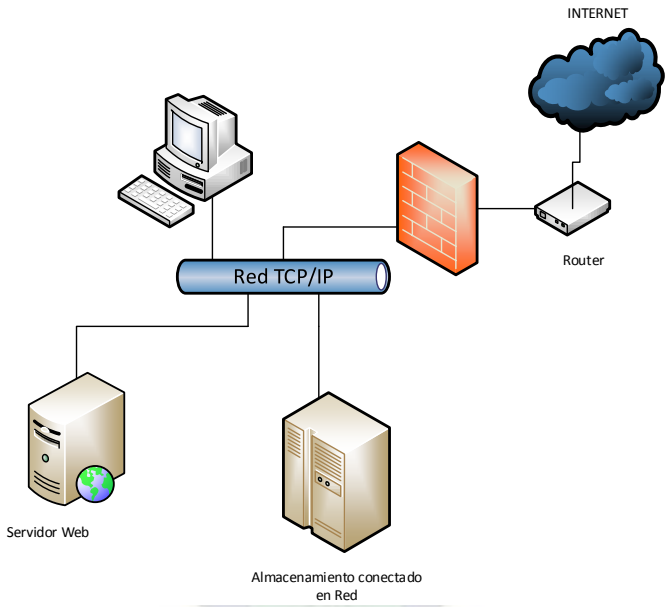


Figura 2.7 Red Ethernet con dispositivo NAS

Fuente: Elaboración propia

2.17.2.1 Equipos NAS

En Profesional Review (2011 – 2019) indica que:

Los NAS actuales soportan distintos sistemas de almacenamiento y no solamente tienen la opción de instalar en ellos discos duros mecánicos SATA (Serial Advanced Technology Attachment) tradicionales. Los nuevos modelos soportan todo tipo de unidades SSD (**Solid State Drive**) e incluso unidades ultrarrápidas como son las M.2 SATA (M.2 Serial Advanced Technology Attachment) y PCIe (Peripheral Component

Interconnect Express). Estos NAS cuentan con la capacidad de realizar RAID híbridos entre diferentes unidades o también destinar las unidades de mayor velocidad a elementos de caché de acceso rápido.

También tienen gestión propia de permisos de acceso mediante cuentas de usuario a según qué directorios o archivos se configuren. Pero además la cantidad de usuarios que vayan acceder al NAS será un aspecto muy importante, siendo un factor para elegir la potencia de almacenamiento del NAS.

En las siguientes figuras, se pueden observar equipos NAS, con puerto RJ- 45, para conectarse directamente a la red, la Figura 2.8 es un equipo NAS que puede utilizarse para empresas pequeñas y en la Figura 2.9 se puede observar un equipo NAS de alto rendimiento para empresas grandes.

Figura 2.8 Equipo NAS, con puerto RJ-45
Fuente: Profesional Review (2011-2019)

Figura 2.9 Equipo NAS de alto rendimiento
Fuente: Profesional Review (2011 – 2019)

Otra de las funciones principales de los NAS, es la de configurar copias de seguridad de varios dispositivos para que actúen como si fueran una nube privada. Con ello, se puede sincronizar copias de seguridad de determinados archivos en varios dispositivos, pudiendo acceder desde cualquiera de ellos.

A las ranuras que tiene el NAS para los discos duros se les llama bahías, y también es importante decidir cuántas se requieren. Para usuarios domésticos convencionales suele haber modelos de una y dos bahías, aunque también hay dispositivos más avanzados con más de ellas.

2.17.2.2 Criptografía en NAS

Encriptar archivos es sencillo de hacer en Servidores NAS tanto si se quiere encriptar los datos de un volumen de almacenamiento completo como de una sola carpeta. Lo más normal es trabajar con el volumen encriptado por completo ya que de esta forma los datos estarán a salvo incluso en el caso de que el servidor sea sustraído de la empresa.

Hay varios tipos de Encriptación que se pueden utilizar con un servidor NAS pero la más habitual es la encriptación de archivos con el AES de 256 bit.

Uno de los inconvenientes con un almacenamiento de datos encriptado es que el trabajo de encriptación requiere de un hardware potente o en su defecto un hardware preparado específicamente para esta función. Al consumir tantos recursos, es fácil que en un sistema que no esté preparado para trabajar con encriptación de archivos sufra una gran bajada de rendimiento. Para mitigar los efectos de la encriptacion y desencriptacion que se realiza en cada uno de los accesos a los datos hay servidores NAS con procesadores específicos para esta función.

Los Servidores NAS que cuentan con esta funcionalidad suelen tenerla dentro de sus especificaciones técnicas como Encriptación de datos acelerada por hardware o Motor de cifrado por hardware.

2.17.3 Red de Área de Almacenamiento (SAN)

Existe la red de área de almacenamiento o Storage Area Network, por sus siglas en inglés SAN.

Se centra en el almacenamiento de datos utilizando una topología de red flexible, además, con conexiones de fibra óptica que permiten alta velocidad en la transferencia de datos; ofrece la conmutación entre múltiples nodos. SAN es otro enfoque de almacenamiento compartido que a menudo se usa en la nube. En SAN, la gestión del almacenamiento de datos se encuentra relativamente independiente a la red de área local, con el fin de lograr el máximo grado de intercambio de datos, así como la extensión del sistema.

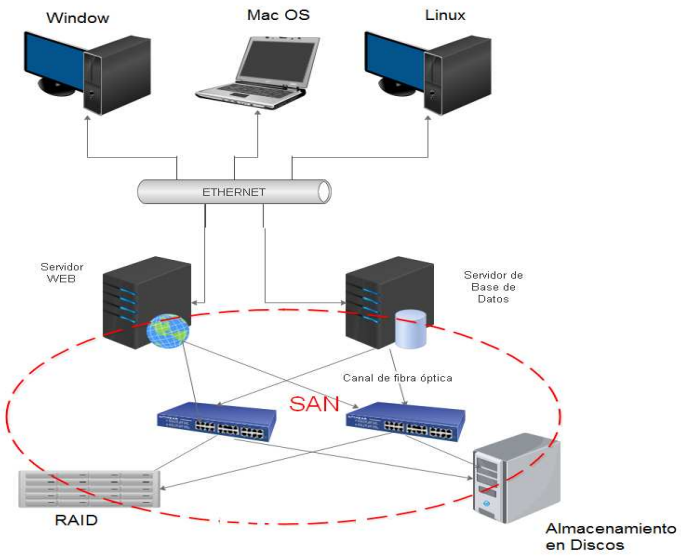


Figura 2.10 Red de Almacenamiento SAN

Fuente: Elaboración propia

La tecnología SAN, se orienta a la alta velocidad de procesamiento de datos masivos, lo que incluye alta velocidad en el acceso, almacenamiento seguro, intercambio de datos, respaldo de datos, migración de los datos, entre otras ventajas de los sistemas distribuidos. El canal de fibra o FC es de gran fiabilidad, a causa de la tecnología de interconexión en gigabytes que provee la comunicación simultánea entre distintas estaciones de trabajo, mainframes, servidores, sistemas de almacenamiento y otros

periféricos de entrada o salida. Cuando se necesita gestionar el sistema de almacenamiento SAN será complejo por la gran cantidad de información, además del alto costo de la infraestructura para el uso de fibra óptica. Así SAN FC es adecuado para grandes unidades de información que tienen mayores presupuestos y requerimientos altos de transferencia y transmisión de datos.

2.17.4 Cloud Computing

El modelo de la nube, según NIST (National Institute of Standards and Technology), se compone de cinco características esenciales, tres modelos de servicio y cuatro modelos de despliegue. La nube en sí misma, es un conjunto de hardware y software, almacenamiento, servicios e interfaces que facilitan la entrada de la información como un servicio.

El NIST además de dar la definición de la Nube, define los modelos de entrega y despliegue de servicios en la Nube más usuales que se ofrecen a los clientes y usuarios de la nube (organizaciones, empresas y usuarios) son:

- PaaS (Platform as a Service), plataforma como servicio,
- IaaS (Infraestructure as a Service), infraestructura como servicio y
- SaaS (Software as a Service), software como servicio

Una bondad de los entornos de la nube es que, proporciona una posible herramienta para el almacenamiento de grandes volúmenes de datos. El almacenamiento en la nube o cloud storage es el espacio para copiar datos, información, objetos digitales, y otros, que se acceden por internet a través de un servicio web, mediante un navegador como Explorer, Firefox y Chrome. (*Salvador E. Vásquez Moctezuma, julio 2015*)

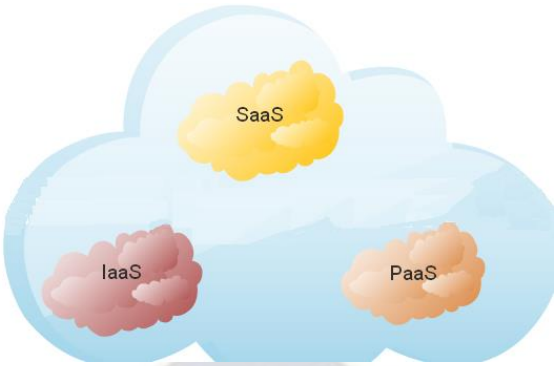


Figura 2.11 Servicios en Cloud Computing
Fuente: Elaboración propia

2.18 CIFRADOS EN BASE DE DATOS

Existe una presunción sobre la afectación del rendimiento de la base de datos cifrada respecto a la no cifrada, como se muestra en el Figura 2.12.

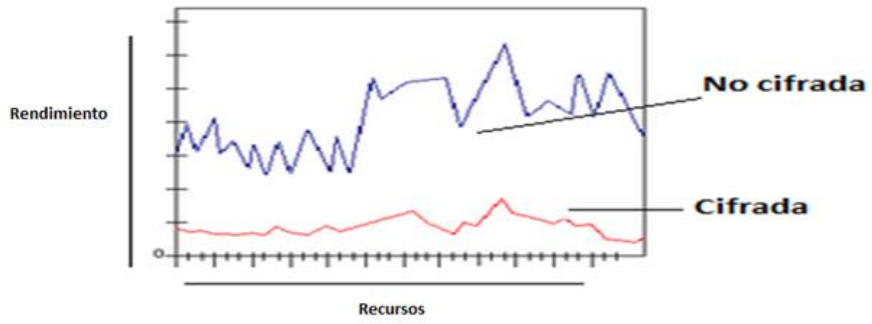


Figura 2.12 Rendimiento en base de datos cifradas (Seguridad de la Información, 2018)
Fuente: Elaboración Propia

Si la organización desea aplicar el cifrado es importante conocer por qué se desea utilizar una base de datos cifrada, ya que esto ayuda a decidir la forma de conectarse, ejecutar transacciones y realizar consultas. Si todas las aplicaciones de la organización comparten el mismo motor de base de datos local y la base de datos está cifrada, al conectar cualquier aplicación o al leer y escribir en un archivo de la base de datos, ésta deberá proporcionar la clave de cifrado.

Para usar una base de datos cifrada debe crearse como cifrada, esto es una opción que existe en la mayoría de los sistemas gestores de bases de datos. Las técnicas para trabajar con una base de datos cifrada son las mismas que para el trabajo con una base de datos no cifrada. (Seguridad de la Información, 2018).

2.19 SEGURIDAD EN VPN

Una VPN es una Red Privada Virtual, que utiliza una red pública (por lo general, Internet) para conectar sitios o usuarios remotos entre sí. En vez de utilizar una conexión real dedicada como línea arrendada, una VPN utiliza conexiones "virtuales" enrutadas a través de Internet desde la red privada de la empresa hacia el empleado o el sitio remoto. (Cisco, 2008)

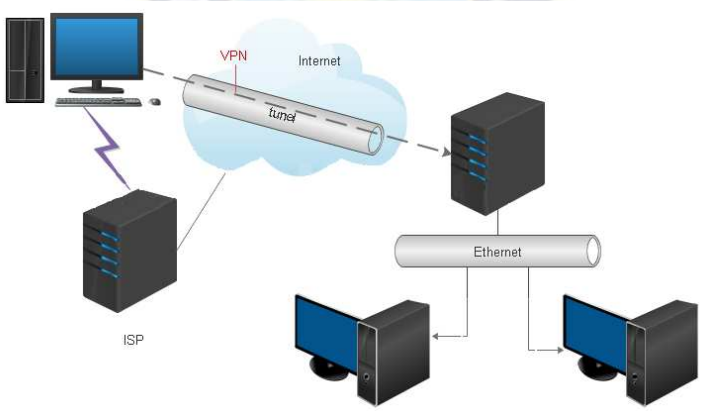


Figura 2.13 VPN Red Privada Virtual

Fuente: Elaboración propia

En aspecto de seguridad en VPN se debe conocer a los códigos de cifrados VPN y los protocolos de VPN.

Códigos de Cifrado VPN

Un código de cifrado es un algoritmo que se utiliza para realizar el proceso de cifrado y descifrado. A diferencia de las claves de cifrado que no se pueden descifrar de manera realista, los códigos de cifrado pueden tener debilidades que hacen posible romper el cifrado. (Tim Mocan, 2019)

Ese tipo de problema de seguridad se evita fácilmente mediante el uso de un cifrado complejo junto con una clave de cifrado fuerte. El nombre de un cifrado VPN normalmente irá acompañado de la longitud de la clave (AES-128, por ejemplo).

Los principales tipos de cifrado que usan los proveedores de VPN:

El código Blowfish: es un sistema de codificación de bloques simétricos. Nos permite codificar información con una llave y decodificarla sólo con la misma llave.

El Código Twofish: este es el sucesor de Blowfish. La principal diferencia es que Twofish tiene un tamaño de bloque de 128 bits en lugar del de 64 bits que tiene Blowfish.

El Código AES: AES puede tener claves de 128 bits, 192 bits y 256 bits. AES es muy popular entre los usuarios de VPN gracias a su certificación NIST.

El Código Camellia: Es rápido y admite claves de 128 bits, 192 bits y 256 bits. Sin embargo, dado que aún no se ha probado exhaustivamente contra posibles debilidades, no tiene certificaciones.

El Código 3DES: Triple DES (3DES; también conocido como TDEA / Triple DEA) es básicamente el Estándar de Cifrado de Datos (DES) que se utiliza tres veces. Es más lento que Blowfish, y solo admite claves de 56 bits, 112 bits y 168 bits. Además, como Blowfish, tiene un tamaño de bloque de 64 bits, lo que lo hace susceptible. Un detalle importante que vale la pena mencionar es que este código ha sido retirado oficialmente y su uso estará prohibido después de 2023.

El Código MPPE: MPPE significa cifrado punto a punto de Microsoft, y es un código que se usa a menudo para conexiones PPTP y conexiones de acceso telefónico. El código admite claves de 40 bits, claves de 56 bits y claves de 128 bits.

El código RSA (Rivest, Shamir y Adleman): Es un sistema criptográfico de clave pública desarrollado en 1979. Es el primer y más utilizado algoritmo de este tipo y es válido tanto para cifrar como para firmar digitalmente. Es otro algoritmo que se puede usar para comunicaciones seguras en línea, la mayoría de los proveedores de VPN usan

RSA para cifrado de apretones de manos ya que el encriptado es relativamente lento. En general, RSA no se utiliza para cifrar directamente los datos del usuario debido a eso. La clave RSA de 1024 bits ya no se considera segura, y los expertos en seguridad recomiendan usar la de 2048 o 4096 bits.

Un “apretón de manos” representa esa comunicación automática entre dos dispositivos de comunicación. Básicamente, se refiere a cómo el cliente VPN y el servidor VPN establecen las claves de encriptado que se utilizan para la comunicación (cifrado y descifrado).

Durante el protocolo de enlace, el cliente y el servidor:

- Generan las claves de cifrado.
- Acuerdan qué protocolo VPN se utilizará.
- Seleccionan los algoritmos criptográficos apropiados.
- Se autentican mutuamente con la ayuda de certificados digitales.

2.19.1 PROTOCOLOS DE ENCRIPTACIÓN VPN

Un protocolo VPN es un conjunto de instrucciones que se utilizan cuando se establece una conexión segura entre dos dispositivos. En este caso, los dos dispositivos seguros serían el dispositivo en el que ejecuta el cliente VPN y el servidor VPN al que se conecta. (Tim Mocan. 2019)

Los proveedores de VPN normalmente usan múltiples tipos de protocolos VPN cuando negocian conexiones seguras.

Los protocolos VPN son:

PPTP (Point to Point Tunneling Protocol): un protocolo de cifrado VPN relativamente veloz. PPTP admite VPN multiprotocolo, con cifrado de 40 bits y 128 bits mediante un protocolo denominado Cifrado de punto a punto de Microsoft (MPPE). Es importante tener en cuenta que PPTP no proporciona cifrado de datos por su cuenta.

L2TP / IPSec : Por sí solo, L2TP (Layer 2 Tunneling Protocol) no proporciona cifrado, por lo que siempre está emparejado con IPSec. Juntos, crean un protocolo bastante seguro. Comúnmente denominado L2TP a través de IPsec, proporciona la seguridad del protocolo de IPsec a través de los túneles de Protocolo de túneles de capa 2 (L2TP). Los proveedores de servicios de Internet también pueden brindar conexiones L2TP para usuarios de acceso telefónico y, luego, cifrar el tráfico con IPsec entre su punto de acceso y el servidor de red de la oficina remota.

IPSec (Internet Protocol Security) : IPSec es un conjunto de protocolos de red seguros que se utiliza para cifrar paquetes de datos que se envían a través de una red IP. Presenta una alta seguridad y puede cifrar el tráfico sin que la aplicación de punto final lo sepa. En la tecnología VPN, IPSec se usa a menudo junto con L2TP e IKEv2.

IKEv2 (protocolo Internet Key Exchange versión 2) : IKEv2 es relativamente rápido, estable y seguro (si se utiliza un cifrado como AES). Con respecto a las desventajas, IKEv2 puede ser difícil de implementar en el lado del servidor VPN. Los cifrados usados para generar las claves Phase1 son AES-256-GCM para cifrado, junto con SHA2-384 para garantizar la integridad, combinado con PFS (Perfect Forward Secrecy) con claves.

OpenVPN: Un protocolo de código abierto, OpenVPN es muy seguro y configurable. El principal inconveniente del protocolo parece ser el hecho de que usarlo con códigos de cifrado fuertes a veces puede ralentizar las velocidades de conexión.

SSTP (Secure Socker Tunneling Protocol): Este protocolo a menudo se compara con OpenVPN, ya que utiliza SSL 3.0 (Secure Sockets Layer), lo que le permite evitar la censura mediante el puerto 443 (el puerto de tráfico HTTPS). SSTP hace uso de certificados SSL/TLS de 2048 bits para la autenticación y claves SSL de 256 bits para el cifrado lo cual lo convierte en un protocolo bastante seguro.

WireGuard: Es un nuevo protocolo VPN de código abierto que tiene como fin simplificar el proceso de cifrado de datos. Promete ser más rápido y ligero que OpenVPN e IKEv2, los dos protocolos que están considerados los mejores

actualmente. Su creador, Jason Donenfeld, tiene una trayectoria impresionante en el campo de la seguridad de Internet. Aunque él es el primero en admitir que aún no existe una versión estable de WireGuard, la llegada de un nuevo protocolo innovador y potencialmente disruptivo es un tema muy importante en el mundo de las VPNs. (VPNmentor, 2019)

2.20 LA FUERTE AUTENTICACIÓN: DESDE LA CONTRASEÑA HACIA LA AUTENTICACIÓN MULTI-FACTORES

Evidian, (2015):

Autenticación o identificación

Existe una diferencia muy simple entre identificación y autenticación: el comprobante.

Una identificación se basa en una simple declaración como la recepción o la lectura de un código de identificación (identificador, n° serie, código barra,…). Este código de identificación no se supone secreto. Es un dato público.

La autenticación se basa en un elemento de prueba como un secreto compartido o un secreto asimétrico. La autenticación permite asegurarse con un nivel de confianza razonable de la identidad del usuario.

Siete elementos de autenticación

Para autentificarse, un usuario proporciona en general al menos 2 elementos:

- Su identificador que permite su definición.
- Uno o más elementos que permiten garantizar la propia autenticación.

Se encuentran elementos bajo distintas formas. Ahí se tienen los más utilizados:

TIPO	DESCRIPCIÓN
El identificador y la contraseña	El identificador y la contraseña son el par de autenticación más conocido. Simple, robusto, incluso rústico, su más grande defecto es que el nivel de seguridad depende directamente de la complejidad de la contraseña. Contraseñas simples son escasas,

	y contraseñas demasiado complejas conducen a los usuarios a aplicar estrategias no siempre correctas para gestionarlas: lista en un archivo Excel o en el SmartPhone.
El identificador y la contraseña OTP (One-Time Password)	El OTP permite asegurar el uso de la contraseña en la red. En efecto, con un sistema OTP el usuario posee un calculador especializado que le proporciona bajo petición una contraseña. Esta contraseña es válida solo durante una duración limitada, y para una única utilización. Esta solución se aplica en general para el proceso de autenticación inicial para los accesos externos mediante IP/VPN
Los certificados PKI sobre tarjeta inteligente o token USB	Los certificados X.509 aplican una tecnología avanzada decodificación que permite calcular o firmar mensajes sin tener que compartir de secreto. El identificador es un certificado público que es firmado y en consecuencia garantizado por una autoridad de certificación reconocida. El usuario debe proporcionar un secreto para poder utilizar los distintos elementos criptográficos: “el código PIN de su tarjeta o su tecla USB”. Esta solución se aplica en general para el proceso de autenticación inicial o para las conexiones a las aplicaciones Red o de servicio de mensajería.
Tecla “Confidencial Defensa”	Se trata de una declinación particular del ejemplo anterior. Es en general una llave multifunciones: almacenamiento de certificado X.509, almacenamiento de datos, recurso criptográfico etc.
El identificador y la contraseña sobre una tarjeta inteligente	El almacenamiento del identificador y la contraseña sobre una tarjeta inteligente permite suplementar la protección del proceso de autenticación. La contraseña puede así ser muy compleja y cambiada regularmente de manera automática y aleatoria. Sin la tarjeta, y sin su código PIN, no se puede acceder a la contraseña. Esta solución se aplica generalmente para el proceso de autenticación inicial.
Biométrica	La autenticación por biométrica se basa en la verificación de un elemento del cuerpo del usuario (generalmente la huella dactilar). Puede basarse en un distribuidor central, en el puesto de trabajo o en una tarjeta inteligente para almacenar los datos biométricos del usuario. Esta solución se aplica en general para el proceso de autenticación inicial y/o para proteger el acceso a aplicaciones muy sensibles.

La definición sin contacto	El RFID es una tecnología que hoy se despliega en los proyectos de Identificación/Autenticación. Un chip RFID es insertada en una tarjeta y lleva un número de identificación. Este número se asocia a continuación a un usuario en un sistema informático. A la base es una tecnología de Identificación que puede, acoplado a una contraseña proporcionada por el usuario por ejemplo, utilizarse en procedimientos de autenticación. Este sistema se utiliza comúnmente para el control de acceso físico por tarjeta o el pago al restaurante de empresa. La detecta una tarjeta HID a algún centímetro. El RFID activo se basa en los protocolos de comunicación RFID pero asocia a la carta una alimentación propia. Esta alimentación permite una detección de la tarjeta a más largo alcance (por ejemplo a partir de la entrada en una sala o una oficina). El interés principal del RFID activo es permitir un acta de ausencia para los puestos de trabajo en zonas accesibles al público.

Tabla 2.2 Siete elementos de autenticación

Fuente: Evidian (2015)

La autenticación multi-factores

Un factor de autenticación es un elemento que se sabe (código secreto), que se posee (apoyo físico) o que es (biométrica). En cuanto varios factores de autenticación se registran en juego, se habla de autenticación multi-factores.

Sistema de Autenticación	Factores
Ejemplos de 1 factor:	Identificador + contraseña (elemento que se sabe), *ƒ* Definición sin contacto (elemento que se posee), *ƒ* Biométrica o identificador + biométrica (elemento que es).
Ejemplos de 2 factores:	Tarjeta inteligente + código PIN (elementos que se posee Y que se sabe), *ƒ* Tarjeta inteligente + biométrica (elemento que se posee Y que es), Biométrica + contraseña (elemento que es Y que se sabe).
Ejemplo de 3 factores:	Tarjeta inteligente + cifra PIN + biométrica (elementos que se posee Y que se sabe Y que es)

Tabla 2.3 Ejemplos de Autenticación multi-factores

Fuente: Evidian (2015)

La multiplicación del número de factores de autenticación aumenta el nivel de seguridad general, pero plantea los siguientes problemas:

- El ciclo de vida de cada factor debe administrarse: inicialización de las contraseñas y códigos PIN, distribución de las tarjetas inteligentes.
- La ergonomía de utilización puede volverse demasiado pesado para los usuarios.
- Se añaden los costes de los periféricos (tarjetas inteligentes, lectores, sensores biométricos). Además, la carga del servicio de ayuda al usuario va a aumentar para administrar el conjunto de estos métodos (desbloqueo de las contraseñas y códigos PIN, distribución de las tarjetas, formación de los usuarios a la biométrica,…).

Por lo expuesto se debería planificar, el uso de los factores de acuerdo a la necesidad y los recursos.

2.21 CONTROL DE ACCESO BASADO EN ROLES (RBAC)

SG (2009):

Uno de los esquemas más comunes es el control de acceso basado en roles, también conocido como RBAC por sus siglas en inglés (Role Based Access Control).

Un sistema RBAC debe proveer como mínimo tres diferentes grupos de funcionalidad: autenticación, autorización y auditoria.

• Autenticación. Capacidad de validar la identidad de un usuario. Típicamente se realiza por medio de nombres de usuario y contraseña.

• Autorización. Es la definición de qué es lo que un usuario específico puede hacer dentro de una aplicación, es decir a qué información y operaciones tiene acceso.

• Auditoría. Se refiere a la capacidad de mantener un registro de las transacciones sensitivas de una aplicación. La auditoría permite saber quién hizo qué, cuando lo hizo, y quién le dio los permisos necesarios a ese usuario.

Componentes

• Repositorio. Se requiere de un lugar seguro para almacenar los usuarios, contraseñas, roles y permisos.

• Interfaz entre aplicación y repositorio. Este es el componente intermedio que sirve de interfaz entre una aplicación y el repositorio de seguridad.

• Consola de administración. La consola que permite administrar las cuentas de usuario, roles y permisos. Debe ser sencilla de usar, de forma que gente no técnica pueda realizar estas tareas.

• Documentación. Un elemento comúnmente olvidado, que sin embargo es necesario para tener un proceso de seguridad confiable y que no dependa de personas específicas.

Es altamente recomendable que los detalles para el control de acceso a aplicación no estén definidos dentro del código de la aplicación misma, sino que se realicen a través de un componente externo que interactúe con un repositorio de permisos, tal como se indica aquí. Esto permite tener independencia entre el código de la aplicación y el control de acceso, lo cual es deseable ya que así no se necesita modificar la aplicación y lanzar una nueva versión cada que se requiera hacer un cambio en la política de accesos. Otra ventaja es que no se necesita personas que entiendan el código de la aplicación, para poder hacer ajustes en el control de acceso.

El acceso a los recursos es determinado por los roles asignados según el cargo desempeñado dentro de la organización, cada usuario solo debe tener acceso a la información y recursos necesarios para el buen desempeño de las funciones para las cuales fue contratado, de acuerdo con los procesos organizacionales. A esto también se le denomina el menor privilegio, es decir, los usuarios solo tienen acceso a lo que deben tener. Por ejemplo, una persona del área de cobranzas no debe poseer acceso a los salarios de toda la empresa.

Un ejemplo de aplicación puede ser el Rol de RBAC que utiliza Azure (proveedor de servicios de la nube), como se puede ver en el siguiente gráfico.

Rol de RBAC de Azure	Permisos	Notas
Propietario	• Acceso total a todos los recursos • Delegar el acceso a otros usuarios	Al administrador de servicios y a los coadministradores se les asigna el rol de propietario en el ámbito de suscripción. Se aplica a todos los tipos de recursos.
Colaborador	• Crear y administrar todos los tipos de recursos de Azure • No se puede conceder acceso a otros usuarios	Se aplica a todos los tipos de recursos.
Lector	• Ver recursos de Azure	Se aplica a todos los tipos de recursos.
Administrador de acceso de usuario	• Administrar el acceso de usuarios a los recursos de Azure	

Figura 2.14 Rol de RBAC de Azure

Fuente: Microsoft Azure (2019)

RBAC de Azure es un nuevo sistema de autorización que proporciona una administración de acceso detallada a los recursos de Azure (Proveedor de Servicios en la Nube). RBAC incluye muchos roles integrados, puede asignarse en distintos ámbitos y le permite crear sus propios roles personalizados. Para administrar recursos de Azure Active Directory, como usuarios, grupos y dominios, hay varios roles de administrador de Azure AD.

2.22 DIRECTORIO ACTIVO O ACTIVE DIRECTORY

McGraw-Hill y Distriforma. (s.f.):

Es el servicio de directorio de una red con Windows Server. Determina la utilización de recursos de red de forma centralizada.

El Directorio Activo es un servicio de red que guarda en una base de datos toda la información sobre los recursos de la red y permite el acceso de los usuarios a dichos recursos y a determinadas aplicaciones. De esta forma se convierte en un modelo para organizar, controlar y administrar de forma centralizada el acceso a los recursos de la red.

El Directorio Activo es, por lo tanto, una herramienta fundamental de administración de toda la infraestructura informática de una empresa.

Una de las ventajas fundamentales de Directorio Activo es separar la estructura lógica de la organización (dominios) de la estructura física (topología de red).

El Directorio Activo permite a los administradores crear políticas a nivel de empresa, aplicar actualizaciones a una organización completa o desplegar programas en múltiples ordenadores.

La estructura de un Directorio Activo se basa en los siguientes conceptos:

- ✓ Dominio. Estructura fundamental. Permite agrupar todos los objetos que se administran de forma estructural y jerárquica.
- ✓ Unidad organizativa. Es la unidad jerárquica inferior al dominio y que puede estar compuestas por una serie de objetos y por otras Unidades Organizativas. Las unidades organizativas son contenedores del Directorio Activo.
- ✓ Grupos. Conjunto de objetos del mismo tipo que se utilizan fundamentalmente para la signación de derechos de acceso a los recursos. Normalmente son de usuarios.
- ✓ Objetos. Forman una representación de un recurso de red, como pueden ser usuarios, impresoras, ordenadores, unidades de almacenamiento, etc.

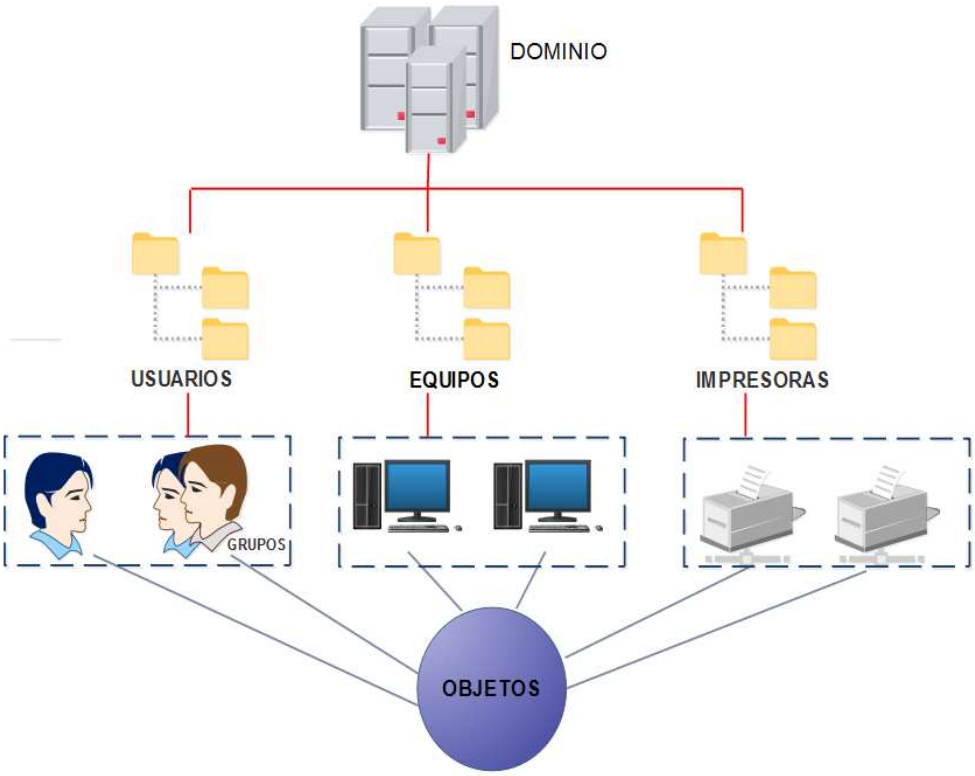


Figura 2.15 Estructura de un Dominio Activo

Fuente: Elaboración propia basado en McGraw-Hill y Distriforma. (s.f.)

2.23 GESTIÓN DE LA RELACIÓN CON EL CLIENTE (CRM)

En Appvizer Revista, 2019 se publicó:

CRM definición: El CRM, Customer Relationship Management o gestión de la relación con el cliente en español (GRC), engloba dos conceptos distintos. Puede tratarse de una estrategia empresarial orientada a satisfacer y fidelizar al cliente o bien de un programa informático, un software, para implementar un sistema de gestión de las relaciones con el cliente. En España, este modo de gestión se conoce por el nombre de marketing relacional. El objetivo principal en ambos casos es establecer una relación de proximidad con el cliente para fidelizarlo.

El sistema CRM se caracteriza por:

Integrar la planificación de las tareas de la empresa y el seguimiento de las ventas.

Permitir la creación de una ficha para cada cliente potencial y seguir el estado de todas las ventas, simplificando la elaboración de los informes de ventas.

En resumen, funciona como una base de datos dinámica que analiza y almacena en tiempo real toda la información relativa a tus clientes.

Estructura de un CRM: ventas, cliente y marketing

Una plataforma CRM está compuesta por varios módulos. Cada uno de estos módulos agrupa varias funciones y herramientas. La organización de un sistema CRM varía en función de las necesidades de cada empresa. Los módulos básicos son: ventas, cliente y marketing.

Módulo de ventas. Está orientado a automatizar las actividades de los comerciales. En este módulo se registran el seguimiento de los clientes potenciales, el flujo de ventas y su estado, así como todas las tareas comerciales.

Módulo de cliente. Permite gestionar de forma eficaz el departamento de atención al cliente y de asistencia. Este incluye toda la información personal y de contacto de cada cliente, así como el historial de incidencias, reclamaciones, registro de compra, entre otros.

Módulo de marketing. Tiene como objetivo analizar toda la información de los módulos anteriores para realizar segmentaciones y campañas de marketing orientadas al desarrollo de la lealtad del cliente en función del comportamiento y las características de los mismos. También facilita el seguimiento de campañas y centraliza todas las tareas y los eventos del departamento de marketing.

Figura 2.16 Definición básica del CRM

Fuente: Appvizer Revista, 2019

Sistema CRM para una empresa

Existen multitud de programas y módulos para implementar un sistema CRM. Pero antes, para que este procedimiento de selección sea eficaz, se recomienda seguir una serie de etapas.

Etapa #1: consiste en realizar un análisis económico inicial de la empresa que incluya un estudio de la situación actual de las relaciones con los clientes, la competencia, la situación de la industria y la gestión de las relaciones con los proveedores.

Etapa #2: se definen los objetivos de negocio. Por lo general, se trata de conseguir nuevos clientes y de fidelizar los existentes.

Etapa #3: se sincronizan los procesos del CRM con la estrategia de mercado de la empresa. Esta etapa permite identificar las actividades más importantes y construir las herramientas necesarias que automatizan las tareas asociadas.

Etapa #4: se diseña o se elige el software empresarial que responde mejor a las necesidades del negocio, identificadas en las etapas anteriores.

Ejemplo de software CRM, existe una gran variedad de software que puede encontrarse, con diferentes características, el que citaremos como ejemplo es Suma CRM que está dirigido a pequeñas y medianas empresas. En el siguiente gráfico se puede observar el software.

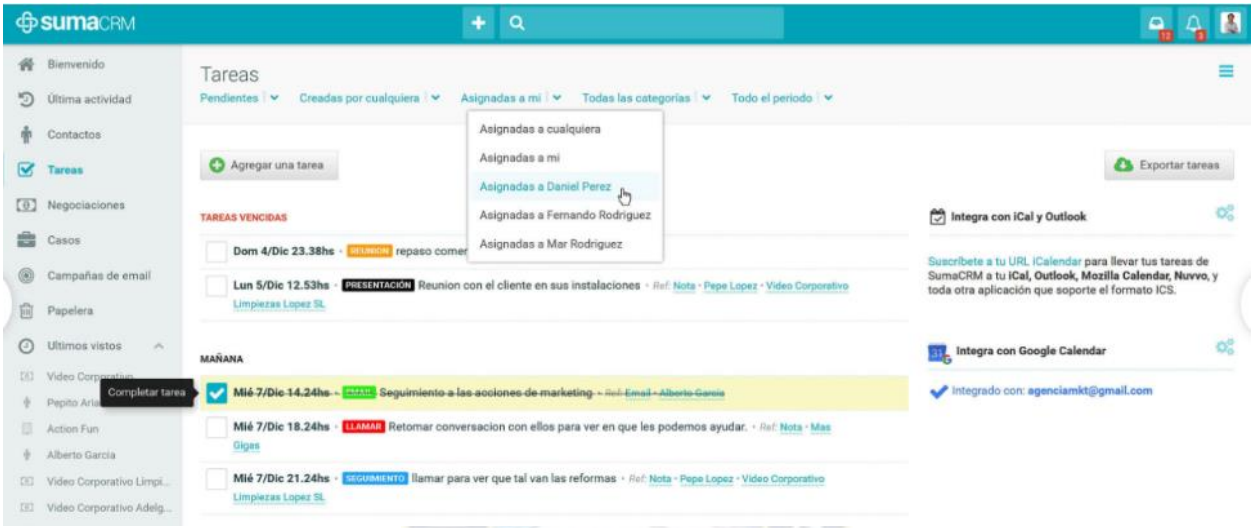


Figura 2.17 Software Suma CRM

Fuente: Appvizer Revista, 2019

En la *Figura 2.17*, se puede observar la opción de Tareas, donde permite asignar tareas, se pueden ver tareas vencidas, tareas programadas para mañana, con el correspondiente detalle, además de la identificación de tareas por colores ejemplo tareas como ser llamadas con color rojo, seguimiento con color celeste y así se puede identificar más fácilmente el tipo de tarea.

Suma CRM también brinda funcionalidades en la gestión de datos de los clientes, seguimiento de ventas, permite importar datos desde Excel, Gmail y Outlook, Sincroniza los correos electrónicos de los clientes con el perfil de los mismos y permite la difusión de campañas de marketing.

CAPITULO 3

3. SEGURIDAD DE LA INFORMACIÓN EN BOLIVIA Y PAÍSES VECINOS

3.1 SEGURIDAD DE LA INFORMACIÓN EN BOLIVIA

La Gestión de Seguridad de la Información no es un tema nuevo, siendo que en los países Europeos como España está bastante desarrollado, y cuenta con leyes, normativas con mucho detalle para cada área relacionada a Tecnologías de la Información.

En Bolivia, el Gobierno ha tomado algunas medidas enfocadas a las TIC, que tienen muchas tareas asignadas entre las cuales se encuentra la Seguridad de la Información. Sin embargo aún no se habla de Gestión en la Seguridad de la Información.

Es así que en septiembre de 2015 se crean dos entidades: la AGETIC (Agencia de Gobierno Electrónico y Tecnologías de la Información y Comunicación) es una entidad pública bajo tuición del Ministerio de la Presidencia y el CTIC - EPB (Consejo para las Tecnologías de Información y Comunicación del Estado Plurinacional de Bolivia).

Una de las tareas del CTIC – EPB es elaborar estándares de seguridad y protocolos de prevención y contingencia de incidentes informáticos que permitan proteger y resguardar los sistemas y la información del Estado. (Consejo para las Tecnologías de Información y Comunicación del Estado Plurinacional de Bolivia s.f.).

En los artículos que han sido consultados, respecto a la Gestión de seguridad de la Información, se ha podido observar que los Países en Sudamérica, están avanzando lento, se incrementó el presupuesto para proyectos de las áreas de seguridad de la información y muchas organizaciones llevan a cabo iniciativas de educación y concientización para su personal. (REALNET, 2016).

Uno de los parámetros que se toma en cuenta es el número de certificados en ISO 27001, Colombia puede ser una de las que más certificaciones posee.

En el desarrollo de la tesis, se ha realizado un análisis con más detalle, respecto a este punto. Ya que la Gestión de Seguridad de la información, ha sido abordada de diferentes formas en cada País, es importante conocer en qué medida se encuentra desarrollado en los países vecinos y estudiar el entorno en el cual se encuentra Bolivia.

A continuación se desarrolla este punto.

3.2 INSTITUCIONES EN BOLIVIA RELACIONADAS CON LA SEGURIDAD DE LA INFORMACIÓN

Tenemos los siguientes Instituciones:

- ADSIB (Agencia para el Desarrollo de la Sociedad de la Información en Bolivia)
- AGETIC (Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación)
- CGII (Centro de Gestión de Incidentes Informáticos)
- COPLUTIC (Comité Plurinacional de Tecnologías de Información y Comunicación)
- COSTETIC (Consejo Sectorial de Telecomunicaciones y Tecnologías de Información y Comunicación)
- ASFI (Autoridad de Supervisión del Sistema Financiero)
- APS (Autoridad de Fiscalización y Control de Pensiones y Seguros)

3.2.1 Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB)

Las funciones de la Red Boliviana de Comunicación de Datos - BOLNET son transferidas a la estructura de la ADSIB (Agencia para el Desarrollo de la Sociedad de la Información en Bolivia) cuya labor es promover la gestión de políticas y estrategias en TIC en áreas como: contribuir a la reducción de la brecha digital mediante el desarrollo de la Sociedad del Conocimiento en Bolivia a través de las Tecnologías de Información y Comunicación en todos sus ámbitos.

ADSIB tiene las funciones de: registrador del dominio de nivel superior geográfico ".bo", emite certificados para firma digital, administra el repositorio Estatal de Software Libre. Brinda la conformidad u oposición para la adquisición o donación, ampliación y/o renovación de Licencias de Software Propietario en entidades públicas y emitir certificados digitales para el Firmante de Documentos – DS, de emisión de pasaporte electrónico como Autoridad Certificadora de Firma de País del Estado Plurinacional de Bolivia. (ADSIB, 2019)

.

3.2.2 Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC)

Decreto Supremo 2514 (2015). En el Decreto Supremo 2514, de 9 de septiembre de 2015, se crea la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación – AGETIC.

Revisando el Decreto Supremo 2514, se pueden extraer los siguientes artículos que hacen referencia a Seguridad de Información:

En el artículo 7 se señala las funciones de la AGETIC, entre las cuales están los incisos "f" y "g", que indican:

f) Establecer los lineamientos técnicos en seguridad de información para las entidades del sector público;

g) Coordinar la gestión de incidentes informáticos con las entidades del sector público;

3.2.3 Centro de Gestión de Incidentes Informáticos (CGII)

En el artículo 8, del Decreto Supremo 2514 (2015), se crea el Centro de Gestión de Incidentes Informáticos – CGII como parte de la estructura técnico operativa de la AGETIC. Entre las funciones del CGII están:

a. Establecer las políticas de gestión de incidentes informáticos gubernamentales y procedimientos para la atención y escalamiento de los mismos;
b. Establecer los lineamientos para la elaboración de Planes Institucionales de Seguridad de la Información de las entidades del sector público;
c. Establecer los lineamientos para la elaboración de Planes de Seguridad de Información de las entidades del sector público;
d. Desarrollar políticas y acciones para la prevención de incidentes informáticos en las entidades del sector público;
e. Desarrollar políticas y acciones para la prevención de incidentes informáticos en las entidades del sector público;

En el artículo 17, sobre obligaciones en materia de seguridad informática indica que:
"Los responsables de seguridad informática de todas las entidades del sector público deberán reportar la ocurrencia de incidentes informáticos que se produzcan en un plazo no mayor a veinticuatro (24) horas de conocido el hecho al CGII, para contener, corregir, recuperar los servicios afectados y/o alertar al resto de las entidades del sector público".

3.2.4 Comité Plurinacional de Tecnologías de Información y Comunicación (COPLUTIC)

Ley No 164 (2011), es la Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación del 8 de agosto de 2011, bajo el artículo 73, se crea el Comité Plurinacional de Tecnologías de Información y Comunicación – COPLUTIC, con la finalidad de proponer políticas y planes nacionales de desarrollo del sector de

tecnologías de información y comunicación, coordinar los proyectos y las líneas de acción entre todos los actores involucrados, definir los mecanismos de ejecución y seguimiento a los resultados.

El Comité Plurinacional de Tecnologías de Información y Comunicación – COPLUTIC, estará integrado por el Ministerio de Obras Públicas, Servicios y Vivienda que lo preside, el Ministerio de Comunicaciones, Ministerio de Educación, Ministerio de Planificación del Desarrollo y la Agencia de Desarrollo para la Sociedad de la Información en Bolivia – ADSIB.

3.2.5 Consejo Sectorial de Telecomunicaciones y Tecnologías de Información y Comunicación (COSTETIC)

Ley No 164 (2011), Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación del 8 de agosto de 2011, bajo el artículo 74, se crea el Consejo Sectorial de Telecomunicaciones y Tecnologías de Información y Comunicación, como instancia consultiva de proposición y concertación entre el nivel central del Estado y los gobiernos autónomos, para la coordinación de asuntos sectoriales.

Reglamento a la Ley Nº 164 (2013), en el artículo 13 inciso romano III indica que COSTETIC, también se enmarca en principios… de la seguridad informática... La soberanía tecnológica del Estado Plurinacional de Bolivia y el uso de estándares abiertos.

Reglamento a la Ley Nº 164 (2013), en el artículo 14, las funciones principales que tiene COSTETIC son: a) Proponer y coordinar mecanismos necesarios para fomentar el acceso, uso y apropiación social de las tecnologías de información y comunicación; b) Coordinar y concertar el despliegue y uso de la infraestructura tecnológica; c) Proponer y concertar servicios y aplicaciones de las tecnologías de información y comunicación en las áreas de educación, salud, gestión gubernamental, en lo productivo, comunicación e información en sus respectivos niveles de gobierno.

3.2.6 Autoridad de Supervisión del Sistema Financiero (ASFI)

El objeto de ASFI es regular, controlar y supervisar los servicios financieros, así como la actividad del mercado de valores, los intermediarios y sus entidades auxiliares. (ASFI, 2019)

La **ASFI** fue creada en el marco de la nueva Constitución Política del Estado mediante Decreto Supremo N° 29894 del 7 de mayo de 2009, en reemplazo de la Superintendencia de Bancos y Entidades Financieras (SBEF), y asumiendo las funciones de supervisión de las entidades que participan en el Mercado de Valores. (Banco Fassil, 2015)

3.2.7 Autoridad de Fiscalización y Control de Pensiones y Seguros (APS)

Es la institución creada para supervisar, fiscalizar, controlar y regular a las personas naturales y jurídicas que desempeñan sus actividades en el ámbito de la Seguridad Social de Largo Plazo y del Mercado de Seguros. (APS, 2019)

3.3 DOCUMENTOS RELACIONADOS CON SEGURIDAD DE LA INFORMACIÓN

Las instituciones ya mencionadas, que tienen entre sus funciones la seguridad de la información, generaron los siguientes documentos:

Plan de implementación de Gobierno Electrónico 2016 – 2025. (Julio, 2016) Documento revisado y corregido por el COPLUTIC (Comité Plurinacional de Tecnologías de la Información y Comunicación).

De la cual extraemos: Línea Estratégica 5. Seguridad Informática y de la Información.
El objetivo de esta línea estratégica es desarrollar capacidades institucionales, normativas y herramientas que permitan accionar operaciones preventivas y reactivas ante la ocurrencia de incidentes informáticos, prácticas orientadas a la seguridad de la información en las entidades públicas y la generación de conocimientos para la reducción de riesgos en incidentes informáticos.

Ante los riesgos y vulnerabilidades a los que se encuentran expuestos los sistemas de información es fundamental generar mecanismos de seguridad que permitan mantener la integridad, disponibilidad y confidencialidad de los servicios y la información en los mismos, estableciendo políticas de gestión y prevención de incidentes informáticos, evaluando la seguridad de los sistemas de información y promoviendo el desarrollo de prácticas de seguridad de la información en las entidades públicas y la sociedad en general. El Centro de gestión de incidentes informáticos – CGII dependiente de la AGETIC está a cargo de elaborar estas políticas.

Adicionalmente, a través del CTIC-EPB, se desarrollarán y adoptarán estándares consensuados en materia de seguridad informática y de la información para las entidades públicas. Finalmente, las entidades públicas elaborarán y presentarán su Plan Institucional de Seguridad de la Información, conforme al Decreto Supremo N° 2514.

Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público (2017)

Este documento ha sido elaborado por los miembros del Consejo para las Tecnologías de Información y Comunicación del Estado Plurinacional de Bolivia (CTIC - EPB) y el Centro de Gestión de Incidentes Informáticos (CGII) año 2017.

Es un documento orientado al sector público, sobre Seguridad de la Información, contiene tres anexos:

- El anexo A, hace referencia al código de prácticas para los controles de seguridad de la información del estándar NB/ISO/IEC 27002
- El anexo B, hace referencia a buenas prácticas de gestión de riesgos del estándar NB/ISO/IEC 27005:2010
- El anexo C está basado en buenas prácticas de gestión de incidentes de la norma ISO/IEC 27035

Todo el documento está basado en la familia de la norma ISO, para dar los lineamientos que se deben seguir en la elaboración del PISI (Planes Institucionales de Seguridad de la Información).

CIRCULARES DE LA ASFI

Las entidades que prestan servicios financieros, son las instituciones con más experiencia en cuanto al tema de seguridad de la información, en Bolivia.

El primer circular que la SBEF emitió en el área de Seguridad de la Información, fue el año 2003, corresponde al circular SB/436/2003 Requisitos Mínimos de Seguridad Informática para la Administración de Sistemas de Información y Tecnologías Relacionadas.

En la Resolución SB Nº 066/2003 del 4 de julio de 2003, en el párrafo cuatro menciona: "… es necesario introducir a las entidades de intermediación financiera y las empresas de servicios auxiliares financieros una cultura de seguridad informática en las transacciones y operaciones que realizan, por lo que es necesario contar con regulaciones prudenciales que establezcan los requisitos mínimos … para administrar los sistemas de información y la tecnología que los soporta … "

La circular SB/436/2003, está dividido en cinco secciones, que se refieren a:

Sección 1: Marco General
Sección 2: Requisitos mínimos de Seguridad Informática
Sección 3: Contrato con proveedores de tecnologías de la información
Sección 4: Transferencias y transacciones electrónicas
Sección 5: Disposiciones transitorias

Estas secciones señalan los aspectos relevantes que deben tomar en cuenta como mínimo, las entidades financieras.

Circular que fue modificada seis veces, a lo largo de estos últimos años, tal como se puede ver en la siguiente tabla.

Circular	Fecha
ASFI / 505 / 2017	04 / 12 / 2017
ASFI / 423 / 2016	30 / 09 / 2016
ASFI / 395 / 2013	14 / 06 / 2016
ASFI / 193 / 2013	16 / 09 / 2013
SB / 466 / 2004	29 / 04 / 2004
SB / 443 / 2003	12 / 08 / 2003
SB / 436 / 2003	04 / 07 / 2003

Tabla 3.1 Control de versiones

Fuente : Circular ASFI/505/2017

Teniendo como referencia, actualmente la circular ASFI 505/2017 “Reglamento para la Gestión de Seguridad de la Información”, emitido el 4 de diciembre de 2017, está circular tiene 14 secciones, las cuales son:

Sección 1: Disposiciones Generales
Sección 2: Planificación Estratégica, estructura y organización de los recursos de Tecnologías de la Información
Sección 3: Administración de la seguridad de la información
Sección 4: Administración del control de accesos
Sección 5: Desarrollo, mantenimiento e implementación de Sistemas de Información
Sección 6: Gestión de Operaciones de Tecnología de Información
Sección 7: Gestión de Seguridad en Redes y Comunicaciones
Sección 8: Gestión de Seguridad en Transferencia y Transacciones Electrónicas
Sección 9: Gestión de Incidentes de Seguridad de la Información
Sección 10: Continuidad del Negocio

Sección 11: Administración de Servicios y Contratos con Terceros Relacionados con Tecnología de la Información.
Sección 12: Rol de la Auditoria Interna
Sección 13: Otras disposiciones
Sección 14: Disposiciones Transitorias

Se puede observar que desde el año 2003 hasta la actualidad, la circular ha tenido un gran cambio, siendo que empezó con cinco secciones, y la última circular ASFI 505/2017 del 4 de diciembre de 2017, Reglamento para la Gestión de Seguridad de la Información, cuenta con catorce secciones, las cuales están fundamentadas en la familia de normas ISO 27000.

ASFI como ente regulador y fiscalizador, ha adoptado normas relacionadas a la Seguridad de la Información, es así que ASFI recibió certificación ISO/IEC 27001:2013 de seguridad de la información (Ministerio de Economía y Finanzas Públicas, Noticias del Ministerio, 14 diciembre 2018), calificación que reconoce la confidencialidad en la información que maneja la entidad pública.

CIRCULARES DE LA APS

En el año 2017 con las circulares APS/DS/JCF/ 153 -2017 dirigido a corredores de Seguros y Reaseguros y APS/DS/JCF 154-2017 dirigido a Entidades Aseguradoras y Reaseguradoras, que trata sobre “Alcance Mínimo para la Realización de Auditorías Externas – Gestión 2017”.

En la circular APS/DS/JCF 154-2017, en el numeral 5 relativo a Tecnología de Información, hace referencia a la Resolución Administrativa APS/DJ/DS/Nº 39/2016 en la cual la firma de auditoria debe evaluar y emitir opinión sobre los controles de los sistemas informáticos y de procesamiento de datos adoptados y/o desarrollados por la Entidad, de acuerdo a la norma NB/ISO/IEC 27001.

La Resolución Administrativa APS/DJ/DS/Nº 39/2016, considera:
Que en la gestión 2007, IBNORCA emite las normas NB/ISO/IEC 27001 y NB/ISO/IEC 27002, donde introduce un nuevo enfoque y define los requisitos mínimos para establecer un sistema de gestión de seguridad de la información, con la finalidad de identificar los requerimientos de seguridad en las instituciones, gestionar los riesgos relacionados a este ámbito, aplicar los controles establecidos y efectuar el mejoramiento continuo de las mismas.

Y en el Artículo 4º Tecnología de la Información indica: “La firma de Auditoria Externa a través de personal calificado, debe evaluar y emitir opinión de acuerdo a la norma NB/ISO/IEC 27001 sobre si los controles de los sistemas informáticos y de procesamiento de datos adoptados y/o desarrollados por la entidad, cumplen mínimamente con los siguientes incisos de la citada norma:”

1. Política de Seguridad
2. Aspectos Organizativos
3. Física y Ambiental
4. Comunicaciones y Operaciones
5. Control Accesos
6. Adquisición, desarrollo y mantenimiento de los sistemas de Información
7. Gestión de Incidentes
8. Gestión Continuidad del Negocio

Si bien, en primera instancia la Resolución Administrativa APS/DJ/DS/Nº 39/2016 está dirigida a entidades Aseguradoras y Reaseguradoras, también se les hizo conocer a las Corredoras de Seguros y Reaseguros.

Con este antecedente es importante que las Corredoras de Seguros y Reaseguros, se preparen para adoptar medidas que puedan conducir al desarrollo de la Gestión en Seguridad de la Información.

Se puede concluir que, en Bolivia, tanto empresas privadas como instituciones públicas, están siendo reguladas en el tema de Seguridad de la Información, por diferentes entes como AGTIC que regula a las instituciones públicas, la ASFI y APS que regulan la actividad financiera y mercado de Seguros respectivamente. También como factor común se puede observar que los documentos que los entes reguladores han publicado referente a Seguridad de la Información están basados en la familia de normas ISO 27000.

En estos últimos tres años la APS ha dado lineamientos sobre seguridad de la información, pero aún no se menciona el tema de Gestión en Seguridad de la Información, el cual se desarrolla en el presente trabajo.

3.4 SEGURIDAD DE LA INFORMACIÓN EN SUDAMÉRICA

En Sudamérica la seguridad de la información está relacionada con varios aspectos, revisando información al respecto se puede mencionar informes sobre la seguridad cibernética, que ha sido desarrollado por la Organización de Estados Americanos y el Banco de Desarrollo Interamericano BID.

Un documento que contiene información relevante en cuanto tema de seguridad de la información, exponiendo datos sobre tecnología, educación y mentalidad sobre seguridad de información.

La expansión de Internet y el uso de las TIC en todas las tareas que normalmente se desarrollan, tienen como desventaja la exposición de la información, que afecta en diferentes medidas al dueño de la información, es difícil pensar en una seguridad al cien por ciento, sin embargo con las buenas prácticas de seguridad se puede hablar de seguridad en el manejo de la información.

Así mismo, en 2016, un informe conjunto de la Organización de los Estados Americanos (OEA) y del Banco Interamericano de Desarrollo (BID) señaló que el cibercrimen le cuesta anualmente al mundo unos 575.000 millones de dólares, es decir,

un 0,5% del PIB global. En el caso concreto de América Latina y el Caribe, la cifra es de unos 90.000 millones anuales (BID y OEA, 2016).

La población en Sudamérica usa más la Tecnología, los gobiernos desarrollan plataformas digitales para brindar servicios y ofrecer accesibilidad a toda la población. El punto débil es que no se han previsto en muchos casos medidas de seguridad del manejo de la información que es un factor común en Sudamérica, no existen programas formales de educación sobre el tema de seguridad, lo que nos hace vulnerables.

En la actualidad se entiende que el delito cibernético no reconoce fronteras nacionales y que se requiere un esfuerzo multilateral y multidimensional para abordar la cantidad de amenazas informáticas.

Mediante programas para países miembros la OEA ha ayudado a elaborar estrategias de seguridad cibernética nacional, ha brindado capacitación a los Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT) nacionales y regionales, ha facilitado ejercicios de gestión de crisis con operadores de la industria nacional crítica y los activos de respuesta a emergencias, la sociedad civil dedicada y el sector privado y ha ayudado a crear conciencia sobre las amenazas y las oportunidades relacionadas con la seguridad cibernética en nuestra región. (BID y OEA, 2016).

La OEA en colaboración con el Banco Interamericano de Desarrollo (BID) y el Centro Global de Seguridad Cibernética de la Universidad de Oxford, el Observatorio de Seguridad Cibernética en América Latina y el Caribe presentan un estudio que tiene como objetivo profundizar en el conocimiento de los riesgos de seguridad cibernética, los retos y oportunidades en América Latina y el Caribe (BID y OEA, 2016).

En base a este estudio es que se recoge información y datos que son útiles para poder analizar la importancia que tiene la seguridad de la información en los países vecinos de Bolivia situados en Sudamérica.

3.5 EQUIPOS DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA (CSIRT)

Muchos países de la región cuentan con instituciones gubernamentales y privadas que han desarrollado documentos relacionados con temas de seguridad de la información, seguridad cibernética y estrategias Nacionales de Ciberseguridad. El nivel de madurez de estos documentos varía de una País a otro e incluso están aún en desarrollo.
Se debe tomar en cuenta que en Sudamérica, Colombia es el primer País en aprobar una Estrategia Nacional de Ciberseguridad en el año 2011. Convirtiéndose en un buen referente para toda la región.

La cooperación entre múltiples interesados es notable en muchos países de América Latina y el Caribe (ALC). Se puede encontrar, por ejemplo, en la creación de Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT), que se han generalizado en toda la región, como se puede ver en el siguiente gráfico.

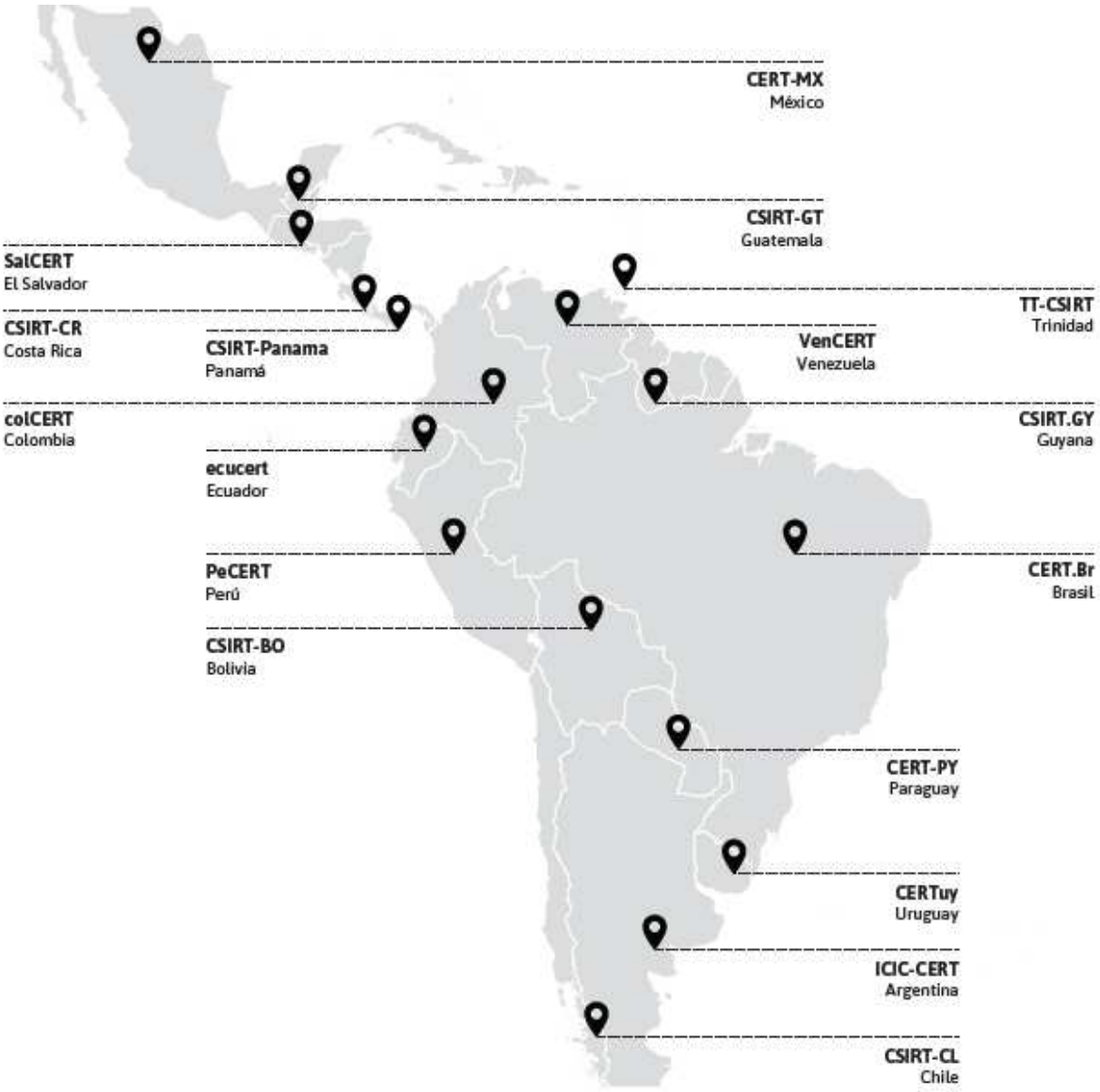


Figura 3.1 CSIRT en América Latina y el Caribe
Fuente: Informe Ciberseguridad 2016 (BID Y OEA)

Al observar en la Figura 3.1 CSIRT-BO, la pregunta es cómo se origino está institución, para lo que se investigó, buscando en la web, se encontró lo siguiente:

En CSIRT Bolivia (2015), indica que: el CSIRT-BO es un Equipo de Respuesta ante Incidentes de Seguridad Informática en el Estado Plurinacional de Bolivia. Su principal objetivo, como CSIRT gubernamental es la prevención, detección y gestión de los

incidentes generados en los sistemas de información de la Administración Pública Nacional y los Entes Públicos. Cuya misión y visión es:

- Prevención, detección y gestión de los incidentes generados en los Sistemas de Información del Estado Plurinacional de Bolivia.
- Asesoramiento, apoyo y formación en materia de seguridad a los diferentes responsables de TIC's en el Estado Plurinacional de Bolivia.
- Proteger y garantizar la seguridad de las entidades gubernamentales.
- Ser un referente en el Manejo de Incidentes y Seguridad Informática.

La naturaleza sin fronteras de Internet aumenta la importancia de la cooperación internacional y la armonización de los marcos legales.

La comunidad CSIRT no puede tener éxito en el aislamiento. Uno de los aspectos interesantes de la región de las Américas es que existen grandes discrepancias en el conocimiento de los asuntos de seguridad cibernética entre los países, tanto en el gobierno como en la población general.

A este respeto la educación tiene un papel muy importante en la enseñanza a los profesionales especializados en seguridad sobre cómo construir tecnologías seguras que sigan estándares nacionales e internacionales.

Se debe entender bien que, al final, cada organización es responsable de su propia seguridad; una institución que regula en el área de tecnología solo puede apoyar en la revisión y recomendación, pero no podrá investigar cada equipo de comunicación o equipo de computación comprometido.

El uso de honeypots para identificar el abuso de la infraestructura de Internet.
El honeypot es similar al llamado contraespionaje de ciberseguridad, que también opta por colocar señuelos de ciberseguridad que, aparentando ser vulnerables, consigan

atraer a los atacantes para engatusarlos y frenar sus ataques a la vez que espían, analizan y monitorizan todos sus movimientos. (Panda, 12 septiembre 2018)

3.6 LEGISLACIÓN SOBRE DELITO CIBERNÉTICO

Es un tema bastante complejo que podría constituirse en un tema de Tesis en el área de Leyes, cada País está independientemente avanzado en este tema, lamentablemente en el caso de Bolivia, no se cuenta aún con leyes específicamente para abordar delitos cibernéticos.

Siendo una buena recomendación de parte de instancias internacionales tomar en cuenta el Convenio de Budapest (Revisar Marco Teórico), que puede servir de lista de verificación para el desarrollo de leyes internas sustantivas y procesales relativas al delito cibernético y la evidencia electrónica.

> Ningún país, grande o pequeño, está inmune a los ataques cibernéticos, que provienen de actores estatales y no estatales en un paisaje tecnológico en constante evolución. (Alexander Seger, 2015)

3.7 ANÁLISIS DE SEGURIDAD CIBERNÉTICA EN PAISES VECINOS

El análisis de seguridad cibernética será útil desde el punto de vista de la Gestión de Seguridad de la Información, dando a conocer los parámetros importantes que determinan el nivel de seguridad de la información de los países vecinos que rodean a Bolivia.

La definición de Seguridad Cibernética conocida también como ciberseguridad es algo difuso, puesto que tiene una definición diferente en diferentes contextos, la definición más acorde con el tema que se emprende se lo encuentra en la Recomendación UIT-T X.1205 Unión Internacional de Telecomunicaciones (UIT) como se describe a continuación.

Ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. El ciberentorno incluye el software que se ejecuta en los dispositivos informáticos, la información almacenada (y transmitida) en estos dispositivos o la información que éstos generan. Las instalaciones y edificios donde residen los dispositivos también forman parte del ciberentorno. (ITU, Ciberseguridad, abril 2008).

Otra definición bastante acertada es:

La seguridad cibernética se enfoca en la búsqueda proactiva y constante, así como en la identificación y entendimiento, de posibles amenazas en los sistemas informáticos capaces de evadir los filtros existentes. Las amenazas pueden provenir de la ingeniería social, los malwares, códigos intrusos que operan sobre bases de datos, vulneraciones derivadas de la pérdida o uso incorrecto de dispositivos y accesos, entre otros.

Requiere la participación de personal capacitado (desarrolladores, analistas, etc.) que domine las tecnologías pertinentes para evitar o contrarrestar los daños. (VISA-Negocios, 2018)

Partiendo de la definición de Seguridad Cibernética, se ha revisado el Informe de Ciberseguridad de 2016, del Observatorio de la Ciberseguridad en América Latina y el Caribe elaborado por el BID (Banco Interamericano de Desarrollo) y la OEA (Organización de Estados Americanos)

Bolivia se encuentra en el centro de Sudamérica, los países vecinos que se tomaron en cuenta para el estudio son: Argentina, Brasil, Chile, Paraguay y Perú, con los que se comparte la frontera, también se hace referencia a Colombia, que es uno de los países con mayor experiencia en temas de Seguridad de la Información.

3.7.1 PENETRACIÓN DE INTERNET

Uno de los aspectos más relevantes y que se puede tomar como un factor común en todos los países es la penetración de Internet, como ya se mencionó para el presente estudio se consideran a los países vecinos: Argentina, Brasil, Chile, Paraguay y Perú, con los que se comparte la frontera, también se hace referencia a Colombia.

Como marco de referencia los siguientes datos expuestos han sido obtenidos del Informe de Ciberseguridad de 2016, elaborado por el BID (Banco Interamericano de Desarrollo) y la OEA (Organización de Estados Americanos), tal como se puede observar en la siguiente tabla:

	Población	Personas con acceso a Internet	Personas sin acceso a Internet	Porcentaje de penetración de Internet
Argentina	42.980.026	27.937.016	15.043.010	65%
Bolivia	10.561.887	4.119.136	6.442.751	39%
Brasil	206.077.898	119.525.181	86.552.717	58%
Chile	17.762.647	12.789.105	4.973.542	72%
Colombia	47.791.393	25.329.438	22.461.955	53%
Paraguay	6.552.518	2.817.583	3.734.935	43%
Perú	30.973.148	12.389.259	18.583.889	40%

Tabla 3.2 Porcentaje de penetración de Internet en Países Vecinos, 2016

Fuente: Elaboración propia con los datos del informe de Ciberseguridad 2016 Del Observatorio de la Ciberseguridad en América Latina y el Caribe

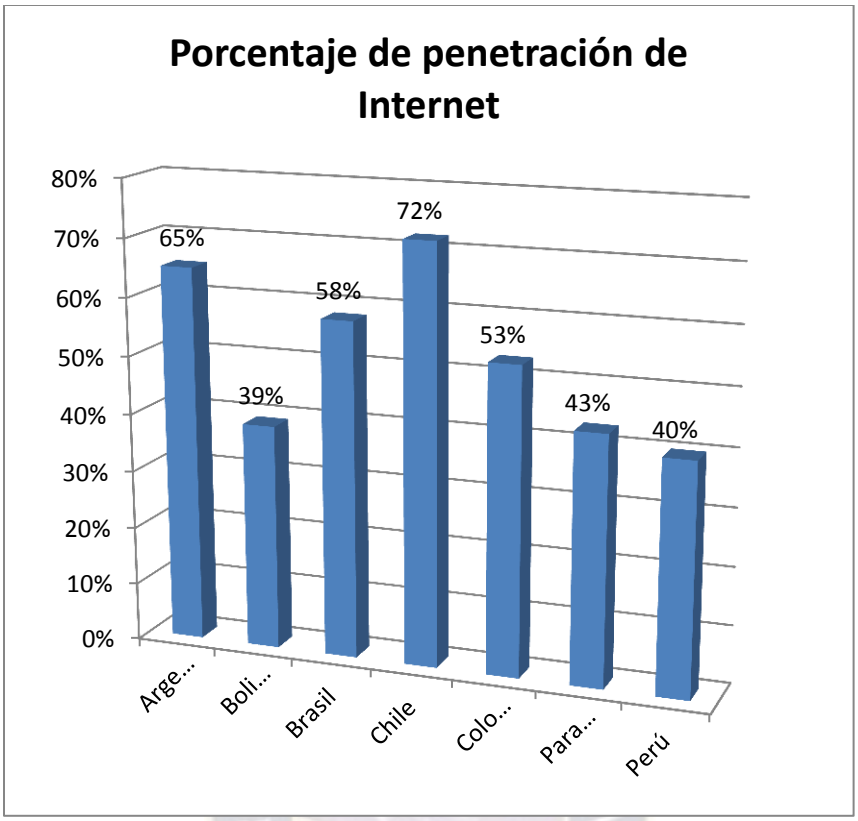


Figura 3.2 Porcentaje de penetración de Internet en Países vecinos al 2016

Fuente: Elaboración propia con los datos del Informe de Ciberseguridad 2016 del Observatorio de la Ciberseguridad en América Latina y el Caribe

Los datos presentados corresponden al año 2016, donde se puede observar que entre los países vecinos, Bolivia tiene el porcentaje más bajo correspondiente a personas con acceso a Internet. Chile tiene el más alto porcentaje de personas con acceso a Internet.

3.7.2 PENETRACIÓN DE INTERNET AL 2019

La penetración de Internet en el año 2019, en los países vecinos, se incrementó, se tienen los resultados en la siguiente tabla y gráfico.

PAÍS	POBLACIÓN ESTIMADA AL 2019	USO DE INTERNET AL 30-06-2019	PORCENTAJE DE PENETRACIÓN
ARGENTINA	44.688.864	41.586.960	93% 65
BOLIVIA	11.215.674	8.817.749	79% 39
BRASIL	210.867.954	149.057.635	71% 58
CHILE	18.197.209	14.108.392	78% 72
COLOMBIA	49.464.683	31.275.567	63% 53
PARAGUAY	6.896.908	6.177.748	90% 43
PERÚ	32.551.815	22.000.000	68% 40

Tabla 3.3 Penetración de Internet en Bolivia y países vecinos al 30 de junio de 2019

Fuente: Elaboración propia con datos obtenidos de Internet World Stats Usage and Population Statistics (18 de noviembre de 2019)

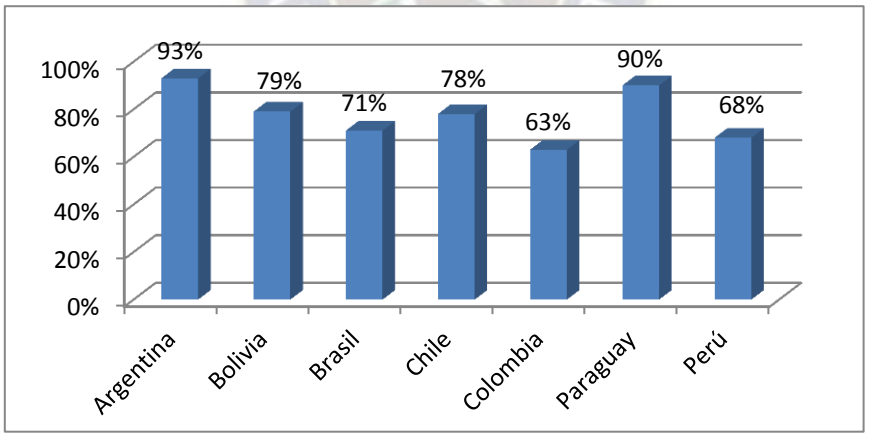


Figura 3.3 Penetración de Internet en países vecinos al 30 de junio de 2019

Fuente: Elaboración propia con datos obtenidos de Internet World Stats Usage and Population Statistics (18 de noviembre de 2019)

Para obtener los datos correspondiente al año 2019, respecto a la penetración de Internet se recurrió a la página web de Internet World Stats, donde se publica las

estadísticas de uso de Internet a nivel Internacional, tomando en cuenta la población total de cada País.

En el caso de Bolivia comparando el año 2016 y el año 2019 se puede observar un gran incremento, en el año 2016 tiene una población de 10.561.887 habitantes y un 39 % de penetración en Internet, en el año 2019 se cuenta con una población estimada de 11.215.674 habitantes y un 79% de penetración en Internet, ubicando a Bolivia en tercer lugar entre los países citados y además se puede observar que es uno de los dos países que más incremento ha tenido con aproximadamente más del 50% de penetración en Internet, en tan solo tres años. Este es un factor común, un indicador útil para comparar a Bolivia con los países vecinos, compartiendo la idea de que "el acceso a internet es fundamental para el desarrollo de un País". Aquí no se entrará en detalles del tipo de tecnología, las velocidades de acceso u otros aspectos, ya que simplemente se observa el crecimiento de la penetración de Internet, como indicador comparativo.

Para corroborar el dato sobre la población se confirmó que el Estado Plurinacional de Bolivia tiene una población aproximada de 11.216.000 habitantes, de los cuales 50,7% es mujer y 49,3%, hombre, según datos procesados por la Encuesta de Hogares (EH) 2017, informó el Instituto Nacional de Estadística (INE, 18 de mayo de 2018)

3.8 INDICADORES EN LA SEGURIDAD DE LA INFORMACIÓN

El análisis de indicadores sobre el tema de seguridad de la información en los países vecinos, está basado en datos que tienen un respaldo reconocido y que tiene las propiedades de un documento formal el cual puede ser revisado en cualquier momento.

Siendo bastante difícil obtener información fehaciente sobre el tema de seguridad de la información que cuente con credibilidad sustentable, se ha visto conveniente y de mucha utilidad el Informe de Ciberseguridad de 2016, del Observatorio de la Ciberseguridad en América Latina y el Caribe elaborado por el BID y la OEA.

Todas las estadísticas que han sido utilizadas para elaborar el Informe de Ciberseguridad de 2016 provienen del banco de datos del Banco Mundial. (Banco Mundial, 2019).

Los datos utilizados en el Informe de Ciberseguridad 2016, se recogieron a través de una encuesta en línea desarrollada en colaboración con el Centro Global de Capacidad sobre Seguridad Cibernética (GCSCC) sobre la base del Modelo de Madurez de Capacidad de Seguridad Cibernética (CMM, por sus siglas en inglés) desarrollado por el GCSCC.

Los datos que se encuentran en el Informe de Ciberseguridad 2016, fueron analizados utilizando los 49 indicadores del CMM, que se dividen entre cinco dimensiones:

1) Políticas y estrategia nacional de seguridad cibernética (“Políticas y estrategia”);
2) Cultura cibernética y sociedad (“Cultura y sociedad”);
3) Educación, formación y competencias en seguridad cibernética (“Educación”);
4) Marco jurídico y reglamentario (“Marco jurídico”);
5) Normas, organizaciones y tecnologías (“Tecnologías”).

Cada dimensión tiene múltiples factores que contribuyen a un estado más maduro de capacidad en materia de seguridad cibernética. Cada factor tiene varios niveles de indicadores (subfactores) que describen un estado de madurez.

Para el cumplimiento de objetivos trazados, en el presente trabajo se revisaron solamente algunas dimensiones y factores que se consideran aportes para un análisis en el área de tecnología, estas dimensiones son:

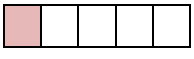
- Cultura cibernética y Sociedad, como factor importante la:
    - Mentalidad de seguridad cibernética: en el gobierno, sector privado y la sociedad.

- Tecnologías, como factores importantes:
    - Adhesión a las normas: Aplicación de las normas y prácticas mínimas aceptables
    - Organización de coordinación de seguridad cibernética: Capacidad de respuesta a incidentes
    - Resiliencia de la infraestructura nacional: Infraestructura tecnológica
    - Respuesta a Incidentes: Identificación y designación, organización y coordinación
    - Gestión de Crisis: planeación y evaluación
    - Redundancia Digital: planeación y organización
- Educación, como factores importantes:
    - Desarrollo Nacional de la Educación de Seguridad Cibernética
    - Gobernanza corporativa, conocimiento y normas: Comprensión de la seguridad cibernética por parte de empresas privadas y estatales

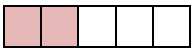
Cada uno de estos factores y subfactores serán expuestos, con los respectivos niveles que presentan, para los países de: Argentina, Bolivia, Brasil, Chile, Colombia, Paraguay y Perú. (Orden alfabético)

3.8.1 INTERPRETACIÓN DE LOS NIVELES DE MADUREZ

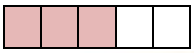
En el informe de Ciberseguridad 2016, se han identificado cinco niveles de madurez de la capacidad de seguridad cibernética, de acuerdo con los cuales el más bajo implica un grado de capacidad inicial, y el nivel más alto es tanto un enfoque estratégico como una capacidad de adaptarse dinámicamente o cambiar por consideraciones ambientales (operativas, amenazas, socio-técnicas y políticas).

Nivel Inicial 

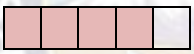
Representado por un cuadrito pintado, este nivel indica que nada existe, o es de naturaleza muy embrionaria. También incluye un pensamiento o una observación acerca de un problema, pero no una acción.

Nivel Formativo 

Representado por dos cuadritos pintados, indica que algunas características han comenzado a crecer y ser formuladas, pero pueden ser casuales, desorganizadas, mal definidas o simplemente “nuevas”.

Nivel Establecido 

Representado por tres cuadritos pintados, que indica que los elementos están establecidos y funcionando. Sin embargo, no se ha considerado bien la asignación relativa de recursos. Ha habido poca toma de decisiones de compensación en relación con la inversión relativa en los distintos elementos del sub-factor. Pero el sub-factor es funcional y está definido.

Nivel Estratégico 

Representado por cuatro cuadritos pintados, donde estratégico no significa importante; más bien, se trata de una selección. A nivel nacional se han elegido las partes del sub-factor que son clave, así como aquellas que son menos importantes para la organización/país en particular. Estas elecciones toman en consideración un resultado esperado, una vez implementado, que contiene circunstancias particulares y otros objetivos nacionales existentes.

Nivel Dinámico 

Representado por los cinco cuadritos pintados. Un nivel dinámico, indica que existen mecanismos claros para alterar la estrategia en función de las circunstancias imperantes. Por ejemplo, la tecnología del entorno de amenazas, conflicto global, un cambio significativo en un área de interés (por ejemplo, la delincuencia cibernética o privacidad). Organizaciones dinámicas han desarrollado métodos para cambiar las estrategias, de acuerdo con una manera de “sentir y responder”. La toma de

decisiones rápida, la reasignación de los recursos y la atención constante a los cambios del entorno son las características de este nivel.

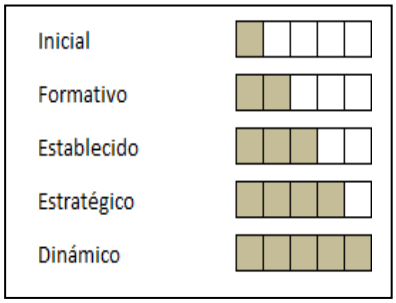
A continuación, se detalla los resultados de nivel de madurez, de los siete países en estudio: Argentina, Bolivia, Brasil, Chile, Colombia, Paraguay y Perú, considerando: Cultura Cibernética y Sociedad, Tecnología y Educación.

3.8.2 MENTALIDAD DE SEGURIDAD CIBERNÉTICA

Es uno de los factores de Cultura Cibernética y Sociedad, siendo que una mentalidad de seguridad cibernética incluye los valores, actitudes y prácticas, hábitos de usuarios individuales, expertos y otros actores en el ecosistema de la seguridad cibernética, incluyendo el gobierno, el sector privado, la academia, los expertos y el comportamiento responsable en línea. Los factores socioeconómicos contribuyen a la existencia de diferentes percepciones de la seguridad cibernética y pueden incidir en el hecho de que la misma se brinde de manera eficaz.

Cultura cibernética y Sociedad
Mentalidad de Seguridad Cibernética

País	Sector	Nivel de Madurez
Argentina	En el Gobierno	
	En el Sector Privado	
	En la Sociedad	
Bolivia	En el Gobierno	
	En el Sector Privado	
	En la Sociedad	
Brasil	En el Gobierno	
	En el Sector Privado	
	En la Sociedad	



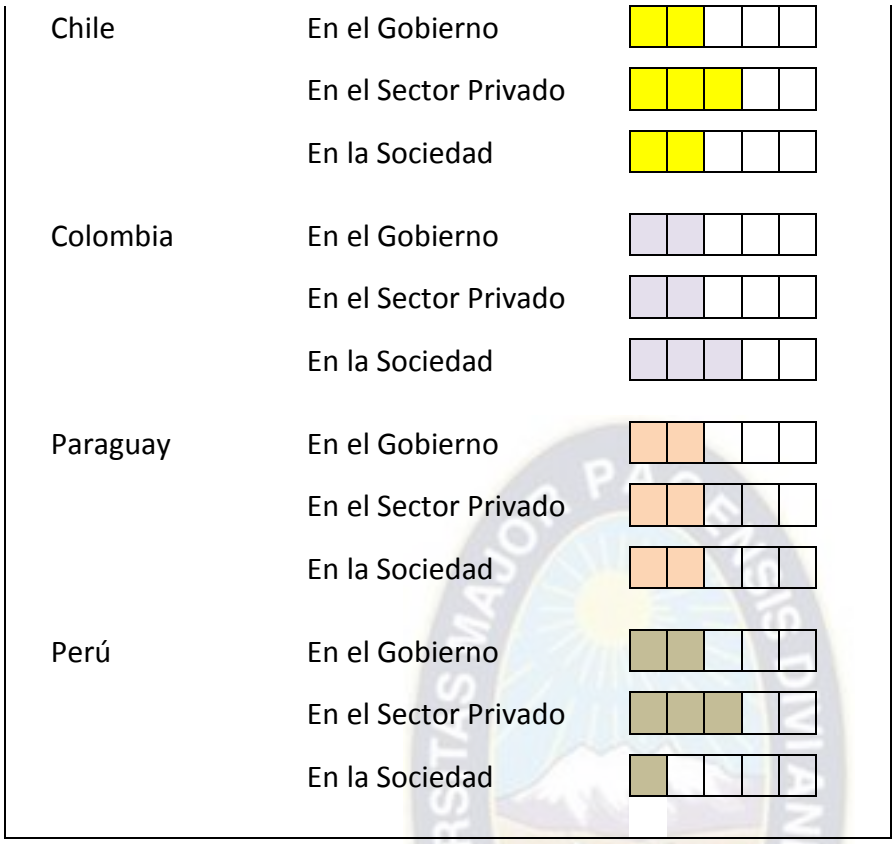


Figura 3.4 Mentalidad de Seguridad Cibernética en Países Vecinos de Bolivia
Fuente: Elaboración propia con datos del Informe de Ciberseguridad 2016 (BID – OEA)

Significado del indicador de la mentalidad de seguridad cibernética en los Gobiernos

En el informe de Ciberseguridad 2016, indica que: "una mentalidad de Seguridad Cibernética toma en cuenta las acciones y las prácticas, hábitos de los usuarios en general". Del cuadro de la *Figura 3.5*, se puede observar que la mentalidad de seguridad cibernética en los gobiernos de Argentina, Bolivia, Brasil, Chile, Colombia, Paraguay y Perú tienen el mismo nivel que corresponde a un nivel de madurez formativo, es decir que los gobiernos han comenzado a darle importancia a la seguridad cibernética, mediante la identificación de los riesgos y amenazas, que están presentes. En este sentido ya existen instituciones gubernamentales que se hacen

cargo de la seguridad de la información, tal como se puede observar en el siguiente cuadro, donde se identifican las instituciones de cada País.

PAÍS	INSTITUCIÓN
Argentina	Ministerio de Seguridad Nacional Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC) Subsecretaría para la Protección de Infraestructura Crítica y Ciberseguridad
Bolivia	Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB) Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGTIC)
Brasil	Agencia Brasileña de Inteligencia (ABIN) Centro de Tecnología e Sociedad (CTS) - Fundação Getúlio Vargas Comité Gestor de Internet en Brasil (CGI.br) Departamento de Seguridad de Información y Comunicaciones, Presidencia de la República de Brasil (DSIC) Equipo Nacional de Respuesta ante Incidentes Informáticos de Brasil (CERT.BR) Gabinete de Seguridad Institucional de la Presidencia de la República (GSI) Instituto de Tecnología e Sociedad (ITS)
Chile	Ministerio del Interior Ministerio de Relaciones Exteriores Ministerio de Telecomunicaciones Comité Interministerial sobre Ciberseguridad
Colombia	Asociación Nacional de Empresarios de Colombia (ANDI) • Cámara Colombiana de Informática y Telecomunicaciones (CCIT) • .CO Internet • Fuerzas Armadas • ISAGEN, EPM • Ministerio de Defensa Nacional • Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) • UniAndes, Escuela Superior de Guerra, Uniminuto, UPB
Paraguay	Secretaría Nacional de Tecnologías de Información y Comunicaciones (SENATICS) Centro de Respuesta ante Incidentes Cibernéticos de Paraguay (CERT – PY)
Perú	Comando Conjunto Fuerzas Armadas Ministerio de Defensa Oficina Nacional de Gobierno Electrónico e Información (ONGEI) Policía Nacional de Perú

Tabla 3.4 Instituciones gubernamentales de países vecinos relacionados con la Seguridad de la Información

Fuente: Elaboración propia con datos del Informe de Ciberseguridad 2016 (BID-OEA)

Significado del indicador de la mentalidad de seguridad cibernética en el sector privado (Ciberseguridad, 2016)

Argentina, Brasil, Chile y Perú tienen un nivel de madurez “Establecido” es decir que en el sector privado tiene una prioridad la seguridad cibernética para lo cual se han generado y establecido los lineamientos a seguir.

Bolivia, Colombia y Paraguay tienen un nivel de madurez “Formativo”, es decir el sector privado ha empezado a darle importancia a la seguridad cibernética.

Significado del indicador de la mentalidad de seguridad cibernética en la Sociedad (Ciberseguridad, 2016)

En Bolivia y Perú, la sociedad presenta un “Nivel inicial”, donde la sociedad desconoce de las amenazas cibernéticas y no puede tomar medidas concretas de seguridad cibernética.

En Argentina, Brasil, Chile y Paraguay se presenta un “Nivel Formativo”, es decir que ya se empieza a tomar conciencia sobre Seguridad cibernética en la sociedad.

En Colombia se presenta un “Nivel Establecido”, es decir la sociedad ya tiene lineamientos y procedimientos a seguir en el manejo de la seguridad cibernética.

3.8.2.1 Análisis del indicador de la mentalidad de seguridad cibernética en Bolivia

El resultado que corresponde a Bolivia, respecto a la mentalidad de seguridad cibernética en:

- El Gobierno presenta un nivel formativo
- Sector Privado presenta un nivel formativo
- Sociedad presenta un nivel Inicial

El nivel inicial indica la inexistencia de mentalidad de seguridad cibernética en la sociedad, indicador que no es de extrañarse. Por tanto se debería dar prioridad al resultado de este indicador, trabajando en programas de información y educación sobre la seguridad cibernética, dirigido a la sociedad en general, ya que la ausencia de conocimiento se convierte en un punto de vulnerabilidad ante las amenazas cibernéticas.

3.8.3 TECNOLOGÍA

Los factores que se han seleccionado, serán útiles para ver aspectos relacionados con temas de seguridad de la información, los cuales son:

- *Adhesión a las normas. Como sub-factor: Aplicación de las normas y prácticas mínimas aceptables.*
  Útil para indicar si se han identificado estándares de seguridad de la información y la gestión de riesgos.

- *Organizaciones de coordinación de seguridad cibernética. Como sub-factor Capacidad de Respuesta a Incidentes.*
  Se determina la existencia y la actividad de los Equipos de Respuesta ante Incidentes de Seguridad Informática (CSIRT, por sus siglas en inglés) y el Centro de Mando y Control en el ámbito nacional, en términos de capacidad de respuesta ante incidentes y mitigación de las amenazas.

- *Resiliencia de la infraestructura tecnológica. Como sub-factor Infraestructura tecnológica.*
  Sub- factor que busca determinar si se han establecido lineamientos de seguridad en las tecnologías de infraestructura a nivel nacional.

- *Respuesta a Incidentes, que se compone de los sub-factores: Identificación y designación, organización y coordinación.*

No todos los incidentes cibernéticos pueden ser mitigados, por lo que la identificación de cuáles de estos eventos constituyen amenazas a nivel nacional puede ayudar a limitar el alcance de la responsabilidad.

- *Gestión de Crisis, que se compone de los sub-factores:* Planeación y Evaluación

  La gestión de crisis es más que la respuesta a incidentes. Ejercicios cibernéticos, por ejemplo, pueden simular una variedad de roles, desde atacantes a defensores, equipos de comunicación, organismos de coordinación y varios otros, todos los cuales son cruciales en caso de una crisis real. La planeación y la evaluación de las aplicaciones de gestión de crisis les ofrecen a los interesados la capacidad para hacerles frente a situaciones del mundo real.

- *Redundancia Digital, que se compone de los sub-factores: planeación y organización*

  En el escenario donde se desactiva la comunicación por medios electrónicos, es fundamental la creación de vínculos de coordinación de respaldo entre los servicios de emergencia que no se basan en redes digitales de comunicación para mejorar la política y la estrategia cibernética.

A continuación en el cuadro, se presentan los niveles de madurez de:

- *Sub-factor: Aplicación de las normas y prácticas mínimas aceptables.*
- *Sub-factor: Capacidad de Respuesta a Incidentes.*
- *Sub-factor: Infraestructura tecnológica.*

País	Sub- Factor	Nivel de Madurez
Argentina	Aplicación de las normas y prácticas mínimas aceptables	
	Capacidad de respuesta a incidentes	
	Infraestructura tecnológica	
Bolivia	Aplicación de las normas y prácticas mínimas aceptables	
	Capacidad de respuesta a incidentes	
	Infraestructura tecnológica	
Brasil	Aplicación de las normas y prácticas mínimas aceptables	
	Capacidad de respuesta a incidentes	
	Infraestructura tecnológica	
Chile	Aplicación de las normas y prácticas mínimas aceptables	
	Capacidad de respuesta a incidentes	
	Infraestructura tecnológica	
Colombia	Aplicación de las normas y prácticas mínimas aceptables	
	Capacidad de respuesta a incidentes	
	Infraestructura tecnológica	
Paraguay	Aplicación de las normas y prácticas mínimas aceptables	
	Capacidad de respuesta a incidentes	
	Infraestructura tecnológica	

Perú	Aplicación de las normas y prácticas mínimas aceptables	
	Capacidad de respuesta a incidentes	
	Infraestructura tecnológica	

Figura 3.5 Indicadores de Tecnología. Parte I

Fuente: Elaboración propia con datos del Informe de Ciberseguridad 2016 (BID-OEA)

Significado de indicadores de Tecnología (Ciberseguridad, 2016)

Significado del Indicador: Aplicación de las normas y prácticas mínimas aceptables. En los siete países de estudio: Argentina, Bolivia, Brasil, Chile, Colombia, Paraguay y Perú se tiene un nivel "Formativo", según el Informe de Ciberseguridad 2016 significa que:

> Se han identificado estándares de seguridad de la información para su uso y ha habido algunos signos iniciales de promoción y adopción del gobierno, sector público y organizaciones de la Infraestructura Crítica Nacional (ICN); hay una aplicación mínima de las normas nacionales e internacionales.

En este sentido y tomando en cuenta que el informe de Ciberseguridad data del año 2016, es importante reconocer las normas de Seguridad de la Información que se han ido adoptando en los países vecinos, que son requeridas para hacer frente a las amenazas cibernéticas existentes, especialmente con el aumento exponencial de penetración de Internet en Sudamérica, en estos últimos cuatro años.

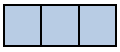
Significado del Indicador: Capacidad de Respuesta a Incidentes, de los siete países en estudio, seis países Argentina, Bolivia, Chile, Colombia, Paraguay y Perú tienen un nivel Formativo, el cual indica la existencia de equipos de respuesta ante incidentes, con responsabilidades definidas. Brasil tiene un nivel Estratégico, el cual indica que existe una colaboración y coordinación de diferentes sectores para responder a los incidentes, existen informes de incidentes e informes de respuesta a incidentes.

Infraestructura Tecnológica, de los siete países en estudio, cuatro países que son: Argentina, Brasil, Chile y Colombia tienen un Nivel establecido, lo que indica que la tecnología desplegada cumple con estándares y buenas prácticas de TI y el servicio de Internet cuenta con procedimientos relacionados a la seguridad de la información. Bolivia, Paraguay y Perú tienen un nivel formativo el que indica que existe la tecnología desplegada pero sin proyecciones y estrategias.

Continuando con los indicadores de Tecnología, se presentan los niveles de madurez correspondientes a los factores de:

- Respuesta a Incidentes
- Gestión de Crisis, es más que la respuesta a incidentes
- Redundancia Digital

País	Factor	Sub - factor	Nivel de Madurez
Argentina	Respuesta a Incidentes	Identificación y designación	
		Organización	
		Coordinación	
	Gestión de Crisis	Planeación	
		Evaluación	
	Redundancia digital	Planeación	
		Organización	
Bolivia	Respuesta a Incidentes	Identificación y designación	
		Organización	
		Coordinación	
	Gestión de Crisis	Planeación	
		Evaluación	
	Redundancia digital	Planeación	
		Organización	

Brasil	Respuesta a Incidentes	Identificación y designación	
		Organización	
		Coordinación	
	Gestión de Crisis	Planeación	
		Evaluación	
	Redundancia digital	Planeación	
		Organización	
Chile	Respuesta a Incidentes	Identificación y designación	
		Organización	
		Coordinación	
	Gestión de Crisis	Planeación	
		Evaluación	
	Redundancia digital	Planeación	
		Organización	
Colombia	Respuesta a Incidentes	Identificación y designación	
		Organización	
		Coordinación	
	Gestión de Crisis	Planeación	
		Evaluación	
	Redundancia digital	Planeación	
		Organización	
Paraguay	Respuesta a Incidentes	Identificación y designación	
		Organización	
		Coordinación	
	Gestión de Crisis	Planeación	
		Evaluación	

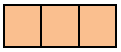
	Redundancia digital	Planeación	
		Organización	
Perú	Respuesta a Incidentes	Identificación y designación	
		Organización	
		Coordinación	
Perú	Gestión de Crisis	Planeación	
		Evaluación	
	Redundancia digital	Planeación	
		Organización	

Figura 3.6 Indicadores de Tecnología. Parte II

Fuente: Elaboración propia con datos del Informe de Ciberseguridad 2016 (BID-OEA)

Significado del indicador: Respuesta a Incidentes

Identificación y designación. Argentina es el único país que tienen un nivel Estratégico lo que indica que se hacen y se priorizan actualizaciones regulares y sistemáticas en el registro de incidentes a nivel nacional. Bolivia tiene un nivel inicial que indica que no se identifican ni catalogan incidentes a nivel nacional. Brasil, Paraguay y Perú tienen un nivel establecido que indica que se establece un registro central de incidentes cibernéticos a nivel nacional. Chile y Colombia presentan un nivel Formativo indica que se han clasificado ciertos eventos cibernéticos o amenazas y se han registrado como incidentes o desafíos a nivel nacional.

Organización. Argentina y Paraguay presentan un nivel Establecido, indica que existe una relación de coordinación rutinaria entre los sectores público y privado para responder a incidentes a nivel nacional con alcance limitado, pero la respuesta sigue siendo reactiva. Bolivia, Chile, Colombia y Perú presentan un nivel Formativo indica que han sido identificadas y contactadas las organizaciones del sector privado que son clave para la seguridad cibernética nacional, sin que haya mecanismos de coordinación

o de intercambio de información con el sector público formal. Brasil es el único País que presenta un nivel Estratégico, respecto al significado en el informe de Ciberseguridad (2016) indica que:

> Se han establecido de manera clara y formal los roles y responsabilidades de seguridad cibernética para el gobierno, la infraestructura crítica, la empresa y los sistemas individuales; los recursos asignados a la respuesta de emergencia son adecuados para enfrentar el entorno de amenazas de seguridad cibernética.

Coordinación. Argentina, Bolivia, Chile, Colombia, Paraguay y Perú presentan un nivel Formativo esto indica que: "se han identificado y publicitado directores de incidentes en cada agencia y ministerio a nivel nacional; los canales de comunicación entre estos directores siguen siendo para una situación concreta e incoherentes". Brasil es el único País que presenta un nivel establecido, indica que: "se ha establecido y publicado una respuesta nacional a incidentes coordinada, con procesos claros, funciones y responsabilidades definidas; se preparan líneas de comunicación para situaciones de crisis".

Significado del indicador: Gestión de Crisis

Planeación. Brasil, Chile, Colombia y Perú presentan un nivel Formativo esto indica que: "se ha llevado a cabo una evaluación preliminar de las necesidades de las medidas que requieren comprobación, con la consideración de un escenario de ejercicio simple, con un tamaño, ámbito geográfico, recursos y coordinación limitados; están incluidos actores clave en el proceso de planeación". Argentina presenta el nivel establecido indica que "un escenario realista de alto nivel informa un plan para poner a prueba los flujos de información y toma de decisiones integral y nueva información alimenta el ejercicio en puntos clave". Paraguay y Bolivia presentan un nivel inicial esto indica que "No hay entendimiento, o es mínimo, de que la gestión de crisis es necesaria para la seguridad nacional; se ha asignado en principio la autoridad de planeación y diseño del ejercicio, pero no se ha esbozado la planeación".

Evaluación. Argentina, Brasil, Chile y Colombia presentan un nivel Formativo indica que "Existe la conciencia general de las técnicas y metas de gestión de crisis; el ejercicio se evalúa y los participantes proporcionan comentarios sobre una situación concreta, pero esto no alimenta la toma de decisiones". Bolivia, Paraguay y Perú presentan el nivel inicial, esto indica que "No se ha realizado ninguna evaluación de los protocolos y procedimientos de gestión de crisis".

Significado del indicador: Redundancia Digital

Planeación. Argentina, Brasil, Chile y Colombia presentan un nivel Formativo indica que "Las partes interesadas se reúnen por medio de asociaciones público-privadas para identificar brechas y superposiciones en las comunicaciones de los activos de respuesta de emergencia y enlaces de autoridad; se establecen prioridades de activos de respuesta de emergencia y procedimientos operativos estándar en el caso de una interrupción de las comunicaciones a lo largo de cualquier nodo de la red de respuesta de emergencia". Bolivia, Paraguay y Perú presentan un nivel inicial indica que: "Pueden considerarse o no medidas de redundancia digital".

Organización. Argentina, Brasil, Chile, Colombia y Perú presentan un nivel formativo, indica que "Los activos de respuesta de emergencia se mapean y se identifican, posiblemente incluyendo detalles sobre su ubicación y sus operadores designados". Bolivia y Paraguay presentan un nivel inicial, indica que: "Los activos de respuesta de emergencia actuales no han sido identificados; si se identifican, carecen de cualquier nivel de integración".

3.8.3.1 Análisis de los indicadores de Tecnología en Bolivia

Según los indicadores expuestos, en Bolivia no se identifican ni catalogan incidentes a nivel nacional, encontrándose en el nivel inicial, que es el más bajo entre los países en estudio. En cuanto a la organización se ha podido observar que el sector privado ha tomado medidas en aspecto de seguridad, sin embargo todavía no hay mecanismos de coordinación con instituciones públicas.

También se ha podido observar que aún, el País no es consciente de que la gestión de crisis es necesaria para la seguridad nacional. Se puede observar que de los siete países citados ninguno tiene el nivel más alto que es el nivel Dinámico.

Si bien Bolivia tiene un nivel inicial, en el que indica que a nivel nacional no existen controles respecto a la seguridad de la información y en algunos aspectos recién se está empezando a generar algunos planes al respecto, se puede observar que en el entorno de los países vecinos tan poco existe un alto nivel de seguridad de la información, que cumpla con los aspectos necesarios para ser considerados como tal. Se puede concluir que a nivel de Sudamérica todavía falta mucho sobre los aspectos de seguridad de la información a nivel general.

3.8.4 EDUCACIÓN

La educación es uno de los factores determinantes en el aspecto de la seguridad de la información, se seleccionaron para analizar cuatro factores que son:

- Disponibilidad Nacional de la Educación y formación Cibernéticas

  Recursos y/o financiación del país destinado a incrementar la disponibilidad de la educación y la formación en seguridad cibernética.

- Desarrollo Nacional de la Educación de Seguridad Cibernética

  Existencia de programas de educación en seguridad cibernética, títulos universitarios y de otro tipo de educación de alta calidad y cursos sobre seguridad cibernética. Creación de centros nacionales e internacionales cibernéticos de excelencia.

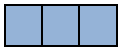
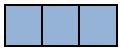
- Formación e iniciativas Educativas públicas y privadas

  Programas destinados a mejorar las habilidades de los empleados para que puedan enfrentar los problemas de seguridad cibernética a medida que ocurren.

- Gobernanza corporativa conocimiento y normas

  Comprensión por parte de las juntas directivas de los riesgos que enfrentan las empresas, algunos de los principales métodos de ataque y cómo su empresa se ocupa de asuntos cibernéticos.

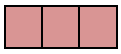
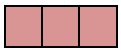
En el siguiente cuadro se puede observar los aspectos señalados para los países de Argentina, Bolivia, Brasil, Chile, Colombia, Paraguay y Perú, con el nivel de madurez correspondiente.

País	Factor	Sub - factor	Nivel de Madurez
Argentina	Disponibilidad Nacional de la Educación y formación Cibernéticas	Educación	
		Formación	
	Desarrollo Nacional de la Educación de Seguridad Cibernética	Desarrollo Nacional de la Educación de Seguridad Cibernética	
	Formación e iniciativas Educativas públicas y privadas	Capacitación de empleados en seguridad cibernética	
	Gobernanza corporativa Conocimiento y normas	Comprensión de la seguridad cibernética por parte de empresas privadas y estatales	
Bolivia	Disponibilidad Nacional de la Educación y formación Cibernéticas	Educación	
		Formación	
	Desarrollo Nacional de la Educación de Seguridad Cibernética	Desarrollo Nacional de la Educación de Seguridad Cibernética	
	Formación e iniciativas Educativas públicas y privadas	Capacitación de empleados en seguridad cibernética	

	Gobernanza corporativa Conocimiento y normas	Comprensión de la seguridad cibernética por parte de empresas privadas y estatales	

Figura 3.7 Indicadores de Educación en seguridad Cibernética. Parte I

Fuente: Elaboración propia con datos del Informe de Ciberseguridad 2016 (BID-OEA)

País	Factor	Sub - factor	Nivel de Madurez
Brasil	Disponibilidad Nacional de la Educación y formación Cibernéticas	Educación	
		Formación	
	Desarrollo Nacional de la Educación de Seguridad Cibernética	Desarrollo Nacional de la Educación de Seguridad Cibernética	
	Formación e iniciativas Educativas públicas y privadas	Capacitación de empleados en seguridad cibernética	
	Gobernanza corporativa Conocimiento y normas	Comprensión de la seguridad cibernética por parte de empresas privadas y estatales	
Chile	Disponibilidad Nacional de la Educación y formación Cibernéticas	Educación	
		Formación	
	Desarrollo Nacional de la Educación de Seguridad Cibernética	Desarrollo Nacional de la Educación de Seguridad Cibernética	
	Formación e iniciativas Educativas públicas y privadas	Capacitación de empleados en seguridad cibernética	

	Gobernanza corporativa Conocimiento y normas	Comprensión de la seguridad cibernética por parte de empresas privadas y Estatales	
Colombia	Disponibilidad Nacional de la Educación y formación Cibernéticas	Educación	
		Formación	
	Desarrollo Nacional de la Educación de Seguridad Cibernética	Desarrollo Nacional de la Educación de Seguridad Cibernética	
	Formación e iniciativas Educativas públicas y privadas	Capacitación de empleados en seguridad cibernética	
	Gobernanza corporativa Conocimiento y normas	Comprensión de la seguridad cibernética por parte de empresas privadas y Estatales	
Paraguay	Disponibilidad Nacional de la Educación y formación Cibernéticas	Educación	
		Formación	
	Desarrollo Nacional de la Educación de Seguridad Cibernética	Desarrollo Nacional de la Educación de Seguridad Cibernética	
	Formación e iniciativas Educativas públicas y privadas	Capacitación de empleados en seguridad cibernética	
	Gobernanza corporativa Conocimiento y normas	Comprensión de la seguridad cibernética por parte de empresas privadas y estatales	

Figura 3.8 Indicadores de Educación en seguridad Cibernética. Parte II

Fuente: Elaboración propia con datos del Informe de Ciberseguridad 2016 (BID-OEA)

País	Factor	Sub - factor	Nivel de Madurez
Perú	Disponibilidad Nacional de la Educación y formación Cibernéticas	Educación	
		Formación	
	Desarrollo Nacional de la Educación de Seguridad Cibernética	Desarrollo Nacional de la Educación de Seguridad Cibernética	
	Formación e iniciativas Educativas públicas y privadas	Capacitación de empleados en seguridad cibernética	
	Gobernanza corporativa Conocimiento y normas	Comprensión de la seguridad cibernética por parte de empresas privadas y Estatales	

Figura 3.9 Indicadores de Educación en seguridad Cibernética. Parte III

Fuente: Elaboración propia con datos del Informe de Ciberseguridad 2016 (BID-OEA)

Significado de los indicadores de Educación en Seguridad Cibernética

Significado del Indicador: Disponibilidad Nacional de la Educación y formación cibernéticas

Educación. Argentina, Brasil y Colombia indican un nivel de madurez establecido, lo que significa que existen ofertas educativas en seguridad cibernética a nivel nacional e institucional.

Bolivia, Chile y Perú indican un nivel de madurez formativo, existe mercado para la educación y la formación en seguridad de la información con evidencia de asimilación; las iniciativas de los profesionales están dirigidas a incrementar el atractivo de las carreras en seguridad cibernética. Paraguay indica un nivel de madurez inicial, significa

que no hay oferta educativa en seguridad de la información, o existe una oferta mínima pero no hay un proveedor reconocido de educación en seguridad cibernética; no existe una acreditación en educación en seguridad cibernética.

Formación. Argentina, Bolivia, Chile, Colombia, Paraguay y Perú indican un nivel de madurez Formativo, es decir existe capacitación en seguridad de la información, pero es sin coordinación; en cuanto a formación, hay disponibles seminarios y recursos en línea para grupos demográficos específicos, pero no existen medidas de efectividad.

Solamente Brasil indica un nivel de madurez establecido que significa que los interesados invierten en capacitación en seguridad cibernética, lo cual no solo es aplicable a roles de TI sino también a roles ejecutivos, de gerencia y a toda una gama de empleados; se entienden bien las necesidades de la sociedad y están documentados los requisitos de formación; se evalúa la eficacia de los modos y procedimientos de formación y se establecen algunas métricas.

Significado del Indicador: Desarrollo nacional de la educación de seguridad cibernética, de los siete países en estudio, cinco países Argentina, Bolivia, Chile, Paraguay y Perú tienen un nivel Inicial lo que indica que no se cuenta con un programa para capacitar a las personas sobre seguridad de la información y las propuestas iniciales sobre el tema están siendo consideradas en diferentes sectores (privados, públicos). Brasil y Colombia tienen un nivel Formativo lo que se puede extraer del Informe de Ciberseguridad de 2016 indica:

> Existen incentivos para la formación y la educación; se identifican líneas presupuestales para la formación y la investigación y el desarrollo, con una oficina establecida para el desarrollo y ejecución del programa; se establece la participación de las partes interesadas para garantizar la continuidad.

Significado del Indicador: Formación e iniciativas Educativas públicas y privadas. Capacitación de empleados en seguridad cibernética

Argentina, Bolivia, Chile, Paraguay y Perú tienen un Nivel Formativo, el significado de este nivel se puede extraer del Informe de Ciberseguridad de 2016 que indica:

> No hay transferencia de conocimientos por parte de los empleados de seguridad cibernética capacitados; debido a una formación limitada, solo hay uso informal de herramientas, modelos o plantillas existentes para la planeación de la seguridad cibernética de la organización, sin la integración automatizada de datos.

Sin la transferencia de conocimientos por parte de los empleados, se hace difícil un seguimiento efectivo en la seguridad de la información.

Brasil y Colombia, tienen un Nivel Establecido, en base al Informe de Seguridad Cibernética de 2016, se puede dar el siguiente significado: “existe transferencia de conocimientos de los empleados de seguridad cibernética formados, se establecen iniciativas de creación de empleo para la seguridad cibernética y esto alienta a los empleadores a capacitar al personal”.

Significado del Indicador: Gobernanza corporativa conocimiento y normas. Comprensión de la Seguridad Cibernética por parte de empresas privadas y estatales, de los siete países en estudio, cuatro países que son: Bolivia, Colombia, Paraguay y Perú tienen un nivel Formativo lo que indica que las empresas tienen algún conocimiento de seguridad, pero no son conscientes de los daños que podrían ocasionar las amenazas y ataques cibernéticos. Argentina, Brasil y Chile tienen un nivel Establecido, lo que indica que las empresas tienen comprensión de los riesgos, ataques que pueden sufrir y además conocen sobre los temas de seguridad de la información.

3.8.4.1 Análisis del indicador de Educación en Seguridad Cibernética en Bolivia

Mediante los indicadores que han sido presentados se puede decir que existe mercado para la educación y la formación en seguridad de la información y se incrementa el interés de las carreras en seguridad, pero la existencia de capacitación en seguridad de la información carece de coordinación; hay disponibles seminarios y recursos en línea para grupos demográficos específicos, pero no existen medidas de efectividad.

En el desarrollo nacional de la educación de seguridad cibernética, al igual que los países vecinos Bolivia se encuentra en un nivel Inicial lo que indica que no se cuenta con un programa para capacitar a las personas sobre seguridad de la información. La capacitación de los empleados en seguridad cibernética no es parte de las funciones de la empresa privada o pública. Las empresas en particular privadas tienen algún conocimiento de seguridad, pero no son conscientes de los daños que podrían ocasionar las amenazas y ataques cibernéticos.

Si bien Bolivia se encuentra con niveles iniciales en cuanto a Educación en seguridad cibernética se puede decir que en el entorno en el cual se encuentra Bolivia, respecto a los países vecinos, todos necesitan trabajar en programas de capacitación sobre seguridad de la información de manera coordinada, las cuales puedan ser accesibles a todas las personas, ya sea a nivel de usuario, a nivel de instructor para formar, a nivel de especialidad para trabajar en instituciones privadas y públicas.

3.9 CERTIFICACIONES ISO EN SUDAMÉRICA

La certificación en ISO 27001 en Sudamérica ha llevado una progresión creciente, en el año 2006 sólo existían 18 certificados, en 2010 ya eran 117 certificados y en el año 2017 la cifra ascendió a 620 certificados. Los países más representativos, en cuanto a número de certificaciones, en Sudamérica pueden ser, Brasil cuenta con 170 certificados, Chile tiene 64 certificados, Colombia cuenta con 163 certificados, Perú cuenta con 43 certificados en ISO 27001 (ISOTools Excellence, 2017).

Todos los años ISO realiza una encuesta de certificaciones realizada, a través de organismos acreditados, de las normas para sistemas de gestión, reportado por cada país. Los últimos datos se encuentran en el documento ISO survey 2018, con el cual realizaremos el análisis de certificados ISO 27001 de los países vecinos en Estudio.

	Total Certificados Válidos
ISO 9001:2015	878.664
ISO 14001:2015	307.059
ISO 22000:2005&2018	32.120
ISO IEC 27001:2013	31.910
ISO 45001:2018	11.952
ISO 13485:2003&2016	19.472
ISO 50001:2011	18.059
ISO 20000-1:2011	5.308
ISO 22301:2012	1.506
ISO 28000:2007	617
ISO 39001:2012	547
ISO 37001:2016	389

Tabla 3.5 Número de Certificaciones ISO a nivel mundial, al 31 de diciembre de 2018

Fuente: The ISO Survey of Management System Standard Certifications 2018 (Septiembre, 2019)

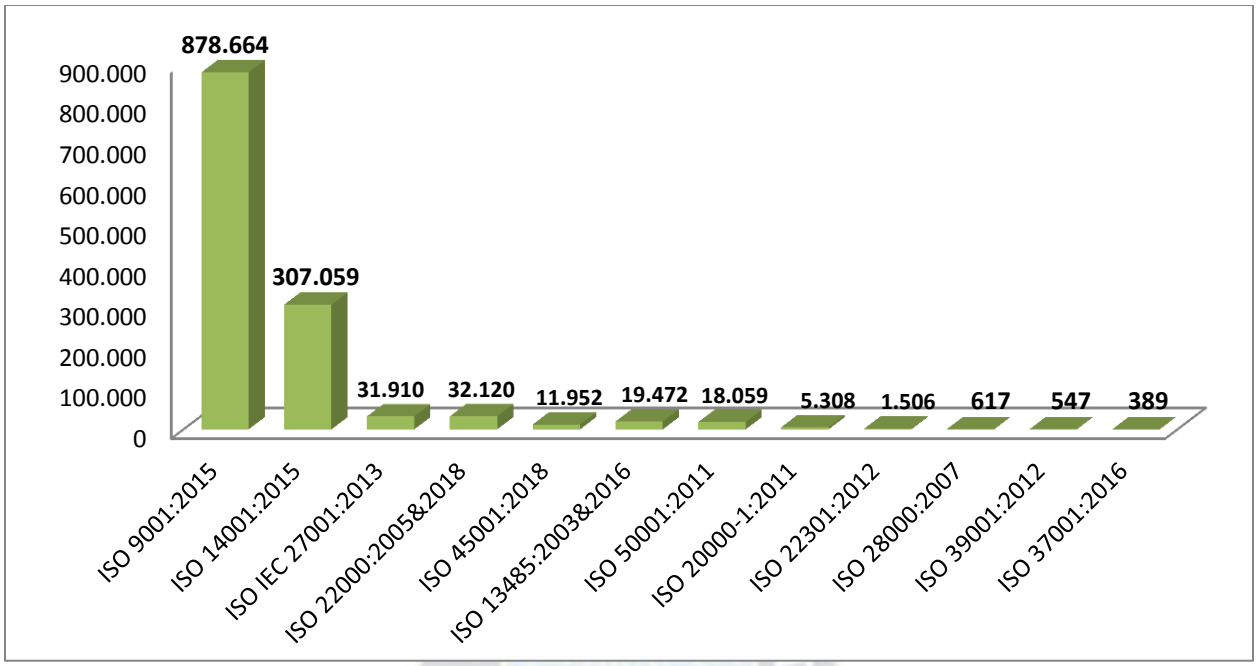


Figura 3.10 Número de Certificaciones ISO a nivel mundial, al 31 de diciembre de 2018

Fuente: Elaboración propia con datos obtenidos de The ISO Survey of Management System Standard Certifications 2018 (Septiembre, 2019)

En la *Figura 3.10* se puede observar que la norma ISO 9001, se encuentra en primer lugar y tiene mucha aceptación a nivel mundial, la norma ISO 27001:2013 se encuentra en cuarto lugar con 31.910 certificados válidos, se debe notar que una vez obtenido el certificado, este tiene una vigencia de dos años, por lo que debe ser renovada cada dos años. Haciendo comparación con otras normas se debe destacar que la ISO 27001, está siendo tomada en cuenta a nivel mundial.

3.9.1 CERTIFICACIONES ISO 27001 EN SUDAMÉRICA

Desde que la norma ISO/IEC 27001 fue publicada en octubre del año 2005, muchos países en todo el Mundo ya en el año 2006 buscaron la certificación, es así que desde ese año empezaron a aumentar exponencialmente el número de certificaciones, como se puede observar en el siguiente gráfico, que corresponde a número de Certificados en ISO 27001 en Países de Sudamérica.

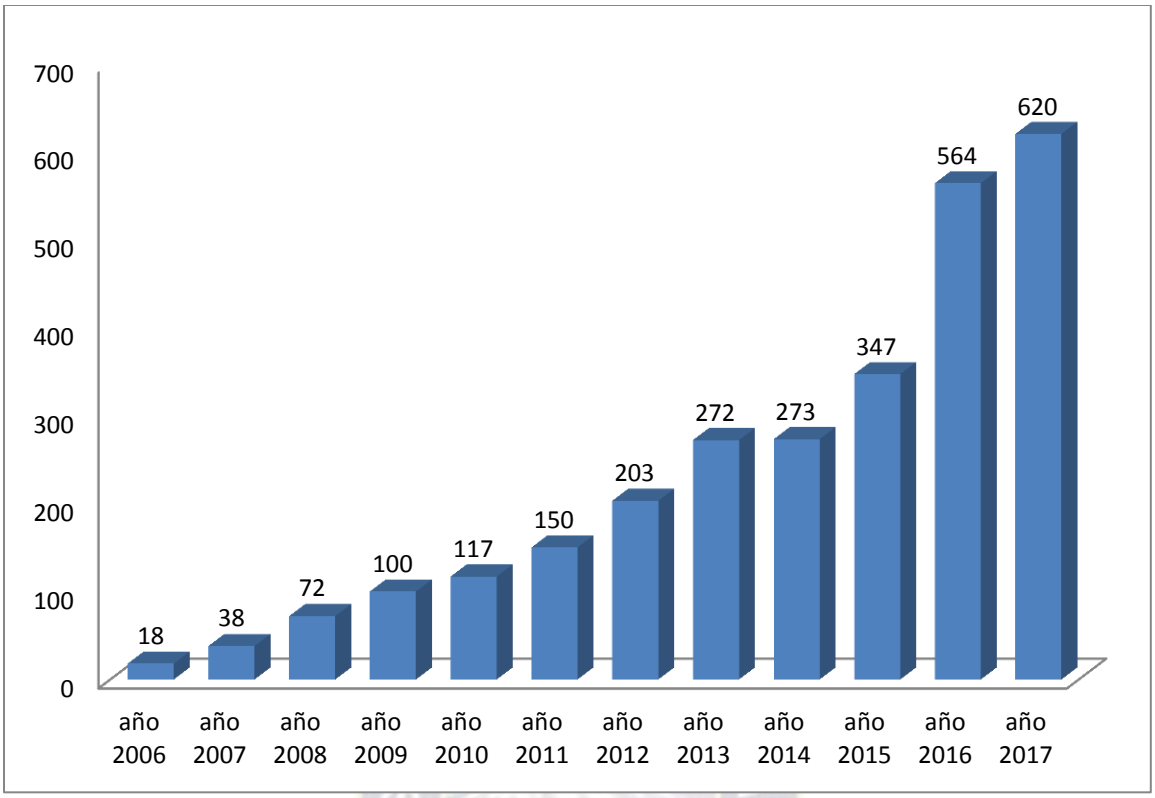


Figura 3.11 Número de Certificaciones ISO 27001 en Sudamérica

Fuente: Elaboración propia con datos de Past Survey 2006 – 2017. (Septiembre 2019)

El crecimiento de certificaciones en ISO 27001, ha aumentado en Sudamérica, desde el año 2006 que se empezó con 18 certificaciones, hasta el año 2017 que se cuenta con 620 certificaciones.

En el siguiente cuadro y gráfico, se muestra los datos de certificaciones ISO 27001: 2013 de los siete países en estudio: Argentina, Bolivia, Brasil, Chile, Colombia, Paraguay y Perú.

AÑO 2017	
País	**Número de Certificados**
Argentina	57
Bolivia	7
Brasil	170
Chile	64
Colombia	148
Paraguay	2
Peru	43

Tabla 3.6 Certificados ISO 27001, correspondiente al año 2017

Fuente: Elaboración propia con datos de ISO/IEC 27001 - Information Technology - Security Techniques - Information Security Management Systems – Requirements Data from 2006 to 2017 (Septiembre, 2019)

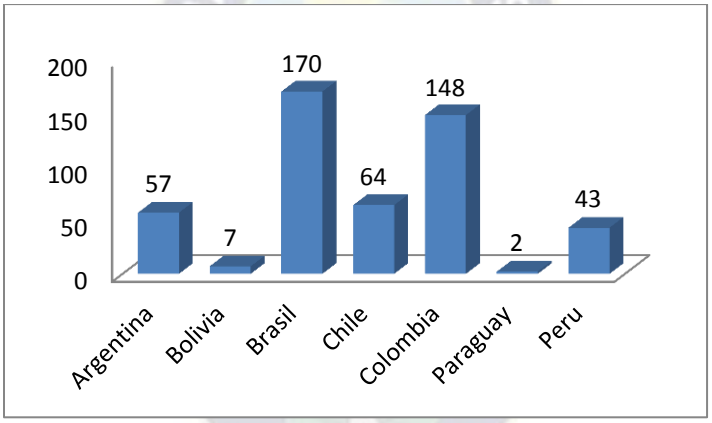


Figura 3.12 Certificados ISO 27001, correspondiente año 2017

Países vecinos en estudio

Fuente: Elaboración propia con datos de Past Surveys 2006 - 2017. ISO/IEC 27001 - Information Technology - Security Techniques - Information Security Management Systems – Requirements Data from 2006 to 2017 (Septiembre, 2019)

En la *Figura 3.12* se puede observar que Brasil y Colombia son los dos países que tienen más certificaciones ISO 27001, lo que demuestra que existe la preocupación por cumplir con parámetros en la seguridad de la Información, para obtener la certificación. Bolivia y Paraguay se encuentran con el menor número de certificados. En el País ya se cuenta con siete certificaciones, que es un indicador para conocer que ya se está iniciando con la obtención de Certificación en ISO 27001.

3.9.2 NORMA ISO EN BOLIVIA

En el siguiente gráfico, se puede observar el porcentaje de certificaciones ISO a nivel general, que se tienen en Bolivia.

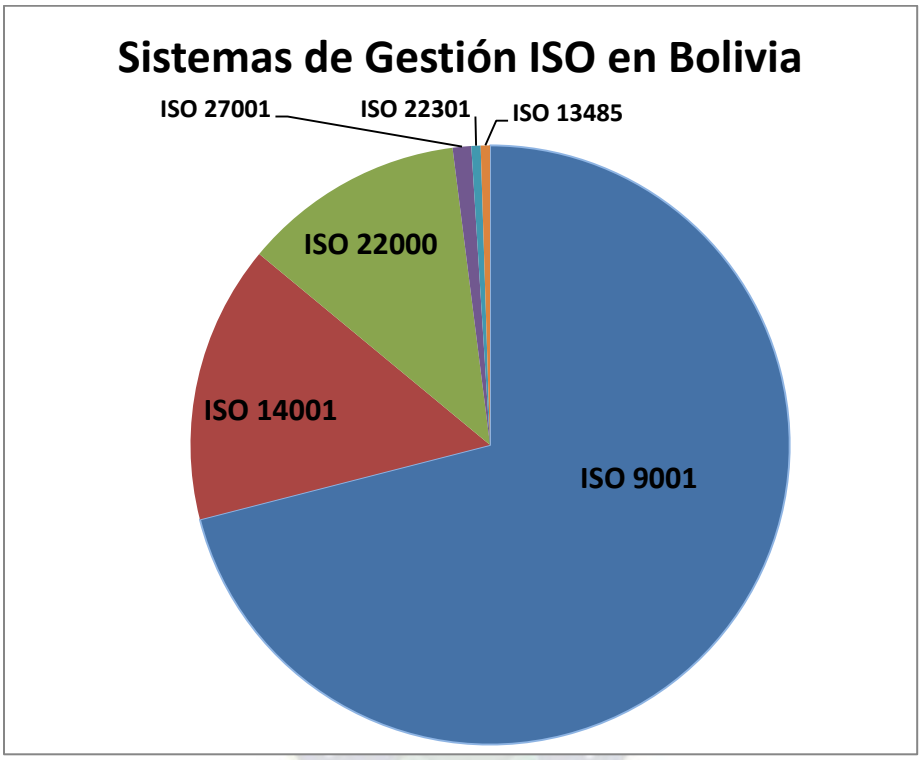


Figura 3.13 Certificaciones de Sistemas de Gestión ISO en Bolivia

Fuente: Elaboración propia con datos de la Publicación de Energy Press Titulada Guía empresas certificadas y acreditadas 2018

La *Figura 3.13*, es útil para esquematizar las normas ISO que se adoptan en Bolivia. La ISO 9001 (Gestión de Calidad) y la ISO 14001 (Gestión de los riesgos medioambientales**)** son las normas de mayor popularidad a nivel internacional y en Bolivia no es la excepción, representando el 71% y 15% del total de certificaciones emitidas en el país. Sin embargo a nivel nacional también ha tomado fuerza la ISO 22000 (Certificación en seguridad alimentaria) que representa el 12 % con 41 certificaciones válidas, el otro 2% está compuesto por la ISO 27001 (Gestión en seguridad de la información), la ISO 22301 (Sistemas de gestión de la continuidad del negocio) y la ISO 13485 (Gestión de Calidad de dispositivos médicos).

Según la publicación de Energy Press, titulada Guía Empresas certificadas y acreditadas 2018, las estadísticas muestran que estamos por debajo de otros países en la adopción de “buenas prácticas de gestión”.

3.9.3 EMPRESAS CERTIFICADAS EN ISO 27001 EN BOLIVIA

Primeramente se realizó la búsqueda de información de Empresas certificadas con ISO 27001 en la página web de IBNORCA, y como resultado solamente se encontró una institución que corresponde al ASFI, los datos que se proporciona son los siguientes:

- ✓ Razón social: Autoridad de Supervisión del Sistema Financiero (ASFI)
- ✓ Nro de Certificado: 2241/1310
- ✓ Certificación: NB/ISO/IEC 27001:2013 ISO/IEC 27001:2013 "Proceso de Supervisión y Control de ASFI que implica el análisis, planificación, inspección, intercambio de información y seguimiento a Entidades Supervisadas por las direcciones de supervisión de riesgos DSR I y II." (IBNORCA)

Autoridad de Supervisión del Sistema Financiero (ASFI). El Instituto Boliviano de Normalización y Calidad (IBNORCA) entregó el 11 de diciembre de 2018, la certificación ISO/IEC 27001:2013 a la Autoridad de Supervisión del Sistema Financiero (ASFI), calificación que reconoce la confidencialidad en la información que maneja la entidad pública. (Ministerio de Economía Finanzas Públicas, diciembre 2018).

Sin embargo en la *Figura 3.13* Bolivia cuenta con siete certificaciones, las cuales fueron obtenidas en el transcurso del año 2006 hasta el año 2017, según los datos de Past Survey página de ISO 27000 basado en encuestas anuales que tienen como propósito averiguar el progreso de sistemas de Gestión a nivel mundial.

Realizando la investigación correspondiente, se encontraron otras empresas bolivianas que han obtenido certificación ISO 27001 en diferentes años y certificados por diferentes organismos, a continuación se citan las empresas:

Minera San Cristobal, en 2010, la empresa fue certificada por la reconocida firma TÜV Rheinland y otorgó a Minera San Cristóbal simultáneamente tres certificaciones con las normas internacionales ISO 9001 a la gestión de calidad de todos los procesos, ISO 14001 a la gestión medioambiental y OHSAS 18001 a la gestión de seguridad y salud ocupacional. Posteriormente, la empresa certificó la norma ISO/IEC 27001 por la seguridad de su información que se constituye en un activo valioso y un elemento clave para su funcionamiento. La certificación es el marco que direcciona los esfuerzos para mantener la confidencialidad, integridad y disponibilidad de la información. (Nueva Economía, La Paz Bolivia, 2013)

Yanapti Corporation, es una empresa que tiene como fin el de brindar apoyo en seguridad informática a entidades públicas y privadas. El año 2014, la empresa se consolidó luego de recibir la certificación internacional ISO 27001 de calidad en seguridad de la información, constituyéndose en la primera en Bolivia que garantiza el servicio de blindaje de la información, entre otros rubros. Es una garantía porque la información es resguardada y certificada a nivel internacional, que fue concedida en Alemania, entonces todo el proceso se rige bajo estándares internacionales pero bajo una entidad alemana. (Página SIETE, *domingo, 16 de febrero de 2014)*

Nuevatel P.C.S. DE BOLIVIA S.A. (VIVA GSM) de Cochabamba, ha sido certificada con la norma ISO 27001 en el área de servicios de procesamientos de información, Internet y soporte técnico que brinda el departamento de TI a Nuevatel P.C.S. de Bolivia y sus clientes. (Lista de empresas certificadas, 2013)

No se ha podido identificar a las otras empresas que tienen una certificación en ISO 27001, puesto que las empresas citadas han sido certificadas por otras empresas, y no se tiene información sobre la renovación de certificados de ISO 27001, que tienen vigencia de dos años una vez que han sido emitidos. Por este motivo no se cuenta con información exacta de estos datos.

Sin embargo es un muy buen dato ya que como referencia la norma ISO 27001 es relativamente nueva que data del año 2005, siendo Bolivia un País que no cuenta con programas de educación en el área de seguridad de la información, es muy positivo dar a conocer que una empresa en el sector de minería como es San Cristobal tenga un compromiso sobre el manejo seguro de la información, así también una empresa privada como es Yanapti, dedicada a la seguridad informática haya obtenido una certificación ISO 27001. Nuevatel una empresa de telecomunicaciones demuestra su compromiso sobre la importancia del manejo seguro de la información al haber obtenido una certificación ISO 27001. Y por último ASFI que es una institución que regula el sector financiero logra obtener su certificación en ISO 27001.

Por lo expuesto se concluye que las empresas en Bolivia no son ajenas al cumplimiento de normas internacionales como lo es ISO 27001, aunque se trate de una minoría, se puede decir que se está empezando con buenas prácticas en Seguridad de la Información.

CAPITULO 4

4. CONTROLES DE SEGURIDAD DE INFORMACIÓN, QUE APLICAN LAS EMPRESAS CORREDORES DE SEGUROS Y REASEGUROS

Identificación mediante la investigación los controles de seguridad de Información, que aplican las empresas Corredores de Seguros y Reaseguros

A través de un cuestionario, mediante la entrevista, a las empresas corredoras de Seguros y Reaseguros, se indaga sobre los controles de seguridad de la información que son aplicados actualmente, para lo cual se ha tomado en cuenta los controles que están detallados en el Anexo A de la norma NB/ISO/IEC 27001, que están alineados con los enumerados en ISO/IEC 27002.

Controles de la norma NB/ISO/IEC 27002. Los controles son los siguientes:

1. Políticas de Seguridad de la Información
2. Organización de la Seguridad de la Información
3. Seguridad ligada a los recursos humanos
4. Administración de activos
5. Control de acceso
6. Criptografía
7. Seguridad física y del ambiente
8. Seguridad de las operaciones
9. Seguridad de las Comunicaciones
10. Adquisición, desarrollo y mantenimiento del sistema
11. Relaciones con el proveedor
12. Administración de incidentes de seguridad de la información
13. Aspectos de seguridad de la información en la gestión de continuidad del negocio
14. Cumplimiento

Cada uno de los controles citados, tiene su correspondencia de preguntas, los cuales están interpretados en un cuestionario que se encuentra en el Anexo A.

4.1 CORREDORES DE SEGUROS Y REASEGUROS EN BOLIVIA

Para el presente estudio, se tomaron en cuenta las empresas que están reguladas por la Autoridad de Fiscalización y Control de Pensiones y Seguros – APS, es así que se cuentan con (APS, 2019):

- 6 Corredores de Reaseguros
- 33 Corredores de Seguros

El detalle se encuentra en la siguiente tabla, el orden en el que se encuentran es alfabético.

Corredores de Reaseguros

	CORREDORES DE REASEGUROS	UBICACIÓN
1	Acces Re Corredora de Reaseguros S.A.	La Paz
2	Conesa Kieffer & Asociados Corredores de Reaseguros S.A.	La Paz
3	Iberam Re Corredores Internacionales de Reaseguros S.A.	La Paz
4	Olsa Bolivia Corredores de Reaseguros S.A.	Santa Cruz
5	Risk Reinsurance Broker S.A "Risk RE S.A."	La Paz
6	Universal Brokers RE S.A. Corredores de Reaseguros "UNIBROSA RE S.A."	La Paz

Tabla 4.1 Corredores de Reaseguros en Bolivia

Fuente: Elaboración propia, con datos de la APS (APS, 2019)

Corredores de Seguros

	CORREDORES DE SEGUROS	UBICACIÓN
1	A.E.C. Fides Brokers Ltda. Asesores, Corredores de Seguros	Santa Cruz sucursal Cochabamba
2	AON Bolivia S.A. Corredores de Seguros	La Paz
3	ASESCOR S.R.L.. Corredores de Seguros	Santa Cruz sucursal La Paz y Cochabamba
4	BCS Brokers Corporativos de Seguros S.R.L.	La Paz, sucursales El Alto, Santa Cruz, Cochabamba, Tarija
5	Cabezas S.R.L. Corredores y Asesores de Seguros.	La Paz
6	Consegur S.R.L. Corredores y Asesores de Seguros	La Paz, sucursales Cochabamba y Santa Cruz
7	Consejeros y Corredores de Seguros Bolivia S.R.L.	Santa Cruz Sucursal La Paz
8	Consultores de Seguros S.A.	La Paz, sucursales Cochabamba, Oruro, Santa Cruz, Sucre y Tarija
9	Corredora Boliviana de Seguros Ltda. Asesores en Seguros	Cochabamba, sucursales Santa Cruz y Sucre
10	Corredora de Seguros G & G Ltda.	Santa Cruz
11	Corredora de Seguros S.R.L. (CONSESO Ltda.)	Cochabamba, sucursales La Paz, El Alto, Oruro, Potosi, Santa Cruz, Sucre, Tarija, Yacuiba y Trinidad
12	Corredores Seguros Ecofuturo S.A.	La Paz
13	CORRESUR S.R.L. Corredores y Asesores de Seguros	La Paz, sucursales Cochabamba, Santa Cruz, Sucre, Tarija.
14	CUBRE SRL Corredores y Asesores de	La Paz, sucursal Santa Cruz

	Seguros	
15	Delta Brokers Insurance S.A. Corredores de Seguros	La Paz
16	Estrategica S.R.L. Corredores y Asesores de Seguros y Riesgos	Santa Cruz, sucursal La Paz y Cochabamba
17	Génesis Brokers Ltda. Corredora de Seguros	Santa Cruz, sucursales La Paz y Cochabamba
18	H.K.A. Corredores y Asesores de Seguros S.R.L.	Santa Cruz, sucursal Sucre
19	HP Brokers Corredores y Asesores de Seguros S.R.L.	Santa Cruz
20	IBA Corredores y Asesores de Seguros S.R.L.	La Paz
21	Intermed Brokers S.R.L. Corredores y Asesores de Seguros	Santa Cruz
22	International Insurance Brokers S.R.L. Asesores y Corredores de Seguros	La Paz
23	Interseguros S.A. Corredores y Asesores	La Paz, sucursales Cochabamba y Santa Cruz
24	Justa S.R.L. Corredores de Seguros	Santa Cruz
25	Kieffer & Asociados S.A. Corredores de Seguros	La Paz, sucursales Cochabamba, Santa Cruz y Tarija.
26	Patria S.A Corredores y Asesores de Seguros	Santa Cruz, sucursales La Paz y Sucre
27	PREVICOR Corredores y Asesores de Seguros S.R.L.	La Paz, sucursales Cochabamba, Potosi, Santa Cruz y Sucre
28	Puerto Seguro Corredores y Asesores de Seguros S.R.L.	Santa Cruz
29	Royal Brokers S.R.L. Corredores de	Santa Cruz

	Seguros	
30	Saavedra Pacheco Corredores de Seguros S.R.L.	La Paz, sucursal Cochabamba
31	Sudamericana S.R.L. Corredores y Asesores de Seguros	La Paz, sucursales Cochabamba, Santa Cruz y Tarija
32	TOCARSBROKERS S.R.L.	La Paz
33	Universal Brokers S.A.Corredores y Consultores de Seguros	La Paz, sucursales Beni, Trinidad, Cochabamba, Oruro, Potosi, Santa Cruz, Sucre y Tarija

Tabla 4.2 Corredores de Seguros en Bolivia

Fuente: Elaboración propia, con datos de la APS (APS, 2019)

Nota. En el presente estudio, no se consideró las corredoras extranjeras de Reaseguros.

En la siguiente tabla se encuentra un detalle de empresas corredores de seguros y reaseguros según su ubicación, por departamento, siendo un factor importante los que se encuentran en el departamento de La Paz. En el departamento de La Paz, se tiene la presencia de 5 Corredores de Reaseguros y 18 Corredores de Seguros, haciendo un total de 23.

	Corredoras de Reaseguros	**Corredora de seguros**	**Total**
Otros departamentos (Oficinas principales)	1	15	16
Departamento de La Paz (oficinas principales)	5	18	23
TOTAL	6	33	39

Tabla 4.3 Corredores de Seguros y Reaseguros en el departamento de La Paz

Fuente: Elaboración propia

Visite algunas empresas corredoras, que tienen sucursal en la ciudad de La Paz, cuya oficina central está en otro departamento y me entreviste con los gerentes de sucursales que me facilitaron los contactos con personal del área de TI, que se encontraban en otro departamento. Sin embargo, está comunicación no dio los resultados esperados ya que se requería de todo un procedimiento formal para que se pueda obtener la información necesaria. Por dicho motivo solo se tomaron en cuenta las corredoras que tienen oficinas principales en la ciudad de La Paz.

Para el desarrollo del trabajo se consideró 23 corredores de seguros con oficinas principales en la ciudad de La Paz.

Las empresas que han sido visitadas en el departamento de La Paz, son 20 de los cuales 4 son corredores de reaseguros y 16 son corredores de seguros.

	Visitadas en el departamento de La Paz	**Existentes en el departamento de La Paz**
Corredores de reaseguros	4	5
Corredores de seguros	16	18
Total	20	23

Tabla 4.4 Detalle de empresas Corredoras visitadas

Fuente: Elaboración propia

Tres empresas corredoras hasta la fecha actual en que se realiza el presente documento, no pudieron ser contactadas. En la tabla tenemos total 20 empresas que han sido visitadas de un total de 23 que se encuentran en el departamento de La Paz, lo que representa el 87 % del total de empresas corredoras de seguros y reaseguros.

En la visita realizada a las empresas se ha podido observar, que es un aspecto a considerar la existencia de personal de T.I. (área de sistemas o encargado de sistemas), como parte de la empresa, dicha característica será importante en el análisis de resultados del cuestionario. En la siguiente tabla se tiene el detalle.

	Corredora de Reaseguros	Corredoras de Seguros	Total
Con personal de T.I.	3	7	10
Personal de T.I. externo	1	9	10
Total	4	16	20

Tabla 4.5 Detalle de existencia de personal de T.I.

Fuente: Elaboración propia

Las empresas que cuentan con personal de T.I. externo, cuentan con soporte técnico tercializado, es decir una empresa o persona externa brinda el soporte. En algunos casos se cuenta con dos empresas externas, una empresa que brinda soporte al software, relacionado con el sistema de producción y otra empresa que se encarga del soporte de Hardware es decir soporte técnico de equipos de computación e impresoras.

4.2 DETALLE DE RESULTADOS DEL CUESTIONARIO

Para la elaboración del cuestionario se revisó con detalle los controles de la norma ISO 27002, obteniendo preguntas que pueden ser aplicables al entorno en estudio. El cuestionario consta de 61 preguntas, separadas por los catorce controles de la norma ISO 27002.

Se utilizó como instrumento de medición, el cuestionario mediante entrevista personal, de acuerdo a la revisión que se hizo respecto a la Metodología de la Investigación, se pueden extraer las siguientes citas, que fueron referenciales para utilizar el cuestionario.

Un instrumento de medición adecuado es aquel que registra datos observables que representan verdaderamente los conceptos o las variables que el investigador tiene en mente (Grinnell, Williams y Unrau, 2009, citado por Hernández, Fernández y Baptista, 2014)

(Bostwick y Kyte, 2005, citado por Hernández, et al. 2014) lo señalan de la siguiente forma: la función de la medición es establecer una correspondencia entre el “mundo real” y el “mundo conceptual”. El primero provee evidencia empírica, el segundo proporciona modelos teóricos para encontrar sentido a ese segmento del mundo real que estamos tratando de describir.

Un cuestionario consiste en un conjunto de preguntas respecto de una o más variables a medir (Chasteauneuf, 2009 citado por Hernández et al. 2014)

El cuestionario por entrevista personal es el que consigue un mayor porcentaje de respuestas a las preguntas, su estimación es de 80 a 85% (León y Montero, 2003 citado por Hernández et al. 2014, pag. 234).

En base a lo expuesto es que el cuestionario elaborado es cerrado dicotómico, ya que las opciones de respuesta han sido delimitadas, con el objeto de realizar una codificación y un análisis sencillo. Lo cual también permite un menor tiempo del llenado del cuestionario de parte del encuestado.

Codificación. Codificar los datos significa asignarles un valor numérico o símbolo que los represente. Es decir, a las categorías (opciones de respuesta o valores) de cada ítem o variable se les asignan valores numéricos o signos que tienen un significado. (Hernández et al. 2014).

Las preguntas fueron codificadas, asignándole un valor numérico a las respuestas, por la respuesta SI se le asigna el valor de “1”, por la respuesta NO se le asigna el valor de “0”. Como se puede observar en la siguiente pregunta:

Existe alguna política o procedimiento sobre el manejo de medios extraíbles (Discos duros externos, DVDs, memorias USB y otros) SI [1] NO [0]

Como ya se mencionó en las visitas a las diferentes empresas corredoras, se encontraron dos casos: empresas corredoras que cuentan con personal de tecnologías de información y empresas corredoras que cuentan con personal de tecnologías de información de manera externa.

En el primer caso, se solicitó por escrito a la Gerencia, una entrevista con el personal de T.I., para que pueda responder el cuestionario. Explicando que dicho cuestionario tiene fines académicos, y que las respuestas serán absolutamente confidenciales, solamente utilizadas para obtener datos estadísticos.

En el segundo caso, las personas que respondieron el cuestionario fueron los gerentes, quienes tienen el contacto directo con los proveedores externos, en relación con servicios de soporte de hardware y software.

El cuestionario fue aplicado mediante entrevista personal, el tiempo promedio para responder fue de 20 a 30 minutos. En algunos casos el tiempo se extendió ya que el encuestado explico algunas de sus respuestas, las cuales fueron registradas.

Los resultados del cuestionario están relacionados con las siguientes consideraciones:

Cabe señalar que dos Empresas cuentan con certificación de Gestión de Calidad ISO 9001, lo que les ha permitido generar documentación de procedimientos y procesos en todas las unidades que conforman la empresa, por lo cual el departamento o unidad de T.I. ha generado documentación.

Entre las empresas corredoras de Seguros y Reaseguros se tiene una gran diferencia, ya que algunas empresas se componen de cinco personas y algunas empresas se componen de hasta 120 personas, incluido sucursales.

4.2.1 Primer control. Políticas de seguridad de la Información

El documento de políticas de seguridad de la Información está vinculado con los otros parámetros de control, por lo cual, para una mejor comprensión del entrevistado, las preguntas relacionadas a políticas de seguridad de la información, se introdujeron como parte de las preguntas relacionadas con los controles correspondientes.

La primera pregunta, fue un filtro cuya respuesta determino el análisis para las otras preguntas relacionadas.

PREGUNTA	RESPUESTA
Existe un documento llamado políticas de Seguridad de la Información?	SI NO

Tabla 4.6 Primera pregunta del cuestionario

Para considerar a un documento como Políticas de Seguridad de la Información, se tomaron en cuenta las siguientes preguntas:

PREGUNTA	RESPUESTA
Existe alguna política o procedimiento sobre el manejo de medios extraíbles (Discos duros externos, DVDs, memorias USB y otros)	SI ☐ Valor 1 NO ☐ Valor 0
Se tiene alguna política del manejo de la información confidencial en los equipos de computación, cuando se realiza el mantenimiento?	SI ☐ Valor 1 NO ☐ Valor 0
Existe alguna política, sobre el uso aceptable de las instalaciones de comunicación?	SI ☐ Valor 1 NO ☐ Valor 0
Se cuenta con algún documento o política sobre el uso de la mensajería, redes sociales?	SI ☐ Valor 1 NO ☐ Valor 0
Existe alguna política sobre manejo de información confidencial?	SI ☐ Valor 1 NO ☐ Valor 0
Existe una política sobre el acceso de los proveedores a la información de la empresa?	SI ☐ Valor 1 NO ☐ Valor 0
Existe una política sobre la privacidad y protección de la información personal identificable?	SI ☐ Valor 1 NO ☐ Valor 0

Tabla 4.7 Preguntas relacionadas con el documento Políticas de Seguridad de la Información

Fuente: Elaboración propia

La puntuación se considera según el número de afirmaciones, es así que la puntuación mínima es cero y la máxima será de siete (1+1+1+1+1+1+1) ya que existen siete preguntas con afirmaciones.

De acuerdo a los resultados se considera la siguiente distribución:

Rango de puntuación (Cantidad de afirmaciones)	**Apreciación (documento de políticas de Seguridad de la Información)**
De 0 a 3	No se Considera
De 4 a 7	Se Considera

Tabla 4.8 Detalle de puntuación relacionado al primer control

Fuente: Elaboración propia

De acuerdo a este criterio se obtuvo el siguiente resultado:

Respuesta	Cantidad de Empresas	Apreciación
De 0 a 3 afirmaciones	7	No se considera
De 4 a 7 afirmaciones	13	Se considera

Tabla 4.9 Respuestas de preguntas relacionadas al primer control

Fuente: Elaboración propia

Es decir en 13 empresas el documento de políticas de seguridad de información, puede ser considerado como tal, ya que contiene los lineamientos generales, se debe aclarar que eso no implica que cumpla con todo lo requerido en la norma NB/ISO/IEC 27001, simplemente es una buen indicador.

En el siguiente gráfico se ilustran los resultados, en porcentaje:

Figura 4.1 Resultado del primer control. Políticas de Seguridad de la Información

Fuente: Elaboración propia

Se considera que el 65% de las empresas corredores de seguros tiene un documento de Políticas de Seguridad de la Información, que están alineadas a parámetros generales.

El 35% no se considera que sigan con lineamientos generales de políticas de seguridad de la Información, en este sentido se tienen dos aspectos, primero que no se cuente con ningún documento que haga referencias a seguridad de la información, segundo que exista algún documento borrador el cual no esté completo, y no cumpla con lineamientos generales, por tanto no ha sido aprobado por Gerencia.

También relacionado con el documento de políticas de Seguridad de la Información, se realizó la siguiente pregunta:

PREGUNTA	RESPUESTA
Con que frecuencia son revisadas las políticas de seguridad de la información?	Semestralmente Anualmente

Tabla 4.10 Pregunta de selección para el primer control

Fuente: Elaboración propia

En este caso las trece empresas, respondieron que revisan el documento de políticas de seguridad de la información anualmente.

Hace tres años la APS mediante la resolución administrativa APS/DJ/DS/ Nº39 – 2016 del 12 de enero de 2016, menciono a la norma NB-ISO-IEC 27001, la cual se convirtió en una guía para el área de Tecnologías de Información, en cuanto a la documentación que se debía generar.

Poco a poco se fueron generando algunos documentos, que tienen diferentes nombres, como ser:

- ✓ Manual de Seguridad de Sistemas
- ✓ Manual de Seguridad de la Información

Los cuales hacen referencia a algunos parámetros de seguridad de la información. Hoy en día aún se continúa con esa falta de normalización respecto al nombre del documento, la cual no permite realizar una referencia general. Otra falencia es que no se encuentran formalmente aprobados por gerencia, por tal motivo no son de conocimiento general, estos dos aspectos deberán ser superados para cumplir con las características de un Documento de Políticas de Seguridad de la Información.

4.2.2 Segundo Control. Organización de la Seguridad de la Información. Fueron dos preguntas asociadas, las cuales son:

PREGUNTA	RESPUESTA
Existe el área de sistemas? Por cuanto personal está integrado? 1 2 3 4 5 más de cinco	SI ☐ Valor 1 NO ☐ Valor 0
Existe alguna persona específica con tareas de seguridad de la información?	SI ☐ Valor 1 NO ☐ Valor 0

Tabla 4.11 Preguntas relacionadas con el segundo control

Fuente: Elaboración propia

La puntuación se considera según el número de afirmaciones, es así que la puntuación mínima es cero y la máxima será de dos (1+1) porque existen dos preguntas con afirmaciones.

De acuerdo a los resultados se considera la siguiente distribución:

Rango de puntuación (Cantidad de afirmaciones)	Apreciación (Organización de seguridad de la información)
Igual a 0	No se Considera
De 1 a 2	Se Considera

Tabla 4.12 Detalle de puntuación relacionado al segundo control

Fuente: Elaboración propia

Este aspecto requiere de un análisis, ya que los resultados están relacionados con las empresas que tienen personal en el área de sistemas, quienes tienen conocimiento sobre la importancia de la seguridad de la información, cabe mencionar que el 10% tiene una persona con funciones descritas sobre seguridad de la información. El resto de las empresas asigna este rol como una tarea genérica al área de sistemas.

De acuerdo a este criterio se obtuvo el siguiente resultado:

Respuesta	**Cantidad de Empresas**	**Apreciación**
0 afirmaciones	13	No se considera
De 1 a 2 afirmaciones	7	Se considera

Tabla 4.13 Respuesta de preguntas relacionadas al segundo control

Fuente: Elaboración propia

Los resultados en porcentaje se lo puede observar en el siguiente gráfico:

Figura 4.2 Resultado del segundo control. Organización de la Seguridad de la Información
Fuente: Elaboración propia

En los resultados el 35% se puede considerar que existe una Organización de la Seguridad de la Información, ya que cuentan con personal del área de tecnologías de la información, que está organizada respecto a roles de Seguridad de la Información.

En el caso de las empresas que tienen personal de tecnologías de información externo, por factores como ser: el tamaño físico de la empresa y el presupuesto. Los gerentes asumen el rol, de la organización de la Seguridad de la Información, realizando estas tareas con los proveedores externos que les brindan soporte técnico a nivel de Hardware y Software, sin embargo la falencia es que no se tiene documentación y en algún caso la documentación no está ordenada. Por este motivo es que no fueron considerados en los resultados mostrados en la *Figura 4.2*

En el departamento o unidad de sistemas, es importante que exista la segregación de deberes, ya que es una forma de crecer y brindar la oportunidad de generar proyectos. El problema que se tiene es que en algunos casos se sobrecarga de responsabilidades y funciones a una sola persona, lo que dificulta el avance y generación de proyectos en el área de T.I. que son importantes para la empresa.

4.2.3 Tercer control. Seguridad de Recursos Humanos. Con relación a este control se realizaron las siguientes preguntas:

PREGUNTA	RESPUESTA
La empresa incentiva el trabajo que realiza el área o encargado de sistemas?	SI ☐ Valor 1 NO ☐ Valor 0
El encargado de sistemas firma algún acuerdo de confidencialidad con la Empresa?	SI ☐ Valor 1 NO ☐ Valor 0
Se ha realizado alguna capacitación sobre seguridad de la información?	SI ☐ Valor 1 NO ☐ Valor 0

Tabla 4.14 Preguntas relacionadas al tercer control

Fuente: Elaboración propia

La puntuación se considera según el número de afirmaciones, es así que la puntuación mínima es cero y la máxima será de tres (1+1+1) porque existen tres preguntas con afirmaciones.

De acuerdo a los resultados se considera la siguiente distribución:

Rango de puntuación (Cantidad de afirmaciones)	Apreciación (En cuanto a la organización de seguridad de la información)
De 0 a 1	No se Considera
De 2 a 3	Se Considera

Tabla 4.15 Detalle de puntuación relacionado al tercer control

Fuente: Elaboración propia

Si el resultado es una afirmación, puede ser que exista incentivo al trabajo que realiza el área o encargado de sistemas, pero no existe un acuerdo de confidencialidad y no existe capacitación al personal sobre seguridad de la información, es decir las tres preguntas se excluyen. Se recalca que los resultados no implican que se estén cumpliendo o no con todos los requisitos que exige la norma ISO 27001.

De acuerdo a este criterio se obtuvo el siguiente resultado:

Cantidad de Respuestas	Cantidad de Empresas	Apreciación
De 0 a 1 afirmación	12	No se considera
De 2 a 3 afirmaciones	8	Se considera

Tabla 4.16 Respuesta de preguntas relacionadas al tercer control

Fuente: Elaboración propia

En la siguiente *Figura 4.3*, se puede observar los resultados en porcentajes:

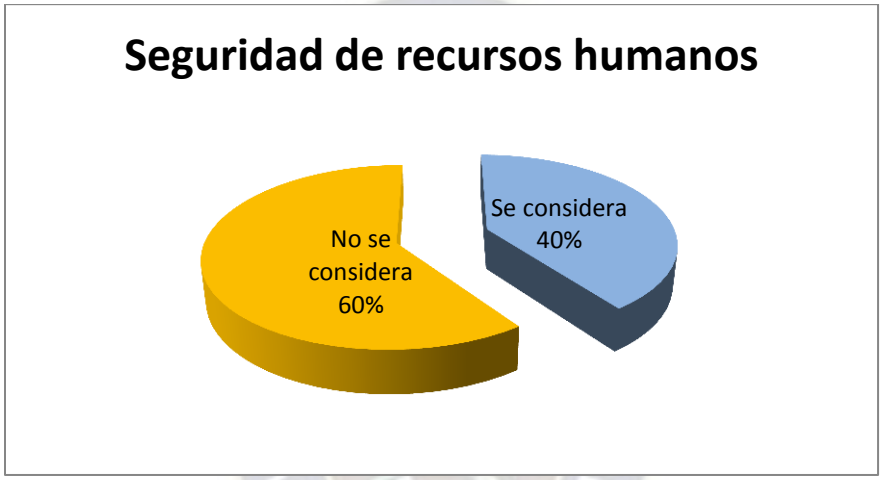


Figura 4.3 Resultado del tercer control, seguridad ligada a los recursos humanos

Fuente: Elaboración propia

En las empresas que no tienen unidad de Tecnologías de Información, respecto a la pregunta: “El encargado de sistemas firma algún acuerdo de confidencialidad con la Empresa”, en la entrevista, se explicó que puede aplicarse al encargado de sistemas, que es una persona externa a contrato. Haciéndoles notar que es un aspecto importante para la seguridad de la información en la empresa. Así también la realización de capacitaciones sobre seguridad de la información a todo el personal.

En este caso, podría considerarse que un 40% está tomando medidas de seguridad de información ligada a los recursos humanos, ya que el personal relacionado a T.I. interno o externo, que realiza soporte de hardware y software, firma un contrato de confidencialidad, además se realiza una capacitación anual sobre temas de seguridad

de la información al personal y en algunos casos se incentiva al personal de T.I. por el trabajo realizado.

4.2.4 Cuarto control. Administración de Activos. En relación a este punto, se realizaron las siguientes preguntas:

PREGUNTA	RESPUESTA
Se cuenta con un inventario de activos físicos?	SI ☐ Valor 1 NO ☐ Valor 0
En el inventario se incluyen los activos intangibles?	SI ☐ Valor 1 NO ☐ Valor 0
Se cuenta con algún registro manual o registro por sistema, que indique características del activo, como nombre del propietario, versión y otros?	SI ☐ Valor 1 NO ☐ Valor 0
Existe alguna política o procedimiento sobre el manejo de medios extraíbles (Discos duros externos, DVDs, memorias USB y otros)	SI ☐ Valor 1 NO ☐ Valor 0

Tabla 4.17 Preguntas relacionadas con el cuarto control

Fuente: Elaboración propia

La puntuación se considera según el número de afirmaciones, es así que la puntuación mínima es cero y la máxima será de cuatro (1+1+1+1) porque existen cuatro preguntas con afirmaciones.

De acuerdo a los resultados se considera la siguiente distribución:

Rango de puntuación (Cantidad de afirmaciones)	Apreciación (Administración de activos)
De 0 a 2	No se Considera
De 3 a 4	Se Considera

Tabla 4.18 Detalle de puntuación relacionado al cuarto control

Fuente: Elaboración propia

La gran falencia es que no se consideran los activos de información, como ser registros, formularios, tan poco se consideran los activos de información intangibles, que están asociados a la información, como ser el software que brinda funciones que la empresa requiere. Si bien todas las empresas cuentan con los registros de inventarios, de activos físicos, en está ocasión se hace énfasis en los activos de información ya sean físicos o intangibles. Al respecto se tiene el siguiente resultado:

Cantidad de Respuestas	Cantidad de Empresas	Apreciación
De 0 a 2 afirmaciones	15	No se considera
De 3 a 4 afirmaciones	5	Se considera

Tabla 4.19 Respuestas de preguntas relacionadas con el cuarto control

Fuente: Elaboración propia

En la siguiente *Figura 4.4*, se puede observar los resultados en porcentajes:

Figura 4.4 Resultado del cuarto control, sobre Administración de activos

Fuente: Elaboración propia

Todas las empresas cuentan con el inventario de activos físicos, ya sea en registros físicos, o en registros digitales. En la entrevista se aclaró la pregunta sobre activos intangibles, como es el caso del software.

El 25% considera en los inventarios, a los activos de información, como ser software con licencia, instaladores y programas de aplicación. El 75 % no considera en los inventarios los activos de información, entonces se desconoce su existencia.

4.2.5 Quinto control. Control de acceso. Se consideraran las siguientes tres preguntas:

PREGUNTA	RESPUESTA
El acceso a la computadora es mediante contraseña?	SI ☐ Valor 1 NO ☐ Valor 0
Existe algún requisito para elegir contraseña?	SI ☐ Valor 1 NO ☐ Valor 0
La máxima autoridad de la empresa tiene conocimiento sobre los niveles de acceso que tiene cada usuario?	SI ☐ Valor 1 NO ☐ Valor 0

Tabla 4.20 Preguntas relacionadas con el quinto control

Fuente: Elaboración propia

La puntuación se considera según el número de afirmaciones, es así que la puntuación mínima es cero y la máxima será de tres (1+1+1) porque existen esa cantidad de afirmaciones.

De acuerdo a los resultados se considera la siguiente distribución:

Rango de puntuación (Cantidad de afirmaciones)	Apreciación (Control de Acceso)
De 0 a 1	No se Considera
De 2 a 3	Se Considera

Tabla 4.21 Detalle de puntuación relacionado con el quinto control

Fuente: Elaboración propia

Si bien el control de accesos tiene muchos aspectos que deben ser analizados cuyo objetivo es limitar el acceso a la información y a las instalaciones de procesamiento de

datos, considerando que no todas las empresas cuentan con una instalación de procesamiento de datos, las preguntas son genéricas, de controles mínimos con respecto al acceso de las computadoras, que en algunos casos tienen funciones de servidores, donde se encuentran instalados sistemas importantes para las empresas, con esa consideración se tienen los siguientes resultados:

Cantidad de Respuestas	Cantidad de Empresas	Apreciación
De 0 a 1 afirmación	13	No se considera
De 2 a 3 afirmaciones	7	Se considera

Tabla 4.22 Respuestas de preguntas relacionadas al quinto control

Fuente: Elaboración propia

En la siguiente *Figura 4.6,* se puede ver la representación en porcentajes:

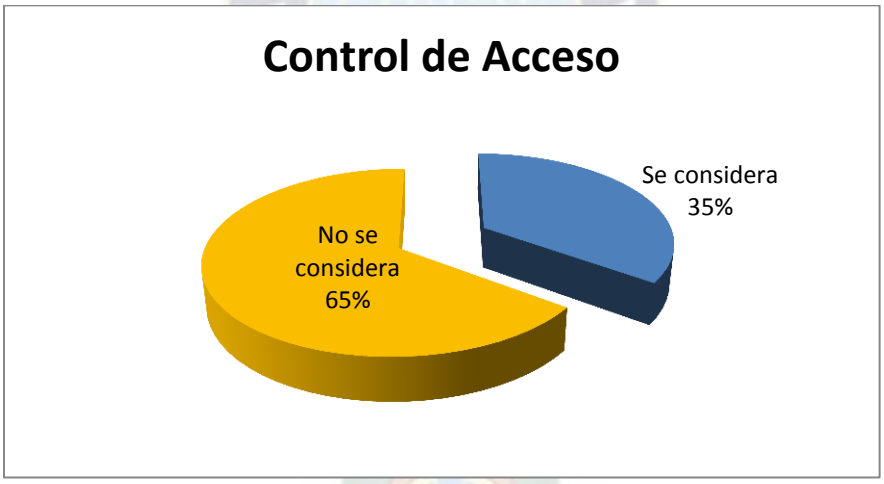


Figura 4.5 Resultado quinto control, Control de Acceso

Fuente: Elaboración propia

El 35 % puede considerarse que tiene algún control de acceso a las computadoras y la Gerencia tiene conocimiento. El 75 % no se considera ya que no existen los mínimos controles de acceso a las computadoras.

En la entrevista, se extendieron las siguientes preguntas para las empresas que cuentan con una instalación dedicada a procesamiento de datos (conocida como C.P.D Centro de Procesamiento de Datos):

PREGUNTAS	RESPUESTAS
Que controles de acceso físico se tienen en el acceso al CPD?	Entrada huella digital. Registro a la entrada. Cámaras de Seguridad. Otros
Que controles de acceso lógico se tienen en el acceso al CPD?	Firewall. VLAN. ACL. VPN. Otros

Tabla 4.23 Preguntas de selección relacionados con el quinto control

Fuente: Elaboración propia

Todos los Centros de Procesamiento de Datos (C.P.D.), tienen uno o dos controles físicos y por lo menos un control de acceso lógico, en este caso el Firewall. En el séptimo control se tienen más datos respecto al C.P.D.

4.2.6 Sexto Control. Criptografía

Se consideraron las siguientes preguntas:

PREGUNTA	RESPUESTA
Conoce algoritmos de cifrado para criptografía?	SI ☐ Valor 1 NO ☐ Valor 0
Se aplica la criptografía, en algún sistema?	SI ☐ Valor 1 NO ☐ Valor 0
La información almacenada, caso backup, utiliza criptografía?	SI ☐ Valor 1 NO ☐ Valor 0

Tabla 4.24 Preguntas relacionadas con el sexto control

Fuente: Elaboración propia

La puntuación se considera según el número de afirmaciones, es así que la puntuación mínima es cero y la máxima será de tres (1+1+1) porque existen tres preguntas con afirmaciones.

De acuerdo a los resultados se considera la siguiente distribución:

Rango de puntuación (Cantidad de afirmaciones)	Apreciación (Criptografía)
De 0 a 1	No se Considera
De 2 a 3	Se Considera

Tabla 4.25 Detalle de puntuación relacionado al sexto control

Fuente: Elaboración propia

Se considera que si se tiene dos afirmaciones entonces se estaría aplicando la criptografía, lo que indica que puede ser considerado como un buen parámetro de seguridad.

En la siguiente tabla se muestran los resultados:

Cantidad de Respuestas	**Cantidad de Empresas**	**Apreciación**
De 0 a 1 afirmación	18	No se considera
De 2 a 3 afirmaciones	2	Se considera

Tabla 4.26 Respuestas de preguntas relacionadas con el sexto control

Fuente: Elaboración propia

En el siguiente gráfico se puede ver, la representación en porcentaje:

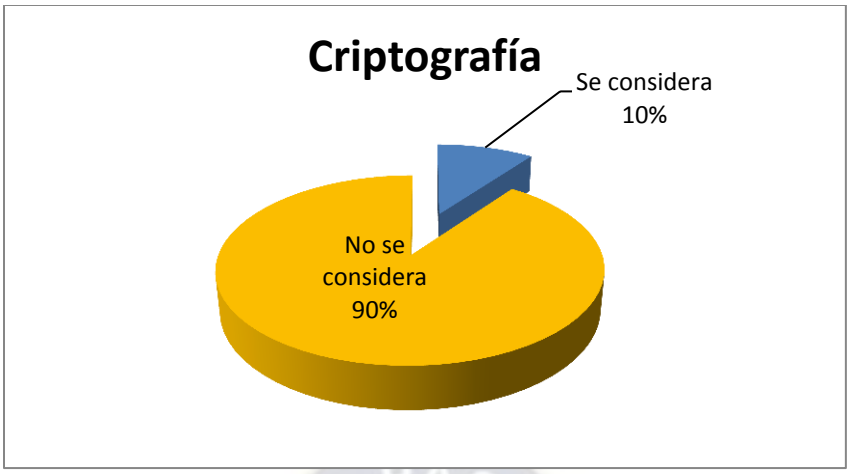


Figura 4.6 Resultado Sexto control, Criptografía

Fuente: Elaboración propia

Al respecto el 90 % de las empresas no utiliza aún métodos de criptografía, en algunos casos se utilizan VPN, para comunicarse con las sucursales de otros departamentos, el proveedor del servicio de VPN usa la criptografía, en el canal de comunicación.

4.2.7 Séptimo control. Seguridad física y del Ambiente

Se consideran las siguientes preguntas:

PREGUNTA	RESPUESTA
Se cuenta con un Centro de Procesamiento de Datos (CPD)?	SI ☐ Valor 1 NO ☐ Valor 0
Existe un medidor de temperatura y humedad en el CPD?	SI ☐ Valor 1 NO ☐ Valor 0

En el CPD Se cuenta con UPS? Se han realizado pruebas de funcionamiento? Se realiza el mantenimiento?	SI ☐ Valor 1 NO ☐ Valor 0 SI ☐ Valor 1 NO ☐ Valor 0 SI ☐ Valor 1 NO ☐ Valor 0
Se cuenta con extintor? Se realiza el mantenimiento? Se cuenta con ventilador o aire acondicionado? Se le realiza el mantenimiento?	SI ☐ Valor 1 NO ☐ Valor 0 SI ☐ Valor 1 NO ☐ Valor 0 SI ☐ Valor 1 NO ☐ Valor 0 SI ☐ Valor 1 NO ☐ Valor 0
Se cuenta con cableado estructurado? Se cuenta con los informes de certificación del cableado estructurado?	SI ☐ Valor 1 NO ☐ Valor 0 SI ☐ Valor 1 NO ☐ Valor 0
Cuenta con un cronograma de mantenimiento de equipos de computación? Existe algún registro del mantenimiento de equipos de computación?	SI ☐ Valor 1 NO ☐ Valor 0 SI ☐ Valor 1 NO ☐ Valor 0

Tabla 4.27 Preguntas relacionadas con el séptimo control

Fuente: Elaboración propia

La puntuación se considera según el número de afirmaciones, es así que la puntuación mínima es cero y la máxima será de trece (1+1+1+1+1+1+1+1+1+1+1+1+1) porque existen trece preguntas con afirmaciones.

De acuerdo a los resultados se considera la siguiente distribución:

Rango de puntuación (Cantidad de afirmaciones)	Apreciación (Seguridad Física y del Ambiente)
De 0 a 7	No se Considera
De 8 a 13	Se Considera

Tabla 4.28 Detalle de puntuación relacionado al séptimo control

Fuente: Elaboración propia

Las preguntas buscan conocer los mínimos parámetros que se utilizan o están desarrollando las empresas corredoras. No se busca saber si cumplen con todos los controles de la norma NB/IEC/ISO 27002.

Los resultados obtenidos se muestran en la siguiente tabla:

Cantidad de Respuestas	**Cantidad de Empresas**	**Apreciación**
De 0 a 7 afirmaciones	11	No se considera
De 8 a 13 afirmaciones	9	Se considera

Tabla 4.29 Respuestas de preguntas relacionadas al séptimo control

Fuente: Elaboración propia

En el siguiente gráfico se puede observar el resultado en porcentajes:

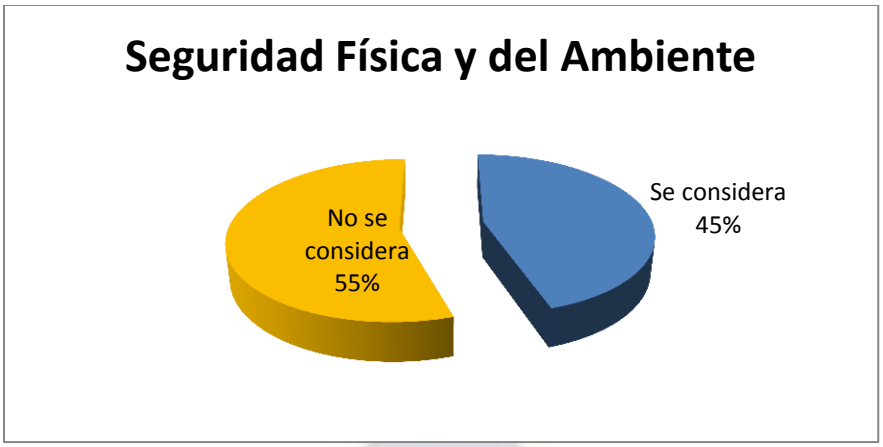


Figura 4.7 Resultado séptimo control, Seguridad Física y del Ambiente
Fuente: Elaboración Propia

El objetivo de este control es evitar el acceso físico no autorizado, los daños e interferencia a la información de la organización y las instalaciones de procesamiento de la información, en ese contexto, las empresas que cuentan con CPD llegaron a obtener entre 10 a 13 afirmaciones, las empresas que no cuentan con CPD llegaron a obtener entre 8 y 10 afirmaciones, por lo cual en ambos casos se considera los aspectos de Seguridad física y del ambiente. Por lo que se obtuvo un porcentaje del 45 % que significa se considera la seguridad física y del ambiente.

En el caso donde se obtuvo de 0 a 7 afirmaciones, el 55% no se considera, tal como se aprecia en la *Figura 4.7,* interpretando el resultado indicaría que si bien cuentan con UPS, Extintor, no se les realiza el mantenimiento respectivo, cuentan con cableado estructurado pero no está certificado, cuenta con un cronograma de mantenimiento de equipos de computación pero no tienen registros, por tal motivo no se considera la seguridad física y del Ambiente. Cabe mencionar que estas preguntas están elaboradas para ajustarse al entorno del ambiente en estudio, y no significa que cumplan o no cumplan con todos los controles de la norma NB/IEC/ISO 27002.

4.2.8 Octavo Control. Seguridad de las operaciones.

Al respecto se tienen las siguientes preguntas:

PREGUNTA	RESPUESTA
Se cuenta con documentos de procedimientos operativos? (Como ser: Descripción de cómo realizar respaldos. Uso de correo electrónico)	SI ☐ Valor 1 NO ☐ Valor 0
Existe restricción en el ancho de banda, en la red, en Internet, para los usuarios?	SI ☐ Valor 1 NO ☐ Valor 0
Se realiza el desarrollo de software, para necesidades de la empresa?	SI ☐ Valor 1 NO ☐ Valor 0
Se cuenta con la instalación y actualización de software de detección de malware?	SI ☐ Valor 1 NO ☐ Valor 0
Los usuarios saben qué hacer en caso de presentarse un malware?	SI ☐ Valor 1 NO ☐ Valor 0
Se obtienen los backups de los equipos más sensibles? Los Backups son probados?	SI ☐ Valor 1 NO ☐ Valor 0 SI ☐ Valor 1 NO ☐ Valor 0

Existen registros de la obtención de backups? Se registran las ejecuciones de pruebas de los backups?	SI ☐ Valor 1 NO ☐ Valor 0 SI ☐ Valor 1 NO ☐ Valor 0
Se cuenta con un documento que identifique las vulnerabilidades técnicas, de equipos sensibles como los servidores?	SI ☐ Valor 1 NO ☐ Valor 0
Existen políticas que rigen la instalación de software por parte de los usuarios?	SI ☐ Valor 1 NO ☐ Valor 0

Tabla 4.30 Preguntas relacionadas al octavo control

Fuente: Elaboración propia

La puntuación se considera según el número de afirmaciones, es así que la puntuación mínima es cero y la máxima será de once (1+1+1+1+1+1+1+1+1+1+1) porque existen once preguntas con afirmaciones.

De acuerdo a los resultados se considera la siguiente distribución:

Rango de puntuación (Cantidad de afirmaciones)	**Apreciación (Seguridad de las operaciones)**
De 0 a 4	No se Considera
De 5 a 11	Se Considera

Tabla 4.31 Detalle de puntuación relacionado al octavo control

Fuente: Elaboración propia

Como ya se mencionó se tienen dos aspectos importantes, empresas con personal de T.I. y empresas sin personal de T.I.

En el caso de las empresas con personal de T.I. fueron seis empresas que alcanzaron las once afirmaciones. Se debe notar que existen empresas que no cuentan con personal de T.I. de planta, sin embargo llegaron a alcanzar entre 5 a 7 afirmaciones, ya que cuentan con software de detección de malware, los usuarios están capacitados para manejar la situación en caso de que se presente el malware. El proveedor de soporte técnico realiza los backups correspondientes de los equipos más sensibles, realiza la prueba respectiva y genera el informe con los registros, además de limitar los privilegios de los usuarios, para instalar software.

En la siguiente tabla se muestran los resultados obtenidos:

Cantidad de Respuestas	Cantidad de Empresas	Apreciación
De 0 a 4 afirmaciones	11	No se considera
De 5 a 11 afirmaciones	9	Se considera

Tabla 4.32 Respuestas de preguntas relacionadas al octavo control
Fuente: Elaboración propia

En el siguiente gráfico se puede observar el resultado en porcentajes:

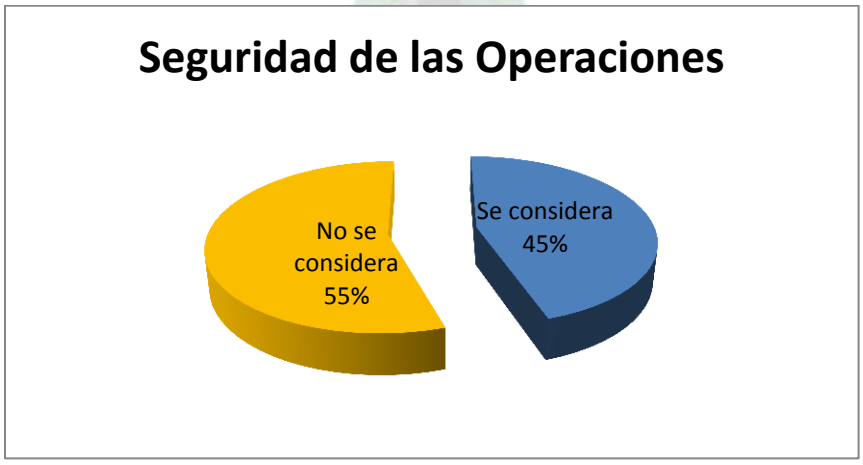


Figura 4.8 Resultados del octavo control, Seguridad de las Operaciones
Fuente: Elaboración propia

Donde se puede apreciar que el 45 %, ha tomado medidas de seguridad de las operaciones, entre las que se encuentran empresas corredoras con personal de T.I. y también las que cuentan con personal de T.I. externo.

El control inadecuado de cambios a las instalaciones y sistemas de procesamiento de la información es una causa común para las fallas de seguridad o del sistema. (NB/ISO/IEC 27002)

Se deberían producir, mantener y revisar de manera periódica los registros de eventos del usuario, las excepciones, las fallas y los eventos de seguridad de la información. (NB/ISO/IEC 27002)

El registro de eventos establece las bases para los sistemas de monitoreo automatizado que son capaces de generar informes y alertas consolidadas sobre la seguridad del sistema. Los registros de eventos pueden contener datos sensibles e información de identificación personal. Se deberían tomar medidas de protección adecuadas para la privacidad. (NB/ISO/IEC 27002)

Donde sea posible, los administradores del sistema no deberían tener permisos para borrar o desactivar los registros de sus actividades. (NB/ISO/IEC 27002)

En algunos casos en las empresas corredoras, como política en el tema de correo electrónico corporativo, se guarda una copia de cualquier correo electrónico saliente de la empresa, esto genera mayor almacenamiento de correos, sin embargo es una medida de seguridad, aceptable.

En este caso se requiere de un profesional especializado que tenga las competencias requeridas para cumplir las funciones de un Oficial de Seguridad de la Información (OSI), quien realice el monitoreo y revisión de registro de eventos.

4.2.9 Noveno control. Seguridad de las Comunicaciones

Al respecto se tiene las siguientes preguntas:

PREGUNTA	RESPUESTA
Existe la separación de unidad de redes e informática?	SI ☐ Valor 1 NO ☐ Valor 0
Se cuenta con Contrato del proveedor de Internet? Se cuenta con contrato de servicios de red? (Provisión de conexiones, servicio de redes privadas, firewalls u otros)	SI ☐ Valor 1 NO ☐ Valor 0 SI ☐ Valor 1 NO ☐ Valor 0
Existe un servidor de dominio? Existe alguna segmentación lógica como uso de VLAN?	SI ☐ Valor 1 NO ☐ Valor 0 SI ☐ Valor 1 NO ☐ Valor 0
Existe alguna política, sobre el uso aceptable de las instalaciones de comunicación?	SI ☐ Valor 1 NO ☐ Valor 0
Se informó a los usuarios sobre las precauciones de envió de información confidencial, en las redes de comunicación?	SI ☐ Valor 1 NO ☐ Valor 0
Se cuenta con algún documento o política sobre el uso de la mensajería, redes sociales?	SI ☐ Valor 1 NO ☐ Valor 0

Tabla 4.33 Preguntas relacionadas al noveno control

Fuente: Elaboración propia

La puntuación se considera según el número de afirmaciones, es así que la puntuación mínima es cero y la máxima será de ocho (1+1+1+1+1+1+1+1) porque existen ocho preguntas con afirmaciones.

De acuerdo a los resultados se considera la siguiente distribución:

Rango de puntuación (Cantidad de afirmaciones)	Apreciación (Seguridad de las comunicaciones)
De 0 a 3	No se Considera
De 4 a 8	Se Considera

Tabla 4.34 Detalle de puntuación relacionado al noveno control

Fuente: Elaboración propia

Realizando el análisis para los dos casos, en el cual existen empresas corredoras con personal de T.I. y otras empresas corredoras con personal de T.I. externo.

En el caso de las empresas corredoras con personal de T.I. llegan desde 2 hasta 8 afirmaciones. En las empresas corredoras con personal de T.I. externo, se resalta que algunos llegaron a tener cinco afirmaciones, ya que cuentan con el contrato de servicio de Internet, existen políticas sobre el uso aceptable de las instalaciones de comunicación, los usuarios están capacitados sobre el envió de información confidencial en las redes de comunicación, el uso de mensajería y el uso de redes sociales.

En la siguiente tabla se muestran los resultados obtenidos:

Cantidad de Respuestas	Cantidad de Empresas	Apreciación
De 0 a 3 afirmaciones	12	No se considera
De 4 a 8 afirmaciones	8	Se considera

Tabla 4.35 Respuestas de preguntas relacionadas al noveno control

Fuente: Elaboración propia

En el siguiente gráfico se puede observar el resultado en porcentajes:

Figura 4.9 Resultados noveno control, Seguridad de las comunicaciones

Fuente: Elaboración propia

Se puede considerar que el 40%, ha establecido algunos lineamientos en el control de seguridad de las Comunicaciones, cabe destacar que dentro de este porcentaje se encuentran indistintamente las corredoras que cuentan con personal de T.I. de planta, y las corredoras con personal T.I. externo.

Otra pregunta, que se realizo es la siguiente:

PREGUNTA	RESPUESTA
Cuál de los siguientes servicios es más importante, para la empresa?	Correo, Internet, sistema de producción, otro sistema…….

Tabla 4.36 Pregunta relacionada al noveno control

Fuente: Elaboración propia

En esta pregunta se obtuvo un 70% de respuestas indicando que el Sistema de Producción, tiene prioridad, sin restarle importancia al servicio de Internet y correo electrónico.

En cuanto al sistema de producción, es software, en algunos casos son desarrollados a medida por personal de T.I., en otros casos se adquieren soluciones genéricas es decir software ya desarrollado y en otros casos no se utiliza, es dependiente del tamaño de la empresa corredora.

4.2.10 Décimo control. Adquisición, desarrollo y mantenimiento de sistemas.

Al respecto se tienen las siguientes preguntas:

PREGUNTA	RESPUESTA
Existe algún contrato sobre adquisición, de sistemas? Existe algún contrato de desarrollo y mantenimiento de sistemas?	SI ☐ Valor 1 NO ☐ Valor 0 SI ☐ Valor 1 NO ☐ Valor 0
Se cuenta con la documentación sobre proyectos de desarrollo de software?	SI ☐ Valor 1 NO ☐ Valor 0
Se documenta el proceso de pruebas, para adquirir un nuevo software?	SI ☐ Valor 1 NO ☐ Valor 0
Tiene conocimiento sobre clave pública y firma digital?	SI ☐ Valor 1 NO ☐ Valor 0
Se cuenta con un documento el cual establezca las reglas para el desarrollo de software y sistemas? Los proveedores son empresas: nacionales o internacionales	SI ☐ Valor 1 NO ☐ Valor 0
Se cuenta con un documento que indique los procedimientos de control de cambios en sistemas?	SI ☐ Valor 1 NO ☐ Valor 0

Cuando se cuenta con un nuevo sistema, se realizan las pruebas de aceptación?	SI ☐ Valor 1 NO ☐ Valor 0
En caso de adquirir un sistema (software) ¿El contrato señala los derechos de propiedad de código y de propiedad intelectual?	SI ☐ Valor 1 NO ☐ Valor 0

Tabla 4.37 Preguntas relacionadas al décimo control

Fuente: Elaboración propia

La puntuación se considera según el número de afirmaciones, es así que la puntuación mínima es cero y la máxima será de nueve (1+1+1+1+1+1+1+1+1) que indican nueve preguntas con afirmaciones.

De acuerdo a los resultados se considera la siguiente distribución:

Rango de puntuación (Cantidad de afirmaciones)	**Apreciación (Adquisición, desarrollo y mantenimiento de sistemas)**
De 0 a 4	No se Considera
De 5 a 9	Se Considera

Tabla 4.38 Detalle de puntuación relacionado al décimo control

Fuente: Elaboración propia

Realizando el análisis para los dos casos, en el cual existen empresas corredoras con personal de T.I. y otras empresas corredoras con personal de T.I. externo.

Algunas empresas corredoras no utilizan sistema de producción, para realizar sus actividades utilizan Hojas de Excel.

En la siguiente tabla se muestran los resultados obtenidos:

Cantidad de Respuestas	Cantidad de Empresas	Apreciación
De 0 a 4 afirmaciones	3	No se considera
De 5 a 9 afirmaciones	17	Se considera

Tabla 4.39 Respuestas de preguntas relacionadas al décimo control

Fuente: Elaboración propia

En el siguiente *Figura 4.10* se puede observar el resultado en porcentajes:

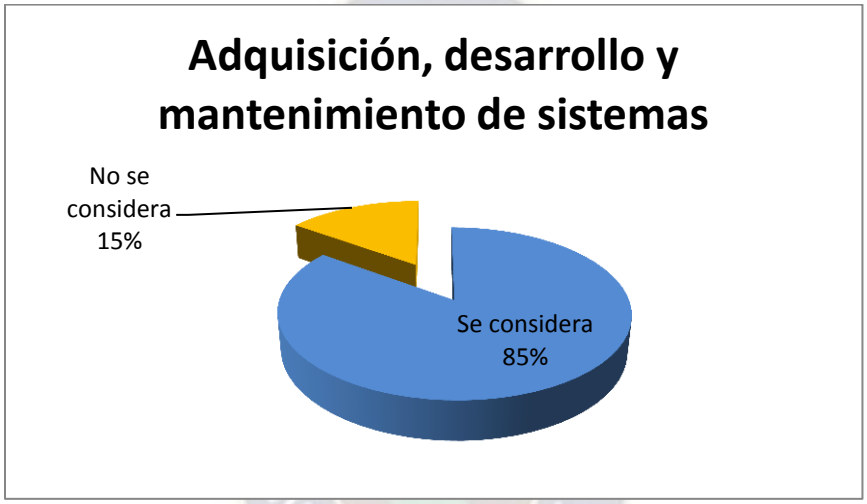


Figura 4.10 Resultados décimo control. Adquisición, desarrollo y mantenimiento de sistemas

Fuente: Elaboración propia

Se puede considerar que el 85%, ha establecido algunos lineamientos en la adquisición, desarrollo y mantenimiento de sistemas, el 15% representa a las empresas corredoras que no tienen sistemas, este caso será analizado con más profundidad en el siguiente apartado.

En algunas empresas que no tienen personal de T.I. de planta, el software de producción es obsoleto (año 2009), que ya no brinda el apoyo que requieren los funcionarios, por lo cual utilizan hojas Excel, bastante elaboradas, con fórmulas que ayudan a obtener los reportes, si bien es una buena forma de obtener los informes requeridos, el problema radica en que no se cuenta con una base de datos, que

permite ver los históricos de manera eficiente, por tanto no se puede realizar trazabilidad y no se cumplen con otros aspectos de control de seguridad.

Más del 50% de las empresas, tienen dos sistemas los cuales son Sistema de Producción y Sistema Contable, separados. Los cuáles es recomendable que sean integrados, por la información que se requiere entre ambos sistemas.

En el décimo control de Adquisición, desarrollo y mantenimiento de sistemas los procedimientos de control de cambios del sistema, debe incluir una evaluación de riesgos.

4.2.11 Décimo primer control. Relaciones con los proveedores.

Se aplicaron las siguientes preguntas:

PREGUNTA	RESPUESTA
¿Existe una política sobre el acceso de los proveedores a la información de la empresa?	SI ☐ Valor 1 NO ☐ Valor 0
¿Existe una capacitación para el personal de la empresa que interactúa con el proveedor?	SI ☐ Valor 1 NO ☐ Valor 0
Se abordan el tema de seguridad dentro de los acuerdos con los proveedores que proporcionan componentes de infraestructura de T.I.?	SI ☐ Valor 1 NO ☐ Valor 0
En el acuerdo o contrato con los proveedores se especifican las obligaciones del proveedor para cumplir los requisitos de seguridad de la organización?	SI ☐ Valor 1 NO ☐ Valor 0
Existe una persona específica que administre las relaciones con el proveedor?	SI ☐ Valor 1 NO ☐ Valor 0

Se cuenta con los informes de servicio de los proveedores?	SI ☐ Valor 1 NO ☐ Valor 0

Tabla 4.40 Preguntas relacionadas con el décimo primer control

Fuente: Elaboración propia

La puntuación se considera según el número de afirmaciones, es así que la puntuación mínima es cero y la máxima será de seis (1+1+1+1+1+1) que indican seis preguntas con afirmaciones.

De acuerdo a los resultados se considera la siguiente distribución:

Rango de puntuación (Cantidad de afirmaciones)	**Apreciación (Relaciones con los proveedores)**
De 0 a 3	No se Considera
De 4 a 6	Se Considera

Tabla 4.41 Detalle de puntuación relacionado con décimo primer control

Fuente: Elaboración propia

Este control independientemente si las empresas corredoras cuentan con personal de T.I. interno o externo, es un parámetro muy importante ya que todas las empresas corredoras, tienen algún proveedor, ya sea de hardware o software y en muchos casos ambos, es decir se tiene un proveedor que presta el servicio técnico de mantenimiento de equipos de computación e impresoras y otro proveedor de soporte para software. Por lo tanto la relación con el proveedor es fundamental y tiene que estar basada por contratos o acuerdos bien estipulados, teniendo en cuenta el tema de seguridad de la información.

En la siguiente tabla se muestran los resultados obtenidos:

Cantidad de Respuestas	Cantidad de Empresas	Apreciación
De 0 a 3 afirmaciones	6	No se considera
De 4 a 6 afirmaciones	14	Se considera

Tabla 4.42 Respuestas de preguntas relacionadas al décimo primer control

Fuente: Elaboración propia

Se tienen acuerdos de servicio con los proveedores de:

- Servicio de Internet
- Servicio de Hosting
- Servicio de Correo Electrónico
- Servicio de soporte técnico para equipos de computación e impresoras
- Servicio de soporte técnico para Sistemas y Programas entre los que se pueden citar: Sistemas de Producción, Sistemas Contables y Sistemas de Facturación
- Servicio de mantenimiento de equipos y dispositivos de telefonía
- Contrato de prestación de servicios, venta de cartuchos de tóner, proveyendo las impresoras y realizando el mantenimiento de las mismas de acuerdo al cronograma.

Cuando en las preguntas se hace referencia a los proveedores, puede ser cualquiera de los que se citaron, ya que son lineamientos generales y las respuestas darán una idea sobre algunos controles de seguridad que se aplican.

En el siguiente gráfico se puede observar el resultado en porcentajes:

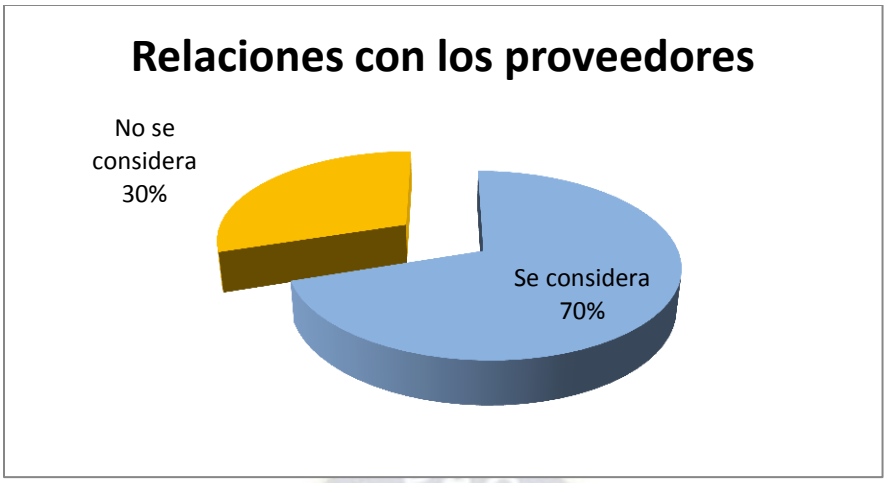


Figura 4.11 Resultados décimo primer control. Relaciones con los proveedores
Fuente: Elaboración propia

Se considera que el 70% de las empresas corredoras han establecido relaciones con los proveedores de servicios basados en parámetros de la seguridad de la información. Entre los parámetros generales, según los resultados del cuestionario se puede indicar que existe una capacitación para el personal de la empresa que interactúa con el proveedor, en el acuerdo o contrato con los proveedores se especifican las obligaciones del proveedor para cumplir los requisitos de seguridad de la empresa, existe una persona específica que administre las relaciones con el proveedor y se cuenta con los informes de servicio de los proveedores.

4.2.12 Décimo segundo control. Administración de incidentes de seguridad de la información

Al respecto se tienen las siguientes preguntas:

PREGUNTA	RESPUESTA
Se cuenta con un documento aprobado por gerencia sobre los procedimientos para la respuesta rápida, eficaz y ordenada a los incidentes que puedan presentarse?	SI ☐ Valor 1 NO ☐ Valor 0

La unidad de TI cuenta con los procedimientos para monitorear, detectar, analizar e informar sobre eventos e incidentes de seguridad?	SI ☐ Valor 1 NO ☐ Valor 0
Se capacito al personal sobre como reconocer incidentes y eventos de seguridad de la información? (fallas en software, accesos no autorizados, errores humanos)	SI ☐ Valor 1 NO ☐ Valor 0

Tabla 4.43 Preguntas relacionadas con el décimo segundo control

Fuente: Elaboración propia

La puntuación se considera según el número de afirmaciones, es así que la puntuación mínima es cero y la máxima será de tres (1+1+1) que indican tres preguntas con afirmaciones.

De acuerdo a los resultados se considera la siguiente distribución:

Rango de puntuación (Cantidad de afirmaciones)	Apreciación (Administración de incidentes de seguridad de la información)
De 0 a 1	No se Considera
De 2 a 3	Se Considera

Tabla 4.44 Detalle de puntuación relacionado al décimo segundo control

Fuente: Elaboración propia

En el análisis de este control, se debe mencionar que aunque existen procedimientos para el manejo y reconocimiento de incidentes, estos no se encuentran documentados, es así que en las entrevistas al respecto, consideraron que sería un buen punto referencial para empezar a documentar los procedimientos que en muchos casos se los tiene sobreentendido con algunas disposiciones de la empresa.

En la siguiente tabla se muestran los resultados obtenidos:

Cantidad de Respuestas	Cantidad de Empresas	Apreciación
De 0 a 1 afirmación	14	No se considera
De 2 a 3 afirmaciones	6	Se considera

Tabla 4.45 Respuestas de preguntas relacionadas al décimo segundo control

Fuente: Elaboración propia

En el siguiente gráfico se muestran los mismos resultados en porcentaje.

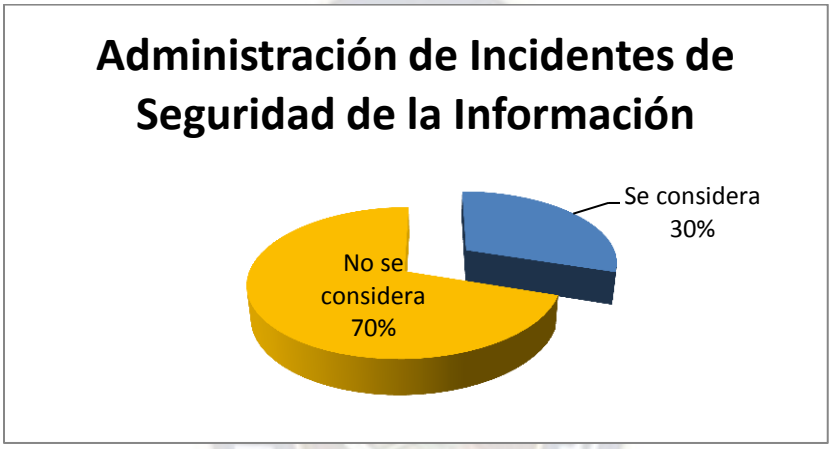


Figura 4.12 Resultados décimo segundo control. Administración de Incidentes de Seguridad de la Información

Fuente: Elaboración propia

En nuestro entorno de Tecnologías de la Información, aún no se ha desarrollado el tema de procedimientos y documentación de incidentes de seguridad de la información, siendo una falencia a nivel general.

Es así que se puede observar que el 70% de las empresas no ha adoptado tareas vinculadas a la administración de incidentes de Seguridad de la Información, por varias razones entre las cuales están la falta de conocimiento, falta de presupuesto y en algunos casos indican que por el hecho de ser empresas pequeñas que tienen un personal de 5 personas, no lo ven necesario.

También cabe mencionar que se cuentan con dos empresas que tienen certificación ISO 9001, lo que permitió generar documentación en toda la unidad de T.I., si bien no se cuenta con todos los procedimientos necesarios para cumplir con la norma NB/ISO/IEC 27001, se tiene una buena base, la cual podría ser explotada.

4.2.13 Décimo tercer control. Aspectos de la seguridad de la información de la administración de la continuidad del negocio

Al respecto se tienen las siguientes preguntas:

PREGUNTA	RESPUESTA
Se cuenta con un plan documentado sobre la continuidad del negocio.	SI ☐ Valor 1 NO ☐ Valor 0
Si se cuenta con este documento, se ha previsto la continuidad de la seguridad en la información?	SI ☐ Valor 1 NO ☐ Valor 0
Se tiene un plan de contingencias tecnológico? De qué año es? ……...	SI ☐ Valor 1 NO ☐ Valor 0

Tabla 4.46 Preguntas relacionadas al décimo tercer control

Fuente: Elaboración propia

La puntuación se considera según el número de afirmaciones, es así que la puntuación mínima es cero y la máxima será de tres (1+1+1) que indican tres preguntas con afirmaciones. De acuerdo a los resultados se considera la siguiente distribución:

Rango de puntuación (Cantidad de afirmaciones)	**Apreciación (Aspectos de la seguridad de la información de la administración de la continuidad del negocio)**
De 0 a 1	No se Considera
De 2 a 3	Se Considera

Tabla 4.47 Detalle de puntuación relacionado al décimo tercer control

Fuente: Elaboración propia

En este control se considera que mínimamente se contemple un plan de contingencias tecnológico, el cual pueda ser aplicado en caso de que se presenten contingencias de cualquier tipo. Se toma en cuenta a todas las empresas corredoras independientemente del tamaño y la existencia de personal de T.I. ya que es un factor importante para mitigar riesgos de índole tecnológico.

El plan de continuidad del negocio, es aún más relevante, ya que es un estudio minucioso especializado el cual requiere bastante tiempo de desarrollo, y está vinculado con áreas administrativas. Los resultados obtenidos, se pueden observar en la siguiente tabla:

Cantidad de Respuestas	Cantidad de Empresas	Apreciación
De 0 a 1 afirmación	15	No se considera
De 2 a 3 afirmaciones	5	Se considera

Tabla 4.48 Respuestas de preguntas relacionadas al décimo tercer control

Fuente: Elaboración propia

En el siguiente gráfico se muestran los mismos resultados en porcentaje.

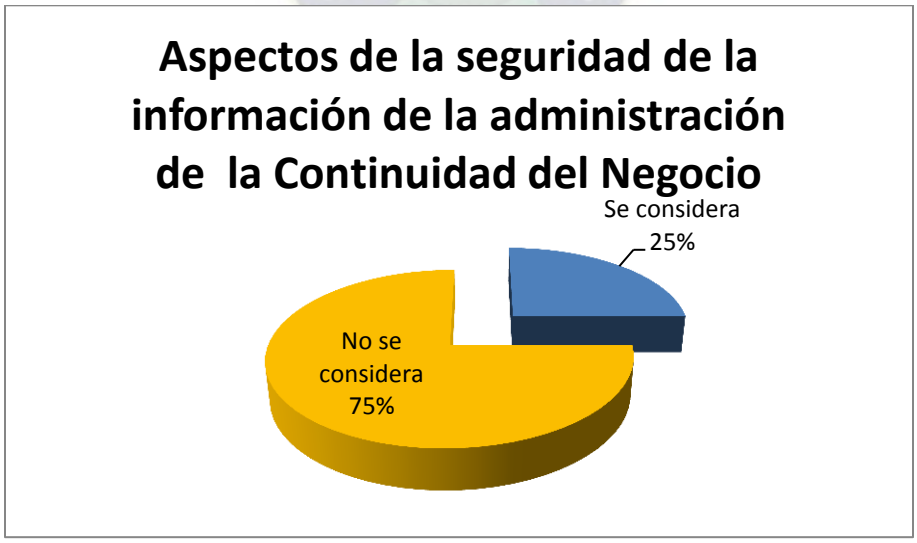


Figura 4.13 Resultados décimo tercer control. Aspectos de la seguridad de la información de la administración de la Continuidad del Negocio

Fuente: Elaboración propia

De acuerdo a los resultado obtenidos el 75% no se considera que hayan previsto el aspecto de la seguridad de la información de la administración de la Continuidad Comercial, este es un aspecto que en nuestro entorno está empezando a desarrollarse, en este ámbito las entidades financieras tienen mayor experiencia.

El 25% se puede considerar que han previsto el aspecto de la seguridad de la información de la administración de la Continuidad Comercial, los documentos de plan de contingencias tecnológicos y plan de continuidad comercial son de hace tres y dos años (años 2017 y 2018).

4.2.14 Décimo cuarto control. Cumplimiento

En referencia a este control, se debe aclarar que no se está evaluando solo el cumplimiento de los requerimientos del ente regulador, ni tan poco se está evaluando el cumplimiento de requisitos de la norma NB/IEC/ISO 27001, solamente es un indicador que ayudará a determinar los lineamientos que se tienen considerando el documento de políticas de seguridad de la información, establecidos en las empresas corredoras.

Para este cometido se realizaron las siguientes preguntas:

PREGUNTA	RESPUESTA
Se cuenta con una matriz de riesgo a nivel de Tecnología, en seguridad de la Información?	SI ☐ Valor 1 NO ☐ Valor 0
Existe una política sobre la privacidad y protección de la información personal identificable?	SI ☐ Valor 1 NO ☐ Valor 0
Se ha realizado pruebas de penetración y evaluaciones de vulnerabilidad, a los sistemas de la empresa? En qué fecha? ……	SI ☐ Valor 1 NO ☐ Valor 0

Tabla 4.49 Preguntas relacionadas al décimo cuarto control

Fuente: Elaboración propia

Otra pregunta que se encuentra en el cuestionario es:

El documento de las políticas de seguridad de la información son revisadas por: Auditoria interna, Auditoria externa, Jefatura de T.I. u otros

Todas las empresas que cuentan con el documento de políticas de seguridad de la información, indicaron que son revisadas por Auditoria Externa y Gerencia.

Otra pregunta que se realizó en la entrevista es:

Cumple con todos los requerimientos del Ente Regulador?

La cual fue respondida afirmativamente por todas las empresas corredoras.

La puntuación se considera según el número de afirmaciones, es así que la puntuación mínima es cero y la máxima será de tres (1+1+1) que indican tres preguntas con afirmaciones.

De acuerdo a los resultados se considera la siguiente distribución:

Rango de puntuación (Cantidad de afirmaciones)	**Apreciación (Cumplimiento)**
0 afirmaciones	No se Considera
De 1 a 3 afirmaciones	Se Considera

Tabla 4.50 Detalle de puntuación relacionado al décimo cuarto control

Fuente: Elaboración propia

En la siguiente tabla se pueden mostrar los resultados:

Cantidad de Respuestas	**Cantidad de Empresas**	**Apreciación**
0 afirmación	11	No se considera
De 1 a 3 afirmaciones	9	Se considera

Tabla 4.51 Respuestas de preguntas relacionadas al décimo cuarto control

Fuente: Elaboración propia

En el siguiente gráfico se muestran los resultados en porcentaje.

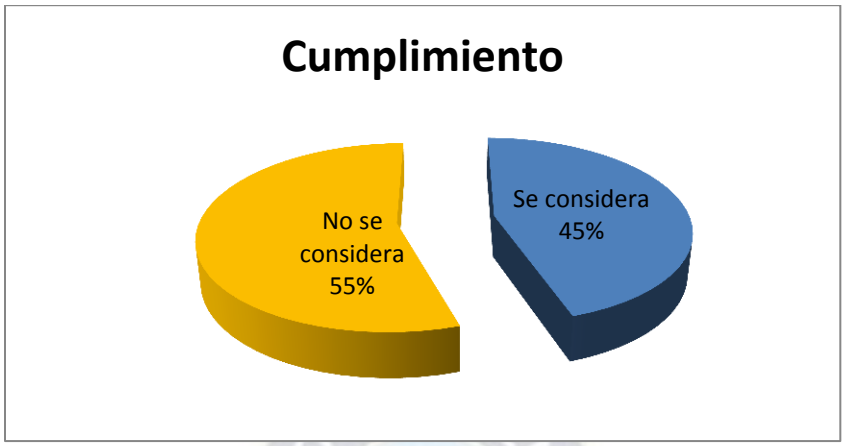


Figura 4.14 Resultados décimo cuarto control. Cumplimiento

Fuente: Elaboración propia

El 45% se considera que ha tomado algunos parámetros, sobre el control de cumplimiento, en referencia a las políticas de seguridad de la información.

Cabe mencionar que siendo reguladas por la APS, cumplen con las resoluciones emitidas, en el caso de Tecnología de Información se puede mencionar: la circular APS/DS/JCF/153 – 2017 del 6 de noviembre de 2017 que trata del alcance mínimo para la realización de Auditorías Externas, que en el numeral cinco relativo a Tecnología de Información indica: “La firma de Auditoría deberá evaluar y emitir opinión sobre los controles de los sistemas informáticos y de procesamiento de datos adoptados y/o desarrollados por la Entidad”.

Revisando con más detalle también se puede mencionar la Resolución Administrativa IS No 1025 del 18 de noviembre de 2005, que en el Artículo 4 referente a Tecnología de Información indica: “Si la corredora adoptó o desarrolló sistemas de procesamiento electrónico de datos para el desarrollo de sus operaciones, los auditores externos deben evaluar y emitir opinión, sobre si dichos sistemas son confiables, íntegros y oportunos; y en particular de los factores tecnológicos de riesgo que se identifiquen y revelar, si encontraran deficiencias que limiten la confiabilidad de dicho sistema”.

Como se puede apreciar son requerimientos generales en el área de Tecnologías de la Información, todas la empresas corredoras cumplen con los requerimientos de la APS.

En el caso del cumplimiento con las políticas de seguridad de la información, se da la importancia a la política sobre la privacidad y protección de la información personal identificable. Como ya se apreció en el primer control, se preguntó sobre la existencia del documento de Políticas de Seguridad de la Información, en el que se obtuvo como resultado que el 35% no se considera, ya que no cuentan con dicho documento o el documento no logro la puntuación necesaria según la parametrización que se adoptó.

4.3 RESULTADO GENERAL DE LOS CONTROLES DE SEGURIDAD DE LA INFORMACIÓN, EN LAS EMPRESAS CORREDORES DE SEGUROS Y REASEGUROS

Finalmente, en base al resultado de cada control, se tiene el siguiente gráfico, en el cual se encuentra un resumen de los resultados obtenidos en el Cuestionario.

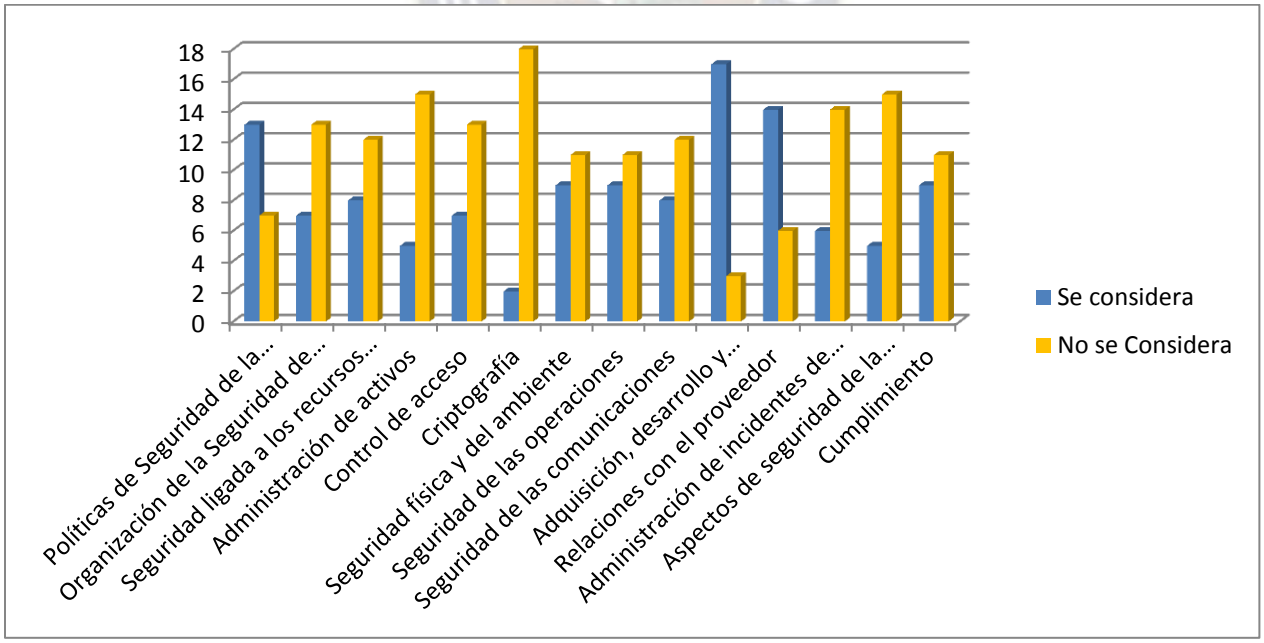


Figura 4.15 Resultado General de los Controles de Seguridad de la Información

Fuente: Elaboración Propia

Los resultados plasman que se han contemplado medidas de seguridad de la información, sin embargo la norma ISO 27001, no solamente trata de la existencia de seguridad de la información si no de la Gestión es decir de la administración de la seguridad.

En este aspecto se cumplen con muchos de los controles sin embargo la gran falencia es la falta de generación de documentación en el área de T.I. es decir registros, formularios, procedimientos, manuales lo cuales puedan reflejar el cumplimiento de controles de seguridad de la información.

Como se observa en los resultados generales, se puede destacar las fortalezas que se han encontrado en los tres controles que son considerados:

- ✓ Políticas de Seguridad de la Información
- ✓ Adquisición, desarrollo y mantenimiento del sistema
- ✓ Relaciones con el proveedor

El documento de políticas de seguridad de la información, tiene puntos relevantes, sin embargo aún está en desarrollo, la revisión que se le realiza es anual y es un requerimiento de auditoria externa.

La adquisición, desarrollo y mantenimiento del sistema, está asociado a un acuerdo entre partes mediante contratos que están basados en la confidencialidad del manejo seguro de la información de la empresa. Se ha observado que el 50% de las empresas corredores no tienen personal de T.I. en planta y el soporte técnico de hardware y software es tercializado, por tal motivo y conscientes de ese factor es que se tienen: cronogramas, registros e informes de las tareas de soporte técnico, ya que mediante esa documentación se genera el pago del servicio.

Las Relaciones con el proveedor, son de confianza, pues realizan un trabajo delicado como es el manejo de la información de la empresa, los usuarios están capacitados para el trato con el proveedor, y las relaciones están regidas por contratos.

En referencia a los restantes once controles, no se los considera ya que tienen bastantes falencias en los lineamientos generales, por lo cual se tiene que trabajar bastante, especialmente en la documentación que debe generar cada control.

Los resultados también son analizados en el Capítulo 6, con el enfoque de Gestión del Riesgo en la Seguridad de la Información.

CAPITULO 5

5. ANÁLISIS DE APLICABILIDAD DE LOS CONTROLES DE LA NORMA NB/ISO/IEC 27001:2013 EN LAS EMPRESAS CORREDORES DE SEGUROS Y REASEGUROS

La Norma NB/ISO/IEC 27001, en el Anexo A nombran los controles que están directamente alineados con la norma NB/ISO/IEC 27002.

La estructura de la Norma NB/ISO/IEC 27002, contiene 14 cláusulas de control de seguridad que en conjunto contienen un total de 35 categorías de seguridad principales y 114 controles.

Basados en la Norma NB/ISO/IEC 27002 y con los resultados obtenidos en el cuestionario, a continuación se extraerá los controles, que pueden ser aplicables a las empresas corredores de Seguros y Reaseguros.

5.1 PRIMER CONTROL. POLÍTICAS DE SEGURIDAD DE INFORMACIÓN.

Se debería definir un conjunto de políticas para la seguridad de la información y la debería aprobar la dirección para publicarla y comunicarla a los empleados y a todas las partes externas pertinentes. (NB/ISO/IEC 27002, 2014)

La política de seguridad de la información debería tener enunciados respecto a lo siguiente:

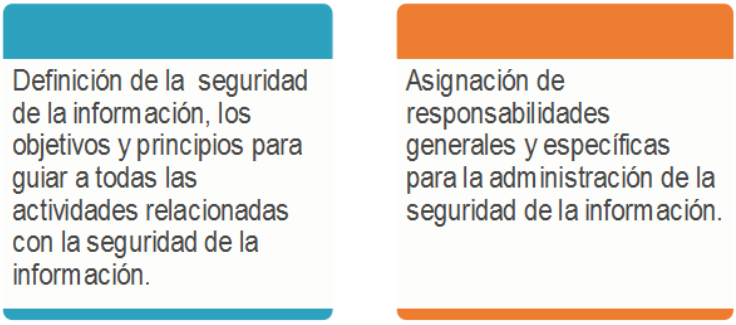


Figura 5.1 Características de la política de Seguridad de la Información

Fuente: Elaboración propia, basada en norma NB/ISO/IEC 27002

En general las políticas de seguridad de la información, deben incluir los siguientes aspectos:

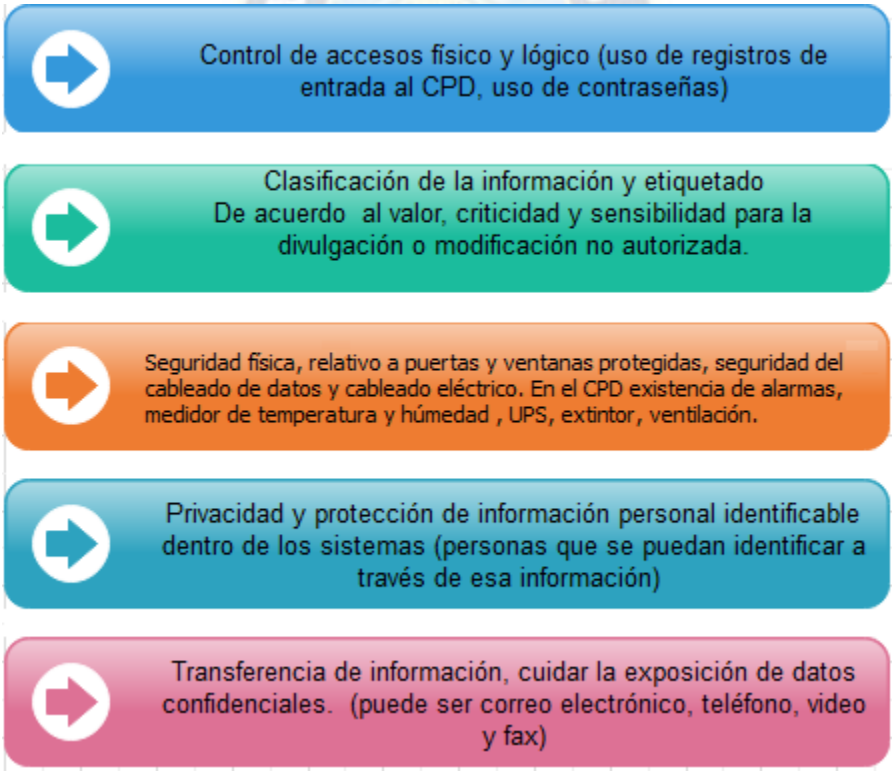


Figura 5.2 Aspectos que deben ser incluidos en la política de Seguridad de la Información
Fuente: Elaboración propia basado en norma NB/ISO/IEC 27002

Las empresas corredores de seguros y reaseguros no son organizaciones grandes, el personal con el que cuentan oscila entre 5 y 120 personas. En relación a este control

sobre la generación de un documento de Políticas de Seguridad de la Información, se observó que el 65% ya posee un documento relacionado. El cual debe ser revisado tomando en cuenta algunos parámetros de la norma NB/ISO/IEC 27001, que aportaran con las mejoras a la Administración de la seguridad de la información.

Por otro lado por muy pequeña que sea la empresa debería tener un Documento de Políticas de Seguridad de la Información basado en el enfoque organizacional de acuerdo al entorno en el que se encuentra. Dicho documento deberá ser revisado, por Gerencia, personal de T.I. si corresponde y revisiones de Auditoria Interna y Auditoria Externa. Por tanto se considera un control Aplicable porque es la base para el resto de los controles.

5.2 SEGUNDO CONTROL. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

El objetivo es establecer un marco de administración para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización. (NB/ISO/IEC 27002, 2014)

Se deberían definir y asignar todas las responsabilidades de seguridad de la información, considerando lo siguiente:

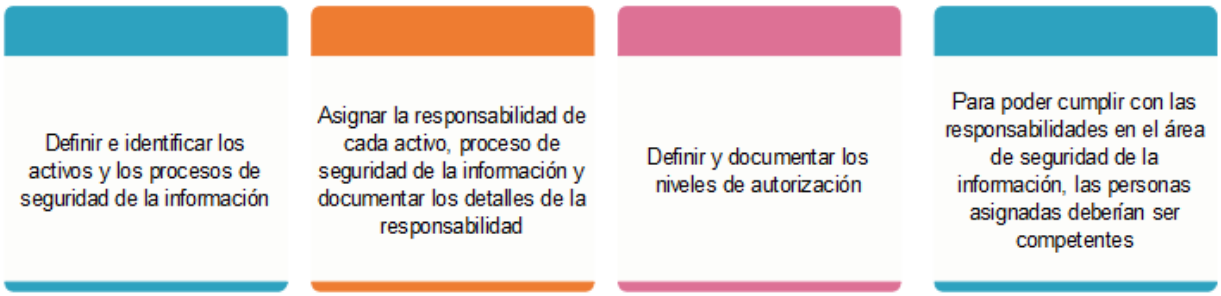


Figura 5.3 Controles en Organización de la seguridad de la Información
Fuente: Elaboración propia basado en norma NB/ISO/IEC 27002

En la norma menciona la asignación específica de personal de seguridad de la información, en el entorno de estudio de las empresas corredoras, donde el personal de T.I. puede ser de planta o externo, no es factible, por tanto este aspecto no es aplicable.

Entonces Gerencia y Jefatura de T.I. tendrán que establecer los siguientes aspectos que se deberían considerar.

- ✓ La segregación de funciones estaría dirigida para empresas con personal de T.I.
- ✓ Los contactos con autoridades y grupos de interés, deberían estar plasmados por escrito.
- ✓ La seguridad de la información debería ser parte de los proyectos en general.
- ✓ Los dispositivos móviles que se utilizan para realizar trabajos, deberían estar sujetos a las políticas de seguridad de la información, además de cumplir con requisitos para la protección física.
- ✓ El trabajo fuera de la oficina conocido como teletrabajo deberían regirse por políticas que protejan a la información a la que se accede, procese o almacene.

En este aspecto como resultado de la entrevista se puede indicar que la unidad o área de Tecnologías de Información está compuesta por un máximo de cinco personas. Observando que el 50% de las empresas cuentan con personal de T.I. de planta y el otro 50% cuenta con personal de T.I. externo, las responsabilidades de organización de la seguridad de la información recaerían en la Jefatura de T.I. y en el caso de las empresas que cuentan con personal de T.I. externo recaería sobre Gerencia. Por tanto este control puede Aplicarse de forma parcial, indicando que la asignación específica de personal de seguridad de la información, no es factible, según el contexto de las Empresas Corredoras.

El control es necesario porqué se requiere de una organización en el aspecto de la seguridad de la información, que implique responsabilidades.

5.3 TERCER CONTROL. SEGURIDAD DE RECURSOS HUMANOS

Se consideran los aspectos: antes del empleo, durante el empleo, desvinculación y cambio de empleo.

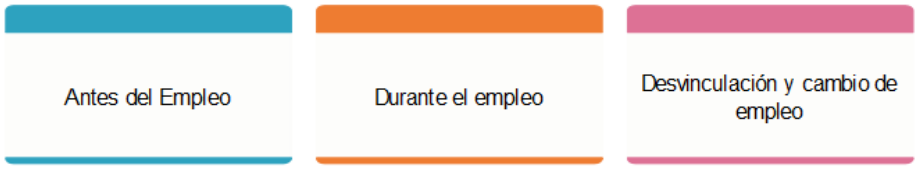


Figura 5.4 Aspectos en la seguridad de Recursos Humanos
Fuente: Elaboración propia basado en norma NB/ISO/IEC 27002

En la norma hace referencia a una persona contratada para un rol de seguridad de la información, para el caso de empresas corredores, este rol será asumido por el personal de T.I. por lo que se debería considerar los siguientes puntos:

- ✓ La selección será realizada de acuerdo a los reglamentos de la empresa.
- ✓ Verificar que el candidato posea las competencias necesarias, ya que tendrá acceso a las instalaciones de procesamiento de información. Debiendo firmar un acuerdo de confidencialidad y no divulgación, que además contemple los siguientes aspectos:
    - Responsabilidad para manejar la información recibida de otras empresas o partes externas.
    - Medidas que se tomaran si el empleado no cumple con los requisitos de seguridad.

Durante el empleo, Gerencia deberá asegurarse que:

- ✓ El personal tenga conocimiento de las políticas de seguridad de la información y de los roles y responsabilidades de seguridad de la información antes de que se le otorgue acceso a la información confidencial o a los sistemas de información.
- ✓ Que el personal este motivado, que continúe teniendo las habilidades y calificaciones adecuadas, capacitándose de manera regular.

De manera general, incluyendo a todo el personal de la empresa, es de vital importancia, la concientización, educación y capacitación sobre la seguridad de la

información, se pueden realizar programas de concientización mediante una charla, preparando los materiales necesarios como presentaciones, boletines informativos y otros. Es importante que el personal entienda el objetivo de la seguridad de la información y el posible impacto, ya sea positivo y negativo, en la empresa y en su propio comportamiento. (NB/ISO/IEC 27002, 2014)

Cuando existe una desvinculación o cambio de empleo, las responsabilidades incluidas dentro del acuerdo de confidencialidad, pueden continuar por un período de tiempo definido, estos aspectos deberán ser coordinados con la unidad o departamento de Recursos Humanos.

Se considera aplicable según el tamaño, contexto y características de la Empresa corredora. Ya que por muy robusta que sea la tecnología de seguridad de la información, no será suficiente si los recursos humanos no están debidamente capacitados.

5.4 CUARTO CONTROL. ADMINISTRACIÓN DE ACTIVOS

Se deberían identificar los activos asociados a la información y las instalaciones de procesamiento de información y se debería elaborar y mantener un inventario de estos activos. (NB/ISO/IEC 27002, 2014)

En el caso del área de Tecnologías de Información, aún no se reconocen a muchos activos asociados a la información como ser: registros, formularios, manuales de procedimientos, directamente se considera activo a los equipos de computación y equipos de comunicación.

La orientación sobre la implementación indica sobre el ciclo de vida de la información que debería incluir su creación, procesamiento, almacenamiento, transmisión, eliminación y destrucción.

El propietario del activo debería ser responsable de la administración correcta de un activo todo su ciclo de vida.

Cuando el propietario del activo se encuentre en proceso de finalización de empleo se debería formalizar para incluir la devolución de todos los activos físicos y electrónicos previamente entregados de propiedad de o encomendados a la empresa. (NB/ISO/IEC 27002, 2014)

En el proceso de finalización del empleo, Recursos Humanos y la unidad de T.I. deberían coordinar las acciones basados en las políticas de seguridad de la información.

Se deberían identificar, documentar e implementar las reglas para el uso aceptable de la información de los activos asociados a la información y a las instalaciones de procesamiento de información.

Una guía para elaborar un registro con activos de información identificados sería el siguiente:

Activo	Tipo	Propietario del activo	Uso aceptable del activo
Formulario de Solicitud de Revisión equipo de computación	Información	Departamento o unidad de T.I.	Llenado de información del formulario
Servidor de base de datos	Hardware	Empresa	Acceso a personal autorizado
Sistema de producción	Software	Departamento o unidad de T.I.	Acceso a personal autorizado

Tabla 5.1 Registro de activos de información

Fuente: Elaboración propia

Otro aspecto importante es asegurar que la información reciba el nivel de protección adecuado de acuerdo con su importancia para la empresa. El nivel de protección debería evaluarse mediante el análisis de la confidencialidad, la integridad y la disponibilidad. A continuación se tiene una forma de caracterizarla.

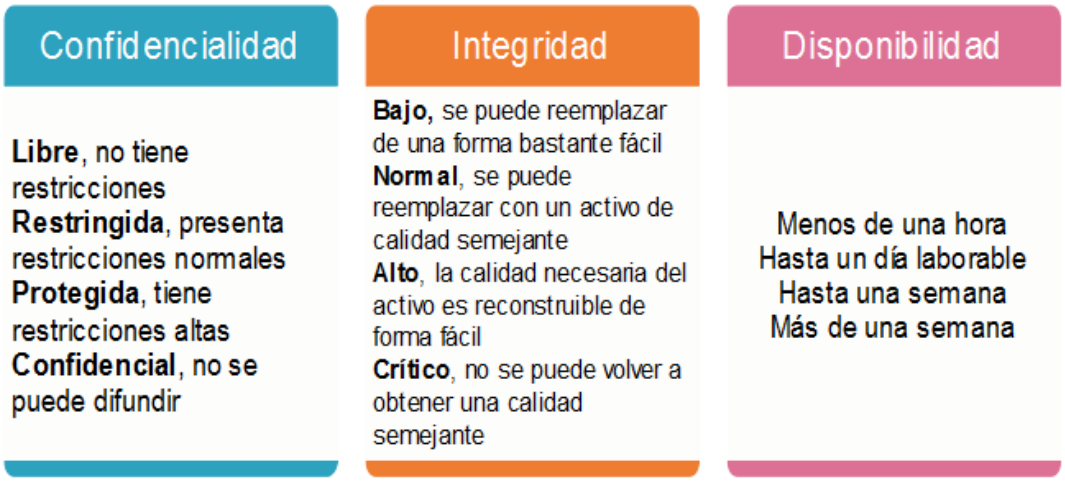


Figura 5.5 Criterios de Confidencialidad, Integridad y Disponibilidad

Fuente: Elaboración propia con base a material del Curso de ISO 27001 IBNORCA

Entonces en el registro de activos, también se tendría que colocar estas características, de la siguiente manera:

Activo	Confidencialidad	Integridad	Disponibilidad
Formulario de Solicitud de Revisión equipo de computación	Libre	Bajo	Hasta una semana (Indisponible hasta una semana)
Servidor de base de datos	Confidencial	Crítico	Menos de una hora (Indisponible hasta una hora)
Sistema de producción	Protegida	Alta	Menos de una hora (Indisponible hasta una hora)

Tabla 5.2 Registro de activos con características de Confidencialidad, Integridad y Disponibilidad

Fuente: Elaboración propia

El etiquetado de la información debería reflejar las características que tiene el activo, es decir se puede colocar un rótulo de Confidencial, a la información que así sea, este control debería ser considerado.

Para el manejo de activos se deberían crear procesos de almacenamiento, procesamiento y comunicación de la información conforme a las características del activo, considerando:

- ✓ Restricciones de acceso que apoyen los requisitos de protección para cada nivel de clasificación.
- ✓ Mantenimiento de un registro formal de receptores de activos autorizados.
- ✓ Almacenamiento de los activos de T.I. de acuerdo con las especificaciones del fabricante.

En el documento de políticas de seguridad de la información se debería contemplar el manejo de medios, para evitar la divulgación, la modificación, el retiro o la destrucción de información almacenada en medios, considerando:

- ✓ Las unidades de medios extraíbles solo se deberían habilitar si existe una razón para ello, se debería monitorear la transferencia de información a dichos medios.
- ✓ Los medios que contienen información confidencial se deberían almacenar y eliminar de manera segura.

En las empresas corredores que cuentan con personal de T.I. externo, este punto es importante, en el entendido de que al prestar servicios de soporte técnico, también realizan backups, por lo que se debe conocer a cabalidad cual es la información que se está transfiriendo. Es un control aplicable y necesario, para cuantificar el valor de los activos asociados al área de Tecnologías de Información.

5.5 QUINTO CONTROL. CONTROL DE ACCESO.

El objetivo limitar el acceso a la información y a las instalaciones de procesamiento de la información.

Se debería establecer, documentar y revisar una política de control de acceso en base a los requisitos del negocio y de la seguridad de la información. (NB/ISO/IEC 27002, 2014)

La política de control de acceso, tiene una estructura, sobre la orientación podría tomarse la siguiente:

POLÍTICA DE CONTROL DE ACCESO

1. **INTRODUCCION**
   Descripción del documento

2. **OBJETIVO**
   Objetivo

3. **ALCANCE**
   Alcance de la política

4. **MARCO REFERENCIAL**
   Referencias en las cuales se basa el documento

5. **CONTROL DE ACCESOS**
   - Control de conexiones a las redes
   - Control de acceso a Internet
   - Control de Acceso al Sistema Operativo
   - Control de Acceso a la Información, archivos compartidos
   - Control de Acceso al correo electrónico
   - Control de acceso en Equipos de Cómputo portable

6. **CONTROL DE CAMBIOS**

   Se debe colocar la fecha de Elaboración, Revisión y Aprobación del presente documento, con las respectivas firmas.

Figura 5.6 Política de Control de Acceso

Fuente: Elaboración Propia

Un ejemplo de política de control de acceso se encuentra desarrollado en el Anexo 2.

Extraemos de la norma NB/ISO/IEC 27002, las siguientes recomendaciones:

- ✓ Las normas de control de acceso se deberían respaldar con procedimientos formales y responsabilidades definidas.

- ✓ El control de acceso basado en roles es un enfoque que se utiliza correctamente en muchas empresas para vincular los derechos de acceso con las funciones de negocio.

El objetivo de la Administración de acceso a los usuarios, es garantizar el acceso autorizado a los usuarios y evitar el acceso no autorizado a los sistemas y servicios, considerando los siguientes aspectos:

- ✓ Procedimiento formal de entrega de acceso a los usuarios
- ✓ Administración de la información de autenticación secreta de los usuarios (las contraseñas son un tipo de información de autenticación)
- ✓ La asignación y el uso de derechos de acceso privilegiado se deberían restringir y controlar.
- ✓ Revisión de los derechos de acceso de usuarios, a intervalos regulares y después de cualquier cambio, como un ascenso o cese de empleo.
- ✓ Eliminación o ajustes de los derechos de acceso, incluyen accesos físico y lógico.

En el siguiente gráfico, se pueden ver estos aspectos:

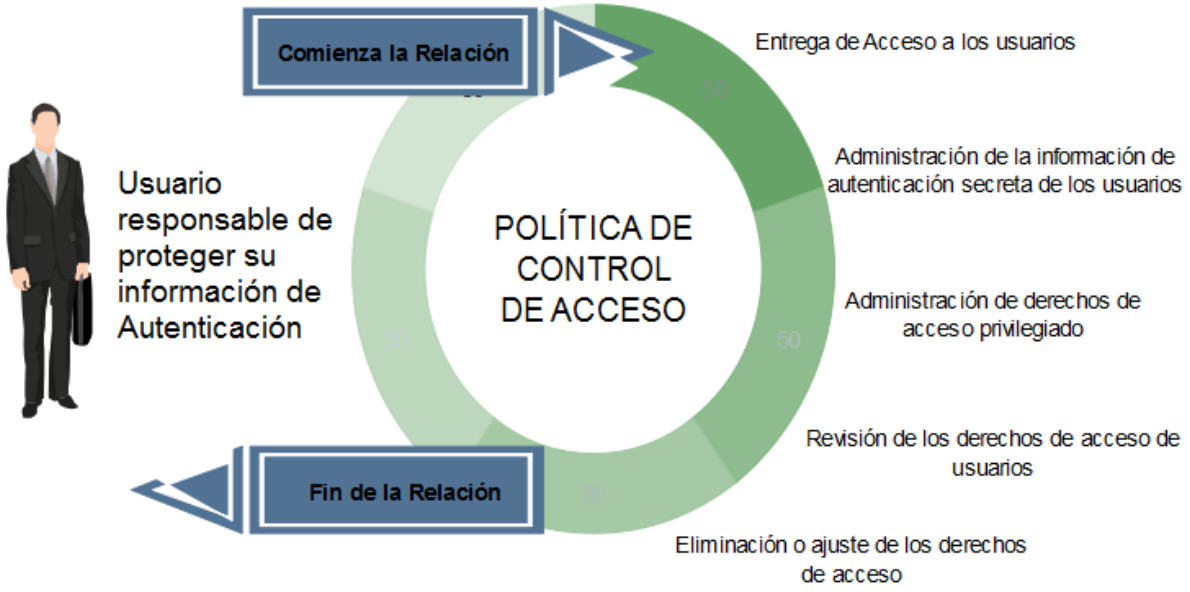


Figura 5.7 Administración de acceso a los usuarios

Fuente: Elaboración propia

La Gerencia junto a Personal de T.I., debería considerar, los siguientes controles:

- ✓ Control de acceso de Sistemas y Aplicaciones, para evitar el acceso no autorizado.
- ✓ Procedimientos de inicio de Sesión Seguros, se debería seleccionar una técnica de autenticación adecuada para corroborar la identidad que un usuario afirma tener. (Más información en el Marco Teórico página 57)
- ✓ Sistema de Administración de Contraseñas, garantizando contraseñas de calidad.
- ✓ Control de acceso al código fuente del programa, incluyendo el mantenimiento y el copiado.

Cada uno de los controles mencionados pueden ser más ampliados para generar mayor control, de acuerdo a la necesidad de la Empresa.

Entre los sistemas y aplicaciones a las cuales el usuario tiene acceso están:

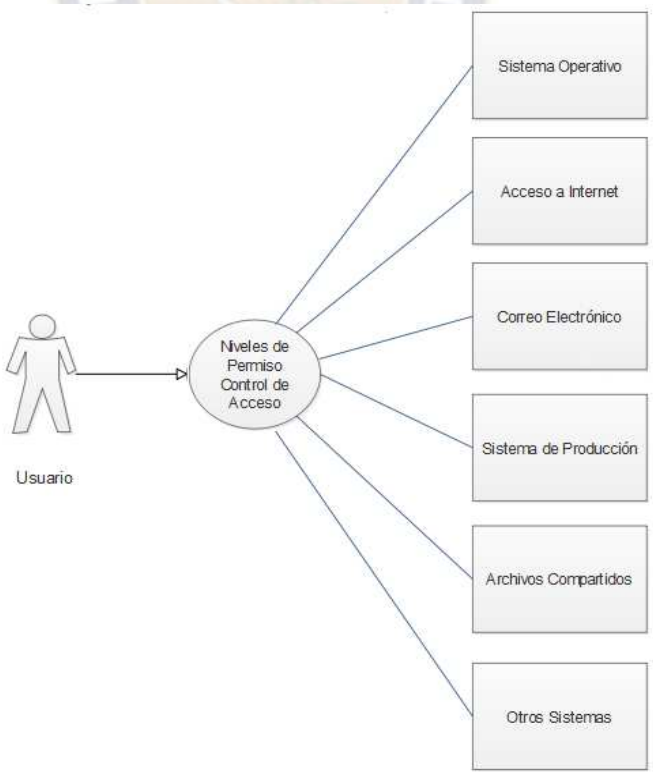


Figura 5.8 Servicios a los que accede un usuario

Fuente: Elaboración propia

Una propuesta para crear un proceso de solicitud de acceso, para un usuario nuevo o cambio de funciones, sería el siguiente:

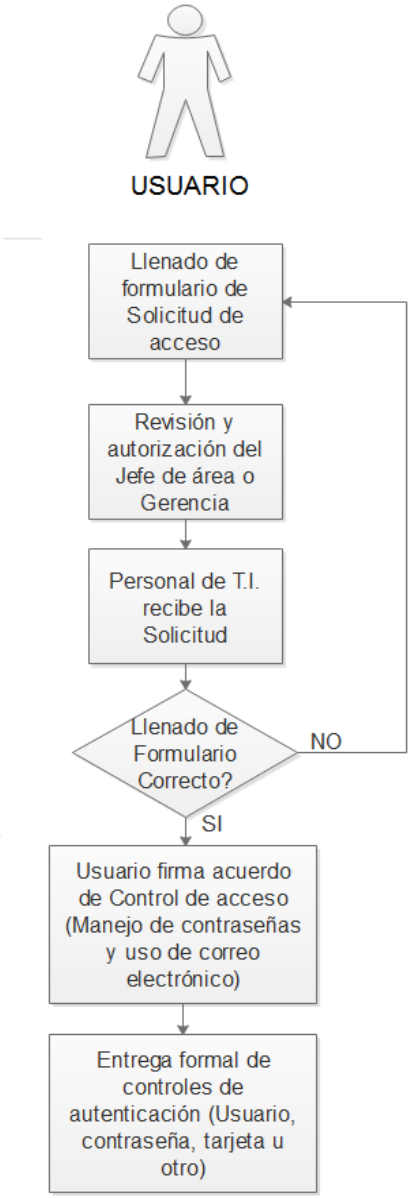


Figura 5.9 Proceso de Solicitud de Acceso por parte del usuario

Fuente: Elaboración propia

Para poder implementar un control de acceso, se debe tomar en cuenta muchos aspectos, las empresas corredores como ya se mencionó están compuestas de 5 a 120 personas, entonces se pueden tener algunas propuestas para este control, como ser:

- ✓ Uso de un Directorio Activo (Active Directory), que es el servicio de directorio de una red con Windows Server. (Más referencia en el marco teórico)
- ✓ Registros físicos de acceso al Centro de Procesamiento de Datos
- ✓ Administración de cuentas locales en Windows, con cuentas de usuario limitadas.
- ✓ Registro de usuarios con el detalle de permisos y privilegios que tiene.
- ✓ Una solución también puede ser acceder a un servicio de Directorio Activo (Active Directory) a través de la nube (por Internet) mediante un proveedor como Azure.

La compra de servidores y las licencias, es una limitante para una empresa pequeña, una posibilidad es montarlo y administrarlo desde la nube, realizando el respectivo estudio técnico económico.

Gerencia debería establecer y conocer los niveles de privilegios que los usuarios tienen a cada uno de los servicios. Así también realizar la capacitación para el personal, sobre seguridad siendo uno de los aspectos fundamentales la información sobre el Control de Acceso.

El control de acceso a los sistemas y aplicaciones es de vital importancia, es un control aplicable, siendo un parámetro de Seguridad que debería ser considerado en todas las empresas corredores independientemente de la cantidad de personal con el que cuente. Podrían tomarse diferentes alternativas de las que se expusieron.

5.6 SEXTO CONTROL. CRIPTOGRAFÍA

El objetivo garantizar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.

Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información. Según el resultado obtenido se puede considerar que el 10% de las empresas corredores de seguros tienen adoptado la criptografía, para proteger la información almacenada (Backup).

La criptografía puede ser utilizada en el proceso de consultas a Bases de Datos, puede ser utilizado para almacenar la información de los backups de servidores, puede utilizarse un DAS o un NAS de acuerdo al tamaño de la información. En el caso específico de las empresas corredoras que utilizan discos externos para guardar los backups, sería recomendable los DAS o NAS con un método de criptografía. Al respecto se puede leer más en el marco teórico, donde se mencionan los Sistemas de almacenamiento de datos digitales. (página 45)

De acuerdo al conocimiento sobre el modo de trabajo de las empresas corredoras se puede indicar que no se utiliza el almacenamiento en la nube, generalmente se almacena backups en discos externos. Por tanto este control, es aplicable solo desde el punto de vista del almacenamiento de los backups. El control de criptografía es el menos conocido, y por tanto está en una fase inicial.

5.7 SÉPTIMO CONTROL. SEGURIDAD AMBIENTAL

El objetivo evitar el acceso físico no autorizado a la información de la empresa y las instalaciones de procesamiento de la información.

Si bien la seguridad Física compete a toda la organización, es decir a todos los ambientes incluyendo oficinas administrativas, se analizará el aspecto de la seguridad física del centro de procesamiento de datos y los equipos de computación. De acuerdo a la norma NB/ISO/IEC 27002, se deberían tomar en cuenta los siguientes aspectos:

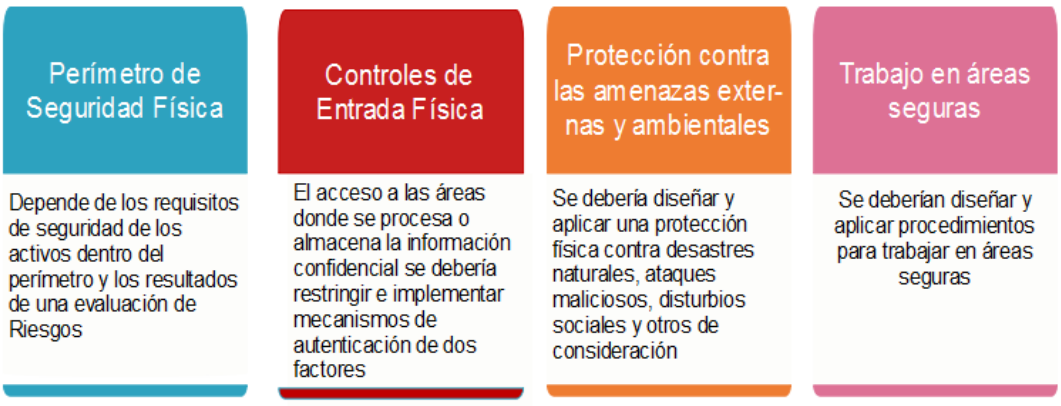


Figura 5.10 Controles en Seguridad Ambiental

Fuente: Elaboración propia basado en norma NB/ISO/IEC 27002

En general un control necesario para la entrada física a los ambientes de una empresa es el área de recepción.

En la protección contra las amenazas externas y ambientales, se pueden tomar en cuenta los extintores, dispositivos de detección de humo, planes de emergencia y evacuación.

En el control de la Protección de oficinas, salas e instalaciones, se presta atención a las instalaciones clave que se deberían ubicar evitando el acceso público. En este punto se puede mencionar a las buenas prácticas de instalación de cableado estructurado.

En el control de Áreas de entrega y carga, en relación con el centro de procesamiento de datos, en muchas ocasiones, los equipos de comunicación, computación, impresoras y otros equipos son entregados por personal externo, se debería evitar el acceso físico a las instalaciones críticas, supervisando en todo momento el trabajo que se realiza.

Equipos. El objetivo evitar la pérdida, los daños, el robo o el compromiso de activos y la interrupción a las operaciones de la empresa. Se consideran los siguientes aspectos:

Figura 5.11 Control en equipos, parte I

Fuente: Elaboración propia basado en norma NB/ISO/IEC 27002

Seguridad del cableado

La mayoría de los edificios cuenta con instalación de cableado eléctrico, ya definida desde la construcción de la edificación, no sucede lo mismo con el cableado de datos, por lo que la instalación se realiza de manera posterior, mediante ductos cuidando la estética de los ambientes, en el mejor de los casos siguiendo las buenas practicas del cableado estructurado que son recomendadas en el estándar ANSI/TIA/EIA 568 B.1, que específica un sistema de cableado genérico para telecomunicaciones para edificios comerciales y admite un entorno de múltiples proveedores y productos. Según esta norma, los elementos que se consideran en el cableado estructurado son:

- ✓ Cableado Vertical (Backbone)
- ✓ Cableado Horizontal
- ✓ Facilidades de Entrada
- ✓ Cuarto de Telecomunicaciones
- ✓ Sala de Equipos
- ✓ Área de trabajo

En muchos casos por razones de espacio, el cuarto de telecomunicaciones y la sala de equipos ocupan el mismo ambiente.

En la Figura 5.12 puede observarse la ubicación de los elementos del cableado estructurado.

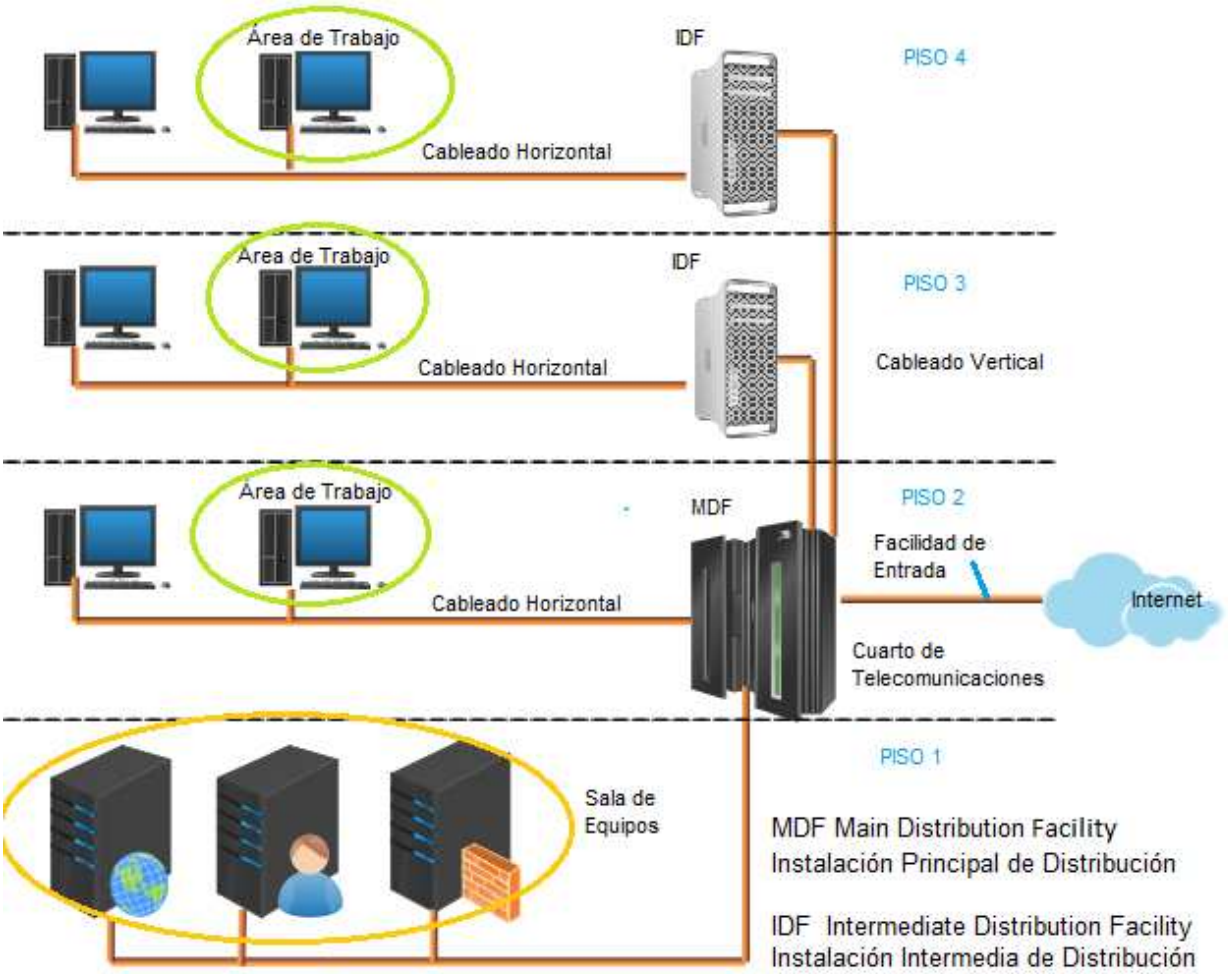


Figura 5.12 Elementos de Cableado Estructurado

Fuente: Elaboración propia

En el estándar ANSI/TIA/EIA 568 B, se explica con detalle las características de cada uno de los elementos que lo conforman.

Actualmente se requiere de un cableado estructurado con cable de categoría 5e con velocidad hasta los 1000 Mbps (1Gbps) o Categoría 6 con una velocidad de 10 Gbps (distancia de 55 m), la elección dependerá mucho del costo, ya que existe una notoria diferencia.

Para poder soportar varios servicios, se requiere de una buena infraestructura de red, que soporte la velocidad y ancho de banda requerido por las aplicaciones.

Otros aspectos a considerar, en la seguridad de los equipos:

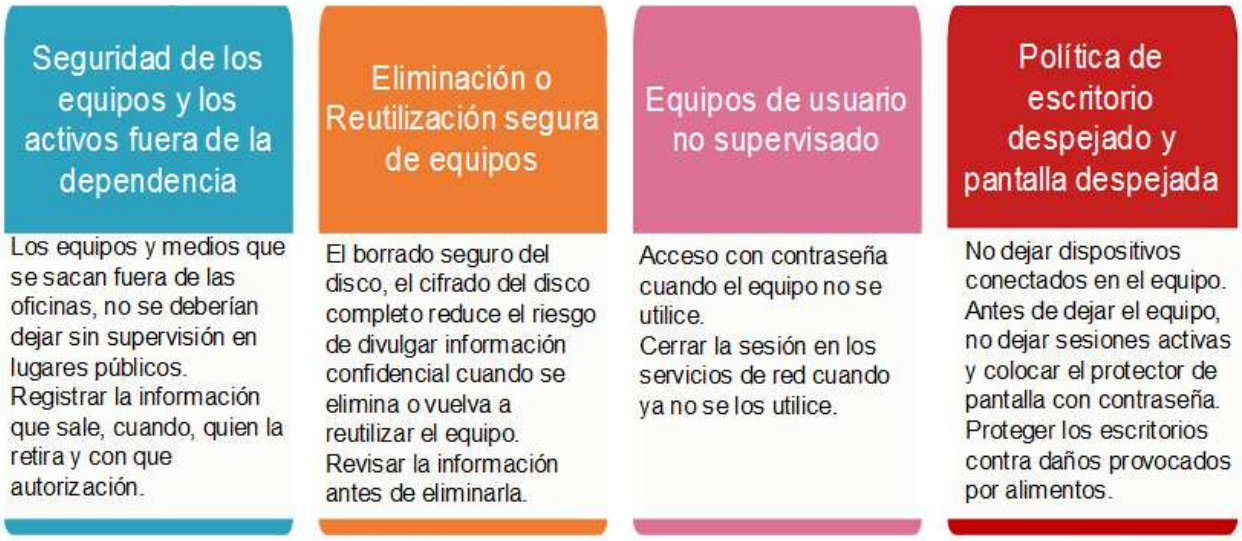


Figura 5.13 Control en equipos, parte II

Fuente: Elaboración propia basado en norma NB/ISO/IEC 27002

La seguridad física, es un control necesario, en todas las empresas corredores de seguros, siendo los controles de seguridad de los equipos bastante sencillos de cumplir y cada una está dirigida a obtener indicadores que puedan establecer lineamientos de seguridad aceptables. Para que sea factible es necesario la capacitación a todo el personal, involucrado con actividades en la empresa, haciendo hincapié en la concientización de cumplimiento con las políticas de seguridad de la información.

Es un control aplicable, con las debidas consideraciones del tamaño de la empresa corredora.

5.8 OCTAVO CONTROL. SEGURIDAD DE LAS OPERACIONES.

Procedimientos y responsabilidades operacionales.

El objetivo es garantizar las operaciones correctas y seguras de las instalaciones de procesamiento de información. Se deberían tomar en cuenta los siguientes aspectos:

Figura 5.14 Control en procedimientos y responsabilidades operacionales

Fuente: Elaboración propia basado en norma NB/ISO/IEC 27002

La separación de entornos de desarrollo, pruebas y operacionales corresponde a las empresas que tienen personal de T.I. que desarrolla software.

Todos los procedimientos operativos, descritos deberían estar documentados, ya que serán parte de los lineamientos de seguridad que se siguen en la Empresa.

Administración de cambios para documentos, el registro de los tiempos que se planifican para realizar tareas como ser la elaboración del documento de "Política de control de acceso", para tal efecto se deberá realizar un seguimiento, con las tareas principales de elaborar, revisar y aprobar, un ejemplo sería el siguiente:

Tareas	Fecha de inicio	Fecha completada	Responsable
Elaboración	20/08/2019	30/08/2019	Firma Personal T.I.
Revisión	30/08/2019	03/09/2019	Firma Jefe de T.I.
Aprobación	03/09/2019	04/09/2019	Firma Gerencia

Tabla 5.3 Control de Cambios para documentos de T.I.

Fuente: Elaboración propia

El detalle de la *Tabla 5.3*, será parte de la caratula de cualquier documento del área de T.I., siendo un parámetro importante donde se observa el control de cambios y posee las firmas correspondientes de los responsables, para realizar el respectivo seguimiento y también es útil en la comprensión del documento.

En la seguridad de las operaciones, se consideran los aspectos de protección contra el malware, respaldo para brindar protección contra la pérdida de datos, control de software operacional y las consideraciones sobre la auditoria de los sistemas de información, en el siguiente gráfico se puede observar los controles que pueden ser implementados para abordar estos puntos:

Figura 5.15 Control en seguridad de las operaciones

Fuente: Elaboración propia basado en norma NB/ISO/IEC 27002

Respaldo. El respaldo o backup, es una tarea fundamental, que toda empresa debe realizar siguiendo las siguientes pautas:

- Elaborar una política de respaldo que debería definir requisitos de retención, protección y comprobación.

- Registrar de forma precisa las copias de respaldo que se hacen.
- Documentar el proceso de restauración basado en las copias de respaldo.
- Los respaldos deberían estar protegidos por cifrado en caso de alta confidencialidad.

Un ejemplo de registro para el seguimiento de copias de respaldo o backups sería el siguiente:

Nº	AREA	TAMAÑO DE BACKUP COMPLETO	PERIODO
PRIMER SEGUIMIENTO			
1	ADMINISTRACIÓN	145,00 GB	enero-abril
2	TECNOLOGÍAS DE LA INFORMACIÓN	452,20 GB	enero-abril
3	RECURSOS HUMANOS	234,00 GB	enero-abril
SEGUNDO SEGUIMIENTO			
1	ADMINISTRACIÓN	285,00 GB	mayo-agosto
2	TECNOLOGÍAS DE LA INFORMACIÓN	631,20 GB	mayo-agosto
3	RECURSOS HUMANOS	317,00 GB	mayo-agosto
TERCER SEGUIMIENTO			
1	ADMINISTRACIÓN	392,00 GB	septiembre-diciembre
2	TECNOLOGÍAS DE LA INFORMACIÓN	764,30 GB	septiembre-diciembre
3	RECURSOS HUMANOS	468,00 GB	septiembre-diciembre

Tabla 5.4 Registro de seguimiento de las copias de Backups

Fuente: Elaboración propia

En este ejemplo se puede observar como se ha incrementado el tamaño de los backups en los periodos comprendidos de cuatro meses, permite determinar a futuro el espacio en disco que se requiere, también se puede observar algunos aspectos irregulares en el crecimiento del backup.

Este registro de seguimientos establecerá indicadores que ayudaran a la toma de decisiones en el área de Tecnologías de Información.

Registro y monitoreo

El objetivo registrar eventos y generar evidencia, para lo cual se consideran los siguientes aspectos:

Figura 5.16 Control en registro y monitoreo

Fuente: Elaboración propia basado en norma NB/ISO/IEC 27002

Registro de eventos

Los registros de eventos son una base importante del seguimiento de incidentes informáticos, para lo cual se puede recurrir a la norma ISO 27035 Gestión de Incidentes de Seguridad de la Información, para más información.

El siguiente registro de eventos, tiene parámetros que pueden ser obtenidos del administrador de eventos del sistema operativo Windows, en este caso personal de T.I. definirá que eventos rutinarios del servidor pueden ser registrados y guardados.

Tipo de Evento	ID de evento	Fuente	Log	Fecha y hora	Nombre usuario	Nombre equipo	Dirección IP	Otros

Tabla 5.5 Ejemplo de Registro de Eventos

Fuente: Elaboración propia

La norma NB/ISO/IEC 27002, recomienda registrar: Intentos de accesos al sistema exitosos y rechazados, intentos de acceso a los recursos, cambios a la configuración del sistema, uso de privilegios, uso de utilidades y aplicaciones del sistema

En este punto se requiere definir y estudiar los equipos sensibles de los cuales se registraran los eventos, en general serán los equipos servidores.

En el caso de tratarse de una red de computadoras compleja compuesta por más de diez equipos es preferible contar con un software especializado, el cual administre los registros de eventos.

Es un control aplicable, sin embargo algunos controles implican la generación de registros, que pueden ocasionar la demora de algunas actividades rutinarias, por lo que debe ser detallado para su implementación, siendo modificado mediante una iteración de mejora continua.

5.9 NOVENO CONTROL. SEGURIDAD DE LAS COMUNICACIONES

Administración de la Seguridad de Redes

El objetivo garantizar la protección de la información en las redes y sus instalaciones de procesamiento de información de apoyo. Se consideran los siguientes aspectos:

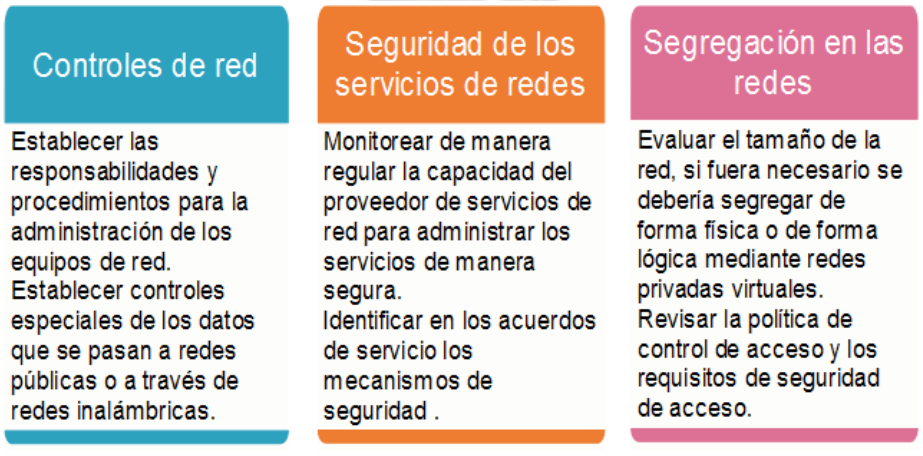


Figura 5.17 Control en administración de la seguridad de redes
Fuente: Elaboración propia basado en norma NB/ISO/IEC 27002

Controles de red. Los controles en las redes están constituidos por varias herramientas la principal un Firewall o cortafuegos que puede ser físico o lógico. Existen muchas opciones al respecto la mejor elección dependerá de un análisis técnico y económico.

Las conexiones inalámbricas que son empleadas en todas las empresas, requieren de controles especiales, para lo cual se puede adquirir algunas soluciones que ofrecen los proveedores de Antivirus, servicios como: Red Wi-fi protegida, cifrado de archivos y fotos entre otros.

Para los entornos sensibles, se debería tener consideración de tratar a los accesos inalámbricos como conexiones externas. (NB/ISO/IEC 27002, 2014)

Transferencia de Información

El objetivo mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa. Para lo cual se consideran los siguientes aspectos:

Figura 5.18 Controles sobre la transferencia de la información
Fuente: Elaboración propia basado en norma NB/ISO/IEC 27002

En las empresas corredoras un 75% se consideran de tamaño pequeño, por tanto sus redes LAN también son pequeños, en consiguiente los procedimientos de controles de

accesos y permisos, pueden conseguir una adecuada seguridad en la transferencia de información dentro la empresa.

El uso de las técnicas de criptografía en la transferencia de información, no serían recomendables ya que podría provocar un desmedro de la capacidad en una red local de pocos equipos. En el caso particular de las VPN, este control escapa de las manos ya que el proveedor es el encargado de garantizar la seguridad en la transferencia de la información, sin embargo como característica técnica se puede obtener información sobre las técnicas de criptografía que se utiliza, además de tener un contrato que aborde los temas de seguridad en la transferencia de la información. Es un control aplicable, ciertos controles específicos pueden ser estudiados particularmente por la empresa corredora. La seguridad en las redes debe estar presente en todo nivel comenzando desde el cableado, terminando en las aplicaciones, como ser los firewalls y programas de monitoreo.

5.10 DÉCIMO CONTROL. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Requisitos de seguridad de los sistemas de información. El objetivo garantizar que la seguridad de la información sea una parte integral de los sistemas de información en todo el ciclo de vida. Considerando los siguientes aspectos:

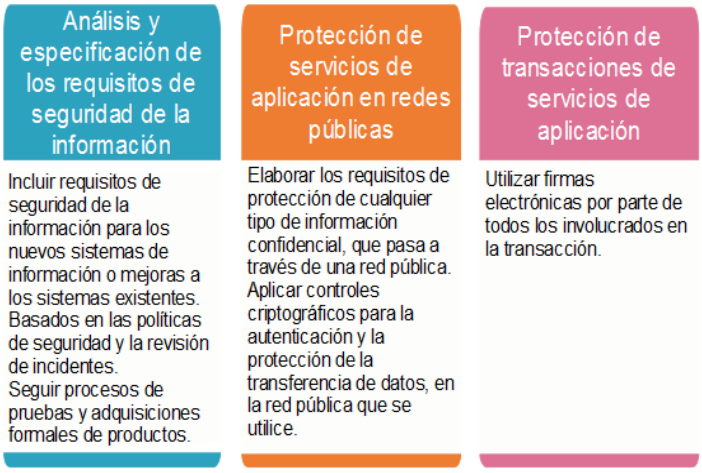


Figura 5.19 Control en requisitos de seguridad de los sistemas de información

Fuente: Elaboración propia basado en norma NB/ISO/IEC 27002

El control de protección de transacciones de servicios de aplicación, no es aplicable a las empresas corredoras a nivel general ya que aún no se realizan transacciones por lo que tan poco se utilizan firmas electrónicas.

Seguridad en los procesos de desarrollo y soporte

El objetivo garantizar que la seguridad de la información se diseñe e implemente dentro del ciclo de vida de desarrollo de los sistemas de información. Considerando los siguientes aspectos.

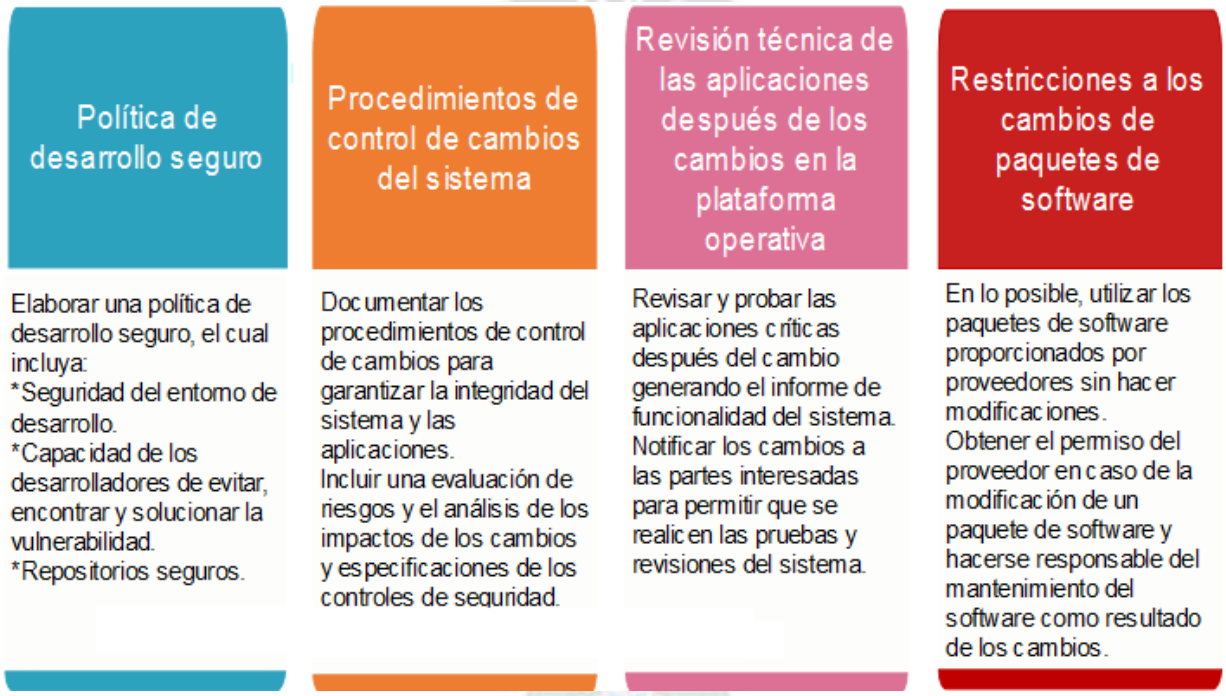


Figura 5.20 Controles sobre la seguridad en los procesos de desarrollo y soporte. Parte I

Fuente: Elaboración propia, basado en la norma NB/ISO/IEC 27002

En el siguiente figura se tiene una propuesta de un procedimiento de control de cambios del sistema:

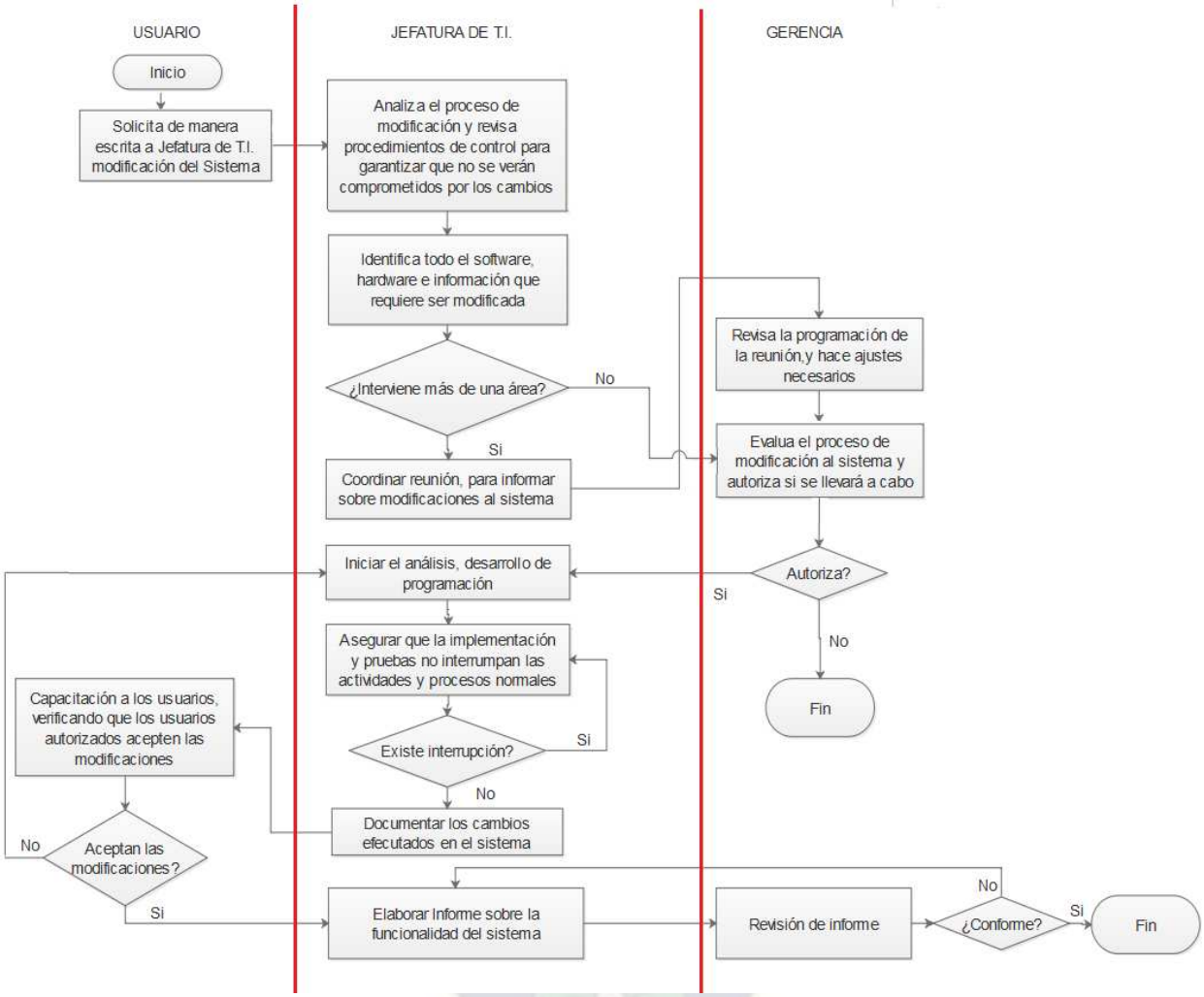


Figura 5.21 Procedimiento de control de cambios del sistema

Fuente: Elaboración propia

El cambio de software puede generar un impacto en el entorno operacional y viceversa. Las buenas prácticas incluyen las pruebas de nuevo software en un entorno segregado de los entornos de producción y desarrollo. (*NB/ISO/IEC 27002, 2014*)

Los siguientes controles, serán mencionados de forma superficial, ya que según los resultados que se tiene en la entrevista, solamente un 10% de las empresas corredores tiene personal de TI que desarrollan software. Sin embargo se considera importante el control de Desarrollo Externalizado, ya que un 90 % utiliza aplicaciones que han sido desarrolladas por proveedores externos.

Continuando con los aspectos de la Seguridad en los procesos de desarrollo y soporte, se consideran los siguientes controles:

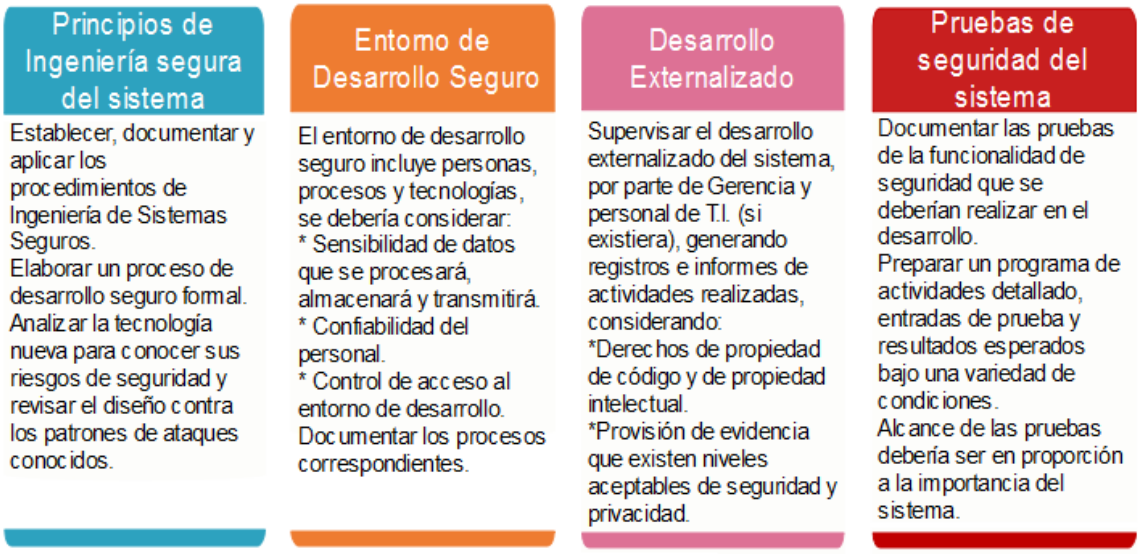


Figura 5.22 Controles sobre la seguridad en los procesos de desarrollo y soporte. Parte II

Fuente: Elaboración propia, basado en la norma NB/ISO/IEC 27002

Se observa que en el aspecto de desarrollo externalizado, se distinguen dos:

- Los desarrolladores externos que son personas independientes, y sus costos son relativamente accesibles, en muchos casos se trabaja de manera informal.
- Los desarrolladores externos son empresas legalmente constituidas que tienen costos elevados, la ventaja se trabaja de manera formal.

En el control de desarrollo externalizado, existen varios controles que son importantes sin embargo considerando los aspectos mencionados, seguir acuerdos con cierto tipo de requerimientos como ser:

- ✓ La solicitud de provisión de evidencia de que se han aplicado pruebas suficientes para protegerse contra la presencia de vulnerabilidades conocidas.
- ✓ El derecho contractual para auditar procesos y controles de desarrollo.

La inclusión en un contrato de estos requerimientos, hace difícil un acuerdo entre partes, lo más factible es documentar cada una de las etapas de desarrollo y solicitar la garantía correspondiente del desarrollador externo. Este aspecto se lo analizará también en el siguiente control Relaciones con el Proveedor.

Un control imprescindible es la Prueba de Aceptación del Sistema siendo que las pruebas se deberían realizar en un entorno de pruebas realista para garantizar que el sistema no introducirá vulnerabilidades al entorno de la empresa y que las pruebas sean confiables. (NB/ISO /IEC 27002, 2014)

Los datos de pruebas se deberían seleccionar cuidadosamente, evitando el uso de datos que contienen información confidencial como ser la información personal identificable. Debería existir una autorización cada vez que se copia la información operacional a un entorno de prueba. Y una vez finalizada la prueba, los datos de prueba deberían ser borrados.

Un dato importante para el desarrollo seguro de los sistemas y aplicaciones es tomar en cuenta OWASP (acrónimo de Open Web Application Security Project) que es el Proyecto Abierto de Seguridad en Aplicaciones Web, es una comunidad abierta dedicada a permitir que las organizaciones desarrollen, adquieran y mantengan aplicaciones y APIs en las que se pueda confiar. Es un buen comienzo en el camino de seguridad de las aplicaciones.

Otro aspecto importante para poder evaluar los controles de seguridad en los procesos de desarrollo y soporte es realizar evaluaciones de vulnerabilidad y pruebas de penetración mediante el Ethicalhacking.

En los resultados de la entrevista se ha podido determinar que el 70% de las empresas considera que el Sistema de producción es el más importante para el trabajo diario. A continuación describiremos las características generales de este sistema.

CARACTERÍSTICA DEL SISTEMA DE PRODUCCIÓN EN LAS CORREDORAS DE SEGUROS

El Sistema de Producción de las empresas corredores de seguros tiene la característica de ser un software que permite administrar la gestión y administración de los clientes de la empresa, contando con una base de datos sobre las compañías de seguros que tengan producción en la Empresa Corredora.

Como parámetro importante se cuenta con los nombres de las Compañías de Seguros que tienen producción en la Empresa, entre estas compañías, se pueden citar:

- ALIANZA VIDA SEGUROS Y REASEGUROS S.A.
- ALIANZA COMPAÑIA DE SEGUROS Y REASEGUROS S.A. E.M.A.
- BISA SEGUROS Y REASEGUROS S.A.
- BUPA INSURANCE (BOLIVIA) S.A.
- COMPAÑIA DE SEGUROS Y REASEGUROS FORTALEZA S.A.
- CREDISEGURO S.A. SEGUROS GENERALES
- LA BOLIVIANA CIACRUZ DE SEGUROS Y REASEGUROS S.A.
- LA VITALICIA SEGUROS Y REASEGUROS DE VIDA S.A.
- NACIONAL SEGUROS PATRIMONIALES Y FIANZAS S.A.
- NACIONAL SEGUROS VIDA Y SALUD
- SANTA CRUZ VIDA Y SALUD SEGUROS Y REASEGUROS PERSONALES S.A.
- SEGUROS PROVIDA S.A.
- SEGUROS Y REASEGUROS PERSONALES UNIVIDA S.A.
- SEGUROS Y REASEGUROS CREDINFORM INTERNATIONAL S.A.
- SEGUROS ILLIMANI S.A.
- SEGUROS Y REASEGUROS PERSONALES UNIVIDA S.A.

Figura 5.23 Compañías de Seguros en Bolivia (No se encuentran citadas todas)
Fuente: Elaboración propia, con los datos de la APS (2019)

También un sistema de producción puede tener almacenado como información el registro de los ramos que cubre el seguro, registrados en la compañía. Los ramos

pueden ser diferentes en cada compañía. Ejemplo de ramos: Accidentes personales, Incendio, Maquinaria, Salud entre otros.

La característica principal del sistema de producción de una corredora de seguros es el manejo de Número de Poliza.

Así mismo el sistema debe cumplir con algunos formatos que son requeridos por la Autoridad de Fiscalización y Control de Pensiones y Seguros (APS) y la Unidad de Investigaciones Financieras (UIF).

Los sistemas de producción que han sido desarrollados en la misma empresa son totalmente adecuados a su entorno, por lo que pueden cubrir todas las necesidades de las áreas que requieren utilizar el sistema, como ser cobranzas, reclamos entre otros.

Es un control que se puede aplicar, de acuerdo a las características específicas de las empresas corredoras, sin embargo se reconoce que algunos controles sobre desarrollo de software se pueden aplicar solamente al 10% de las empresas corredoras.

5.11 DÉCIMO PRIMER CONTROL. RELACIONES CON LOS PROVEEDORES

Seguridad de la información en las relaciones con los proveedores.

El objetivo es garantizar la protección de los activos de la empresa accesibles a los proveedores. Para lo cual se consideran los siguientes aspectos:

Figura 5.24 Controles sobre Seguridad de la información en las relaciones con los proveedores

Fuente: Elaboración propia, basado en la norma NB/ISO/IEC 27002

Administración de prestación de servicios de proveedores

El objetivo es de mantener un nivel acordado de seguridad de información y prestación de servicios conforme a los acuerdos del proveedor. (*NB/ISO/IEC 27002, 2014*)

Considerando los siguientes aspectos más relevantes:

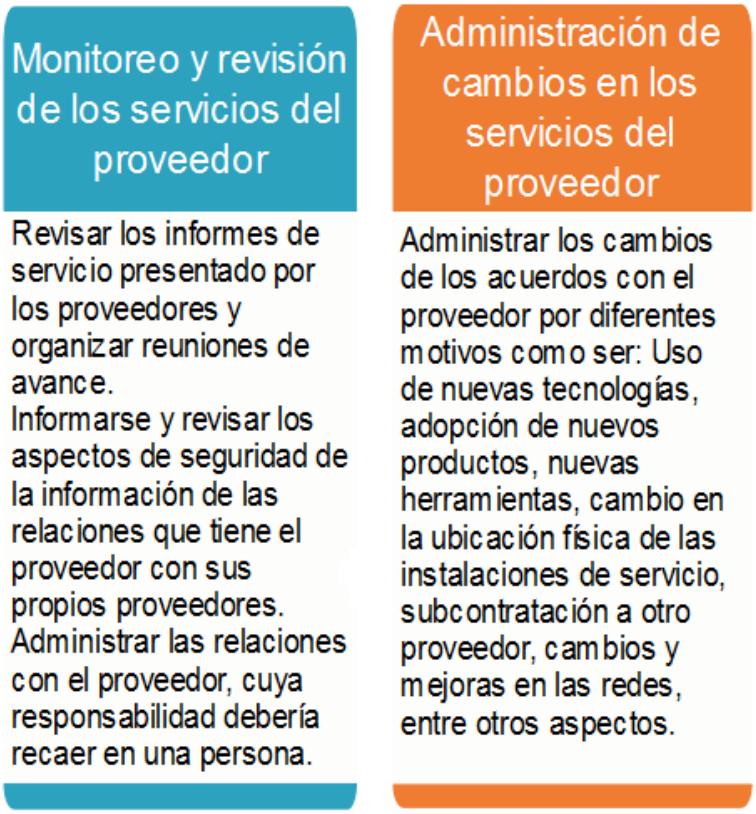


Figura 5.25 Controles sobre administración de prestación de servicios de proveedores
Fuente: Elaboración propia, basado en la norma NB/ISO/IEC 27002

Existen dos controles, aunque son necesarios, en el entorno en el cual hoy en día se realizan los acuerdos con los proveedores, es complejo obtenerlos, es el caso de:

- ✓ Revisar los aspectos de seguridad de la información de las relaciones que tiene el proveedor con sus proveedores.
- ✓ Solicitar al proveedor el plan de trabajo, para garantizar que el servicio continuará, a pesar de la ocurrencia de fallas o desastres.

Siendo muchas veces aspectos que causan susceptibilidad al proveedor, más aún si la relación con el proveedor no es directamente con personal de jerarquía. Es el caso de los proveedores del servicio de Internet.

Como parte del control de monitoreo una buena práctica es elaborar un registro de bitácora de acceso de los proveedores de Tecnologías de Información y Comunicación.

El control es Aplicable, pero asumiendo las características de los proveedores con los que se relaciona la empresa corredora, puede ocurrir que no se pueda cumplir a cabalidad todos los controles mencionados.

5.12 DÉCIMO SEGUNDO CONTROL. ADMINISTRACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Administración de incidentes y mejoras de seguridad en la información

El objetivo garantizar un enfoque coherente y eficaz a la administración de incidentes de seguridad de la información, incluida la comunicación sobre los eventos y las debilidades de seguridad. (*NB/ISO/IEC 27002, 2014*)

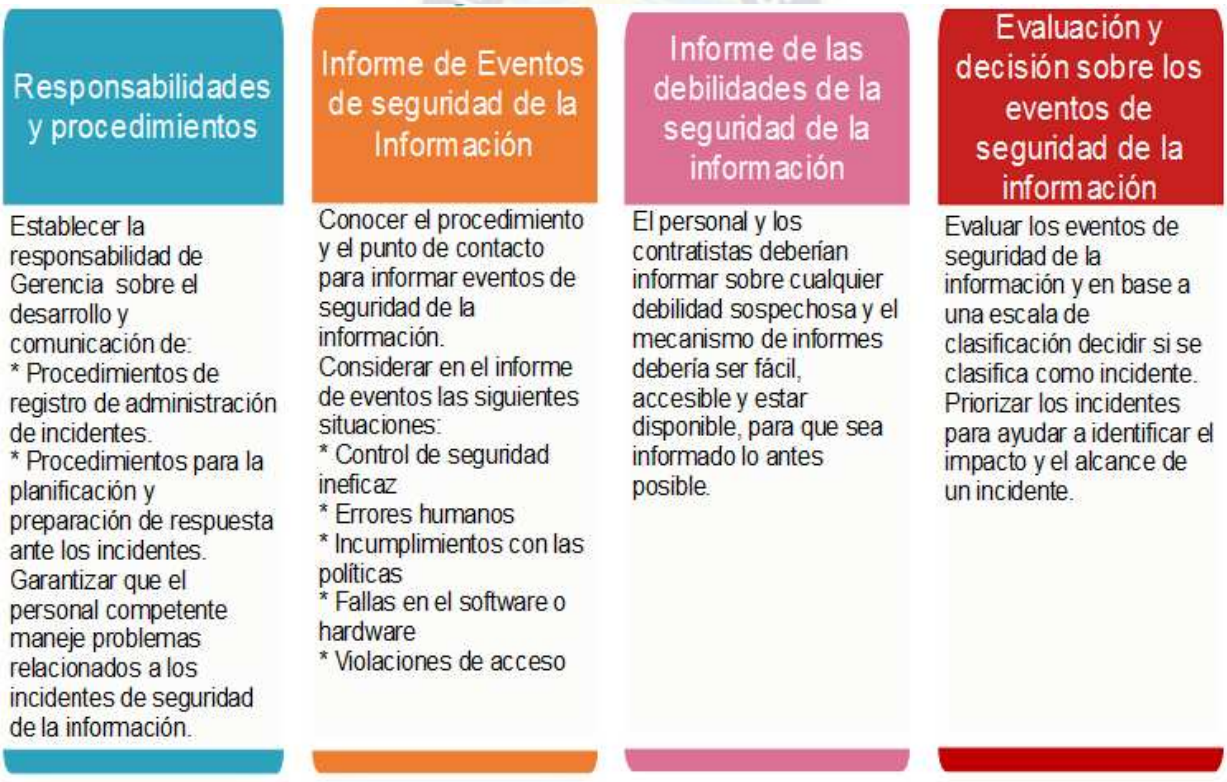


Figura 5.26 Controles sobre administración de incidentes y mejoras de seguridad en la información. Parte I

Fuente: Elaboración propia, basado en la norma NB/ISO/IEC 27002

La ocurrencia de un incidente debería registrarse, a continuación se tiene una propuesta de registro de incidente:

Vigencia 01/01/2020	Identificación de la Empresa	Código: REG-SEG-01-01

Ubicación (Oficina)	Fecha y hora	Equipo afectado	Procesos afectados	Sistemas afectados	Persona quien informa	Descripción de Incidente

Figura 5.27 Registro de Incidentes

Fuente: Elaboración Propia

La fecha de vigencia indica, la fecha desde la cual se encuentra en vigencia el Registro.

Donde: **REG-SEG-01-1** Significa Registro de Seguridad Número 01 versión 1

La propuesta de registro que se muestra puede ser utilizado tal como está o modificado de acuerdo a la necesidad de la empresa, por lo que con el tiempo se llegará a modificar y existirán diferentes versiones las cuales también deben ser controladas, una vez que se le de utilidad al registro, se puede llegar a sistematizarlo, como parte de un sistema.

El incidente puede informarlo todo el personal de la Empresa, a través del llenado de este registro, para lo cual se requiere una capacitación previa. A partir de este registro personal de T.I. puede realizar el Informe de Incidentes dirigido hacia Gerencia.

Continuando con los aspectos que se deberían considerar para la administración de incidentes y mejoras de seguridad en la información, se consideran:

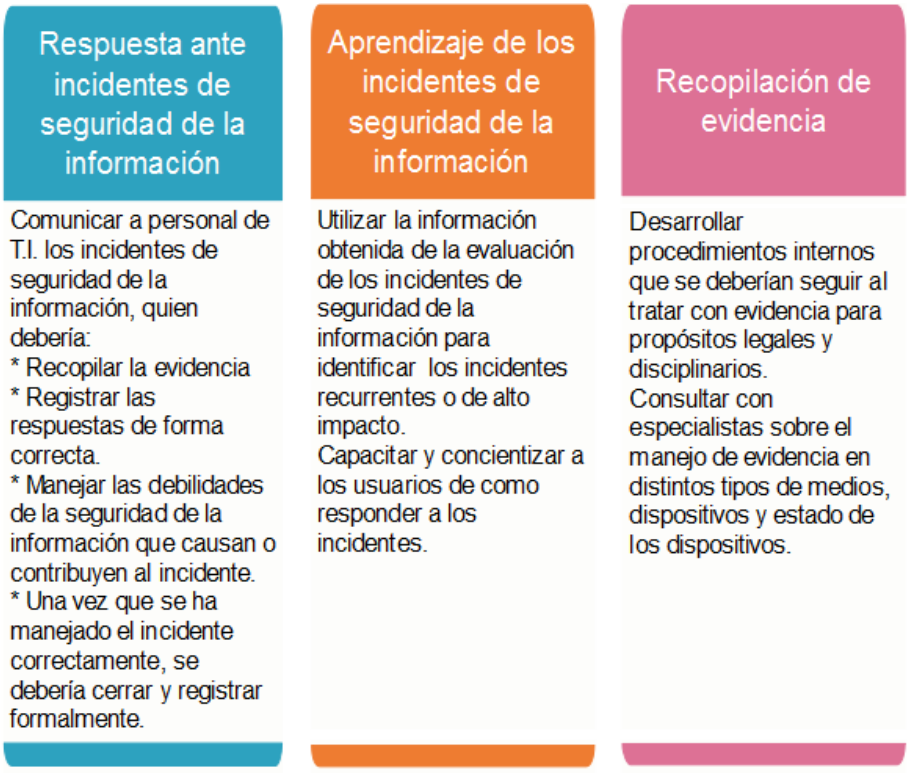


Figura 5.28 Controles sobre administración de incidentes y mejoras de seguridad en la información. Parte II

Fuente: Elaboración propia, basado en la norma NB/ISO/IEC 27002

Siendo el control de Administración de Incidentes de Seguridad de la Información, bastante importante y amplia se proporciona más orientación en la norma ISO/IEC 27035 Gestión de incidentes de Seguridad de la información.

Así también la norma ISO/IEC 27037 brinda orientación para la identificación, la recopilación, la adquisición y la preservación de evidencia digital.

Es un control que aún no puede ser aplicable, por el contexto de las Empresas Corredoras. La cultura sobre el tema de seguridad de la información es escasa y no es asumida de manera responsable, por lo que el control de la Administración de Incidentes, está muy lejos de implementarse.

5.13 DÉCIMO TERCER CONTROL. ASPECTOS DE LA SEGURIDAD DE LA INFORMACIÓN DE LA ADMINISTRACIÓN DE LA CONTINUIDAD DEL NEGOCIO

Continuidad de la seguridad de la información

El objetivo es integrar en los sistemas de administración de continuidad del negocio o comercial la continuidad de la seguridad de la información. Para lo cual se consideran los siguientes aspectos:

Figura 5.29 Controles sobre Continuidad de la Seguridad de la Información
Fuente: Elaboración propia, basado en la norma NB/ISO/IEC 27002

En muchos casos no se cuenta con un plan de continuidad del negocio y en otros casos, se encuentran en fases iniciales, por lo cual es difícil hablar de la continuidad de seguridad de la información en el plan de continuidad del negocio.

Redundancia. Mediante la redundancia se garantiza la disponibilidad de las instalaciones de procesamiento de información, en el caso específico de la empresas corredores de seguros que tienen personal de T.I. externo una opción, será el de contar con la redundancia en un equipo de computación con el software necesario y los últimos backups, para poder trabajar en un lugar alterno en caso de contingencia. En la siguiente Figura 5.30 se puede esquematizar el proceso de utilizar un plan de continuidad del negocio, el cual será más amplio y complejo de acuerdo con el análisis de entorno de la Empresa.

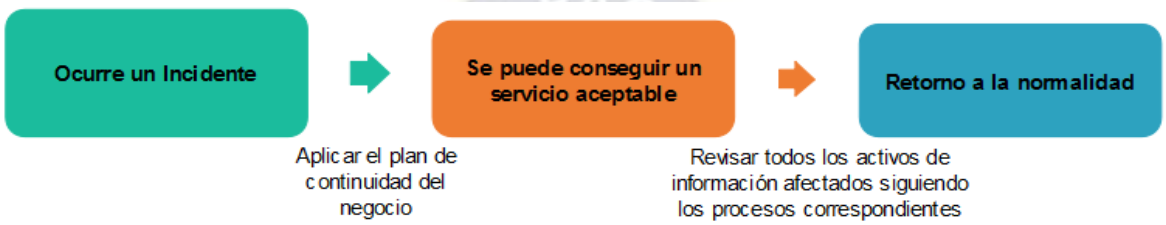


Figura 5.30 Proceso de continuidad del negocio

Fuente: Elaboración propia

El reconocimiento de los activos de información, las actividades que conllevan el análisis de impacto de incidencia, son parte de la Gestión de Riesgo en la Seguridad de la Información, la cual será útil para la elaboración de un plan de continuidad del negocio que incluya un plan de Contingencia Tecnológico.

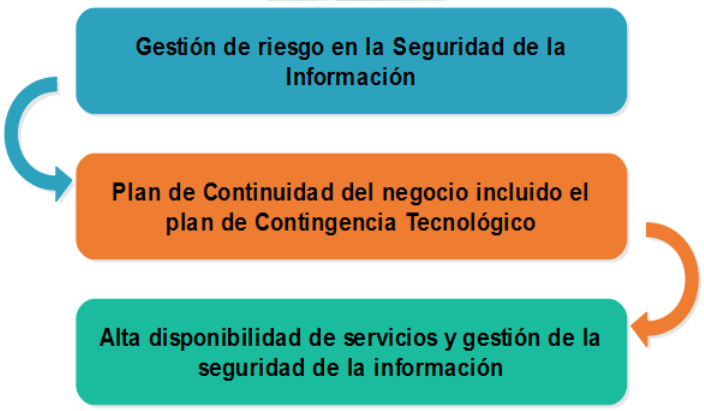


Figura 5.31 Gestión de Seguridad de la información en el Plan de Continuidad del Negocio

Fuente: Elaboración propia

En el Anexo 4. Se propone un esquema de Plan de Continuidad del Negocio.

La continuidad de la seguridad de la información en el plan de continuidad del negocio es un tema que aún no está desarrollado, según entrevista. Solamente un 25% se puede considerar que ha previsto el aspecto de la seguridad de la información en una fase inicial. Es un aspecto que todavía no puede ser analizado, ya que en las empresas que no se considera a la seguridad de la información como una necesidad y no existe ni un plan de contingencias tecnológico, entonces no se puede hablar aún de este tema.

No es aplicable como tal, ya que la elaboración de un documento de Continuidad del Negocio, es compleja y debe ser desarrollado por personal capacitado, con el apoyo de Gerencia, donde debe participar todo el personal. El control implica incluir los aspectos de la Seguridad de la Información en el Documento de Continuidad del Negocio.

5.14 DÉCIMO CUARTO CONTROL. CUMPLIMIENTO

Cumplimiento con los requisitos legales y contractuales

El objetivo es evitar incumplimientos a las obligaciones legales, estatuarias, normativas o contractuales relacionadas a la seguridad de la información y a cualquier requisito de seguridad. (NB/ISO/IEC 27002, 2014)

Considerando los siguientes aspectos:

Figura 5.32 Controles sobre Cumplimiento con los requisitos legales y contractuales
Fuente: Elaboración propia, basado en la norma NB/ISO/IEC 27002

Las empresas corredores de seguros y reaseguros están reguladas por la APS, de acuerdo a la Resolución Administrativa IS Nº 1025/05 del 18 de noviembre de 2005 y según la última circular APS/DS/JCF 153 – 2017 Alcance Mínimo para la Realización de Auditorías Externas – Gestión 2017 donde en el numeral 5 trata sobre Tecnología de Información que solicita a la Auditora Externa Evaluar y emitir opinión sobre los controles de los sistemas informáticos y de procesamiento de datos adoptados y/o desarrollados por la Entidad. Aunque aún no se ha determinado utilizar la norma ISO 27001, es una referencia importante para realizar una evaluación en el área de gestión de seguridad de la información.

El derecho intelectual es muy importante, especialmente para las empresas corredores, que tienen personal de T.I. y desarrollan software, se debería ver el tema de propiedad intelectual.

La protección de registros, también se debería contemplar, ya que todos los documentos generados por el área de T.I. deberían ser resguardados por un tiempo prudente.

El Control de regulaciones de controles criptográficos no es aplicable a las Empresas Corredores ya que no se realizan tareas de importación o exportación de hardware y software informático para realizar funciones criptográficas.

Revisiones de la seguridad de la información

El objetivo garantizar que se implementa y opera la seguridad de la información de acuerdo a las políticas y procedimientos organizacionales. (NB/ISO/IEC 27002, 2014)

Considerando los siguientes aspectos:

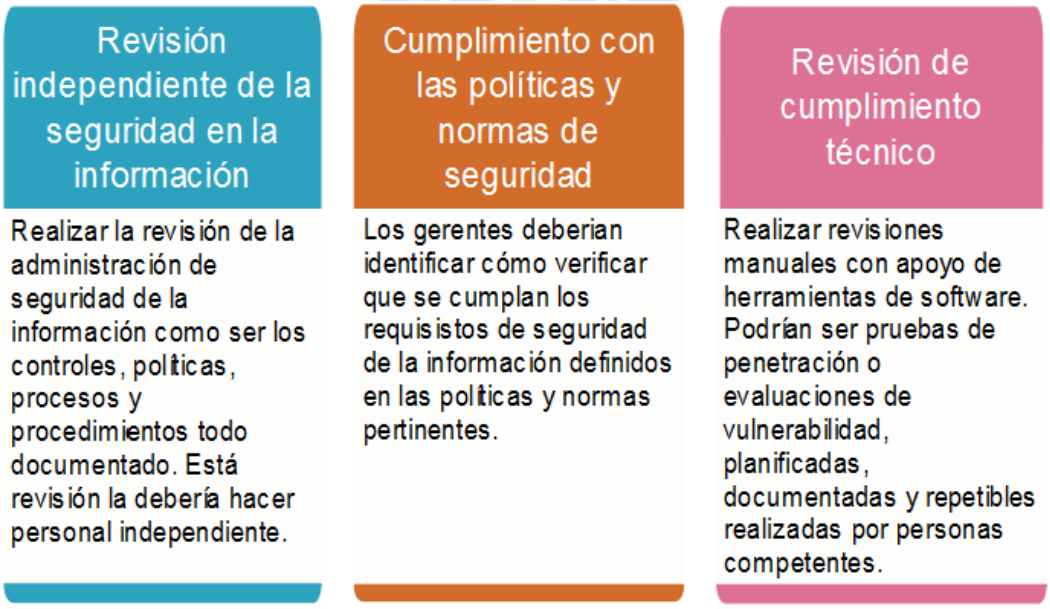


Figura 5.33 Controles sobre Revisiones de la seguridad de la información
Fuente: Elaboración propia, basado en la norma NB/ISO/IEC 27002

La revisión de todos los documentos que forman parte de la seguridad de la información, puede ser planificada de forma anual, juntamente con la auditoria externa.

Siendo base el documento de políticas de seguridad de la información, es prudente llevar el control de cambios indicando las modificaciones efectuadas con las fechas y firmas correspondientes, de forma anual.

La realización de pruebas de penetración, se puede aplicar a aproximadamente el 25% de las empresas corredoras, que cuentan con sistemas robustos, y tienen las condiciones técnicas, para realizar dichas pruebas. En el resto de las empresas que son el 75% podría estudiarse otros métodos por los cuales evaluar el cumplimiento técnico del software y la red.

Es aplicable en los controles dirigidos al documento de políticas de seguridad, puesto que las corredoras de seguros y reaseguros son empresas privadas, que cuentan con políticas, contratos y acuerdos. Además que son fiscalizados por la APS.

CAPITULO 6

6. GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN APLICADO A EMPRESAS CORREDORAS DE SEGUROS Y REASEGUROS QUE OPERAN EN LA PAZ BOLIVIA

Este Capítulo, permitirá al personal del área de TI, desarrollar una metodología de Gestión de Riesgos en la Seguridad de la Información apropiada para los requerimientos del negocio, que pueda mostrar a la Gerencia de la empresa corredora, a los tipos de amenazas informáticas que se exponen y del porque implementar controles basados en los riesgos altos encontrados.

Para comenzar se elige una metodología de evaluación del riesgo apropiada para los requerimientos del negocio. Existen numerosas metodologías estandarizadas de evaluación de riesgos. Aquí explicaremos la metodología sugerida en la Norma NB/ISO/IEC 27005, siguiendo con la familia de normas ISO 27000.

En el establecimiento del contexto, se analiza a las empresas corredoras de seguros y no así a las empresas corredoras de reaseguros, ya que el contexto de este último es diferente y el análisis también requiere de otras consideraciones, como ser la identificación de partes interesadas y el mismo sistema informático que debe cubrir otras necesidades específicas. A partir de la valoración del riesgo, se pueden generalizar algunos criterios que pueden ser adaptados de acuerdo al enfoque de las empresas Corredores de Reaseguros.

El proceso de gestión del riesgo en la seguridad de la información consta del establecimiento del contexto, valoración del riesgo, tratamiento del riesgo, aceptación del riesgo, comunicación del riesgo y monitoreo y revisión del riesgo. (NB/ISO/IEC 27005, 2010)

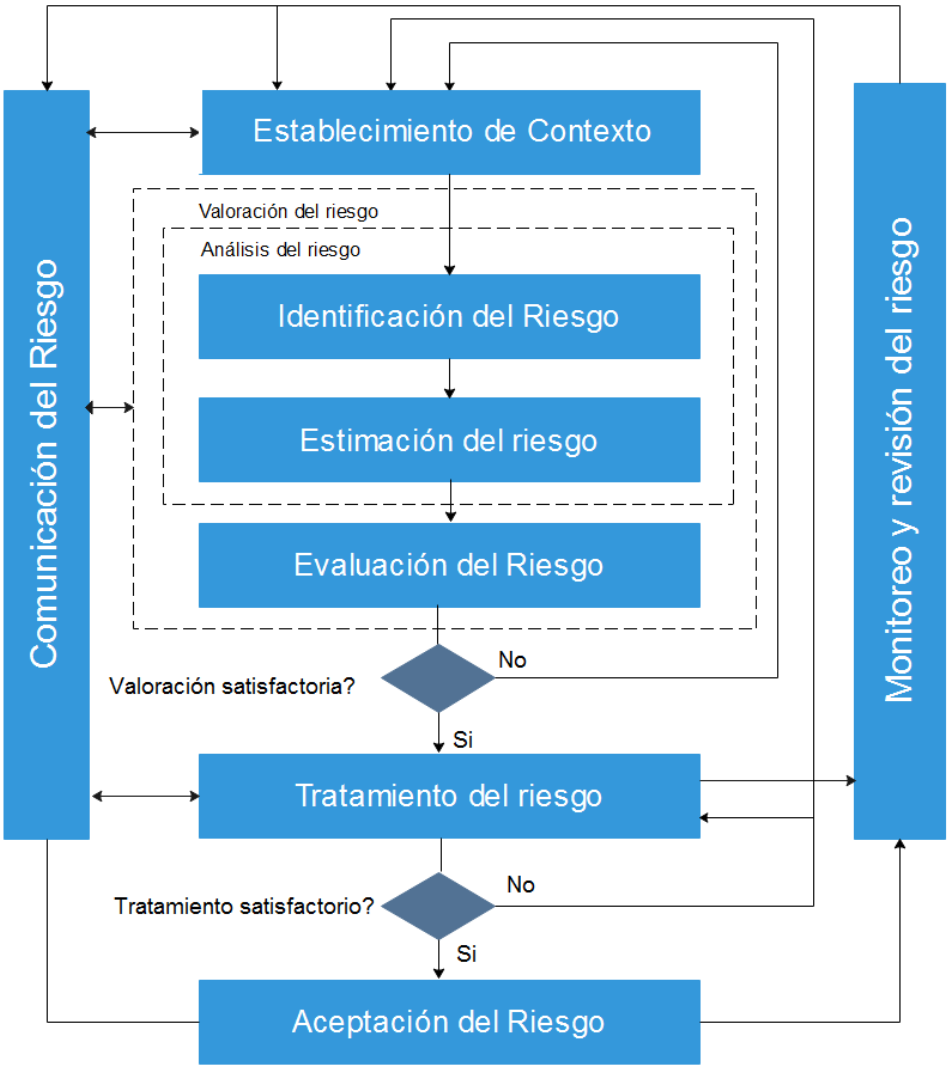


Figura 6.1 Aplicación del proceso de gestión del riesgo en la seguridad de la información
Fuente: Norma NB/ISO/IEC 27005

Siguiendo el proceso de gestión del riesgo en la seguridad de la información, primero se establecerá el contexto, que implica reunir y exponer la información necesaria para explicar la actividad de la empresa corredora. En el presente estudio el contexto ha sido desarrollado para las empresas corredoras de seguros, el cual varia con el contexto de las corredoras de reaseguros, sin embargo el objetivo es presentar una forma de esquematizar la organización y funcionamiento de una empresa corredora, de forma genérica utilizando diagramas de bloques y mapas de procesos.

6.1 ESTABLECIMIENTO DEL CONTEXTO

6.1.1 CARACTERÍSTICAS GENERALES DE CORREDORES DE SEGUROS

Un corredor de seguros puede estar conformado por una persona, o puede tratarse de una Empresa, ambos tienen la misma finalidad, ofrecer al cliente un acceso a las mejores condiciones técnicas otorgadas por las Aseguradoras, en la cobertura de interés del cliente.

El mundo de los seguros se va renovando de manera permanente, aumentando constantemente nuevas Coberturas con mayores alcances y beneficios. El poder obtener una Póliza acorde a las necesidades implica un amplio conocimiento técnico de Coberturas, Exclusiones, Cláusulas, Anexos, etc. Por ello es importante contar con un Asesor especializado que guie al cliente en la contratación y administración, tanto de pólizas individuales, como empresariales o institucionales. (Sudamericana Corredores & Asesores de Seguros, s.f.)

En Bolivia, se cuenta con 33 empresas Corredoras de Seguros reguladas por la APS, para el análisis del entorno y establecimiento del contexto, se toma como base la misión que tienen, entre las cuales se pueden citar:

Misión de Sudamericana Corredores & Asesores de Seguros

Ser líderes en el mercado Asegurador a través de propuestas competitivas e innovadoras en materia de prevención y protección de riesgos, mediante asesoría integral basada en el uso de sistemas tecnológicos al servicio de nuestros clientes. Ser además, reconocidos por el alto nivel técnico de nuestros funcionarios y nuestra solidez financiera. (Sudamericana Corredores & Asesores de Seguros, s.f.)

Misión de Consultores de Seguros S.A.

Brindamos servicios profesionales de asesoramiento e intermediación de seguros con personal altamente especializado y enfocado en la satisfacción de los requerimientos de nuestros clientes, ofreciéndoles soluciones integrales a sus necesidades. (Consultores de Seguros S.A. s.f.)

Entonces se puede concluir que en general una empresa corredora de seguros, ofrece al cliente un asesoramiento para elegir el mejor proveedor de seguros, de acuerdo a las coberturas que ofrecen las compañías de Seguros en los diferentes ramos. Como se puede observar en la *Figura 6.2*

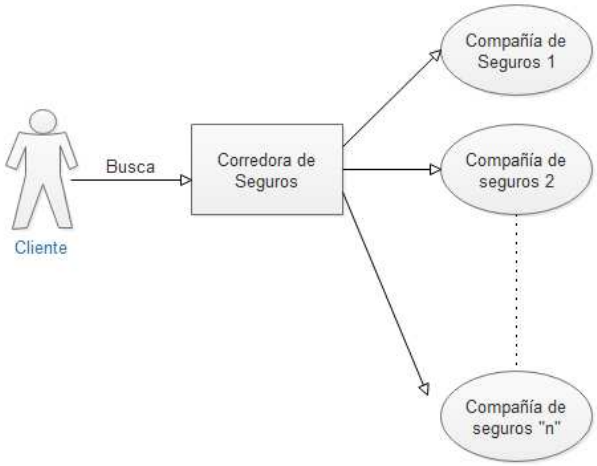


Figura 6.2 Aplicación de diagrama utilizado para analizar el Contexto en una Corredora de Seguros

Fuente: Elaboración propia

6.1.2 ANÁLISIS DEL ENTORNO

Se reconocen las partes interesadas

Partes Interesadas	**Expectativas o necesidades**
Propietarios	Desempeño de sus inversiones
Cliente	Buen asesoramiento, información actual y verídica, calidad de servicio
Empleados	Satisfacción con su carrera y puesto de trabajo, remuneración adecuada
Aseguradoras	Oportunidades comerciales, Buena comunicación de los seguros que ofrecen

Tabla 6.1 Identificación de partes interesadas en corredoras de seguros

Fuente: Elaboración propia

En la Figura 6.3 se puede observar la relación de la Empresa Corredora con sus partes interesadas.

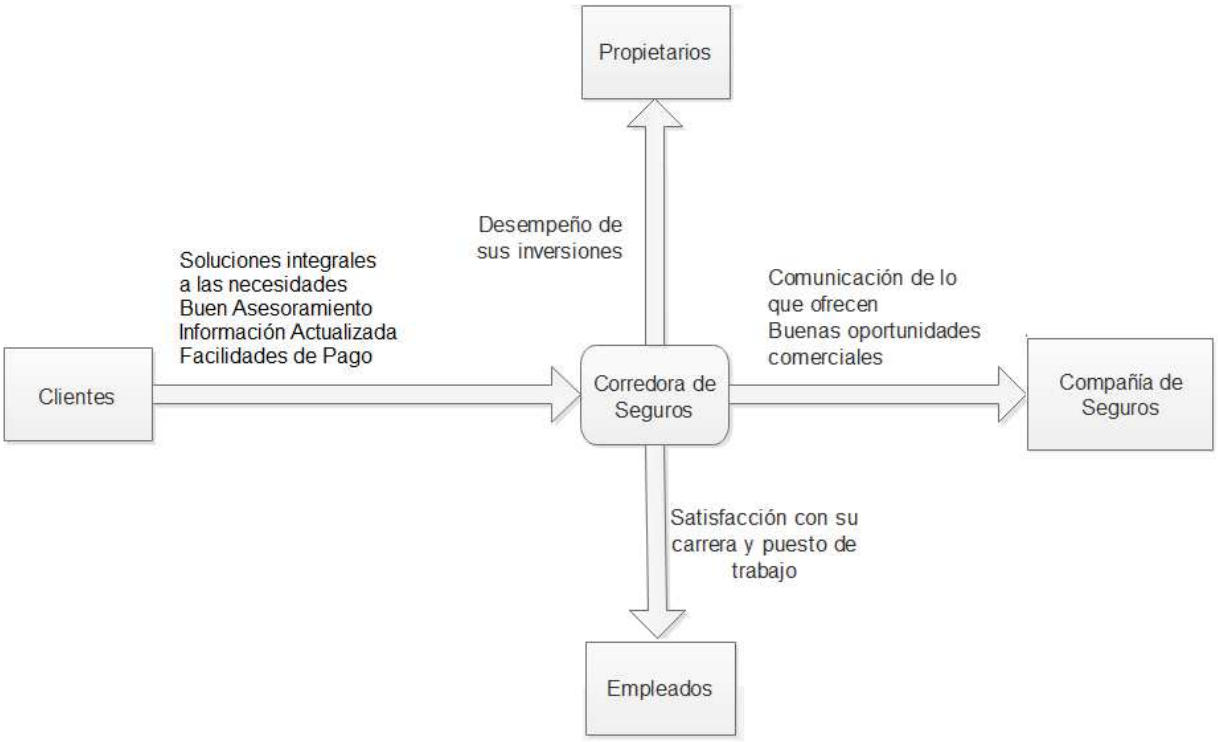


Figura 6.3 Diagrama de bloques aplicado para la Identificación de partes interesadas en una corredora de Seguros

Fuente: Elaboración propia

6.1.3 RECONOCIMIENTO DE PROCESOS

La identificación de procesos e interrelación existente entre todos los procesos de la Empresa, puede representarse mediante un mapa de procesos que es una representación gráfica o un diagrama. Puede parecer sencillo, pero la verdad es que es una tarea dificultosa, ya que implica el conocimiento de la organización y los departamentos por los cuales está compuesta la empresa corredora.

En una corredora de seguros, es importante la obtención de una Póliza acorde a necesidades del cliente, lo que implica un amplio conocimiento técnico en el ámbito de los Seguros, siendo la clave de una corredora de seguros, para asesorar al cliente, contando con varias empresas proveedores de seguros en diferentes ramos, se realiza la cotización del mejor seguro.

Es sustancial comprender al cliente a quien se va asesorar, identificando y analizando los riesgos que pueden afectar el patrimonio del Cliente. De acuerdo a este conocimiento se estructura técnicamente una póliza (La póliza de seguro, es el documento que certifica el respaldo al que accede el asegurado cuando paga una prima para ello), de acuerdo a las características propias de la actividad, intereses y bienes del Cliente, que ahora ya se convierte en Asegurado.

Se revisan los documentos emitidos por las Aseguradoras minuciosamente para la determinación de las coberturas requeridas. Así también se puede solicitar a las Aseguradoras las modificaciones que se producen por decisiones de la APS, según corresponda.

Como asesor de seguros uno de las características es el recordatorio de fechas de pago de manera oportuna, negociando programaciones de fecha de pago, si así lo requiere el Asegurado.

Para realizar los procesos mencionados, se requiere de procesos de apoyo, que son realizados por diferentes áreas de la Empresa, entre las cuales se destacan: Gerencia, área de contabilidad, área de gestión de clientes y cotizaciones, área de gestión de pólizas y área de Tecnología de Información (T.I.)

Con estas consideraciones se pueden reconocer los siguientes procesos:

- Procesos Estratégicos
- Procesos Clave
- Procesos de Apoyo

Se pueden ver en la siguiente figura:

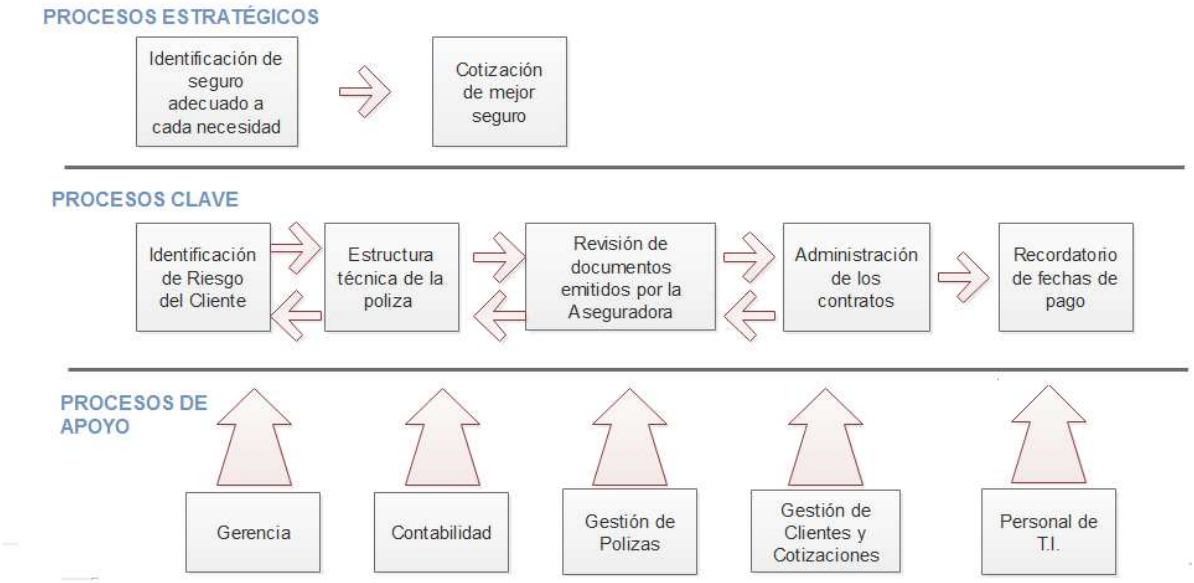


Figura 6.4 Mapa, aplicado para la Identificación de Procesos en una Corredora de Seguros
Fuente: Elaboración propia

NOTA. Siendo un análisis genérico, el cual no es específico para una empresa y mucho menos obligatorio, este esquema ayuda a la comprensión del contexto en el cual se ha realizado el desarrollo del presente estudio, por lo que no se encuentran a detalle todos los procesos, ni subprocesos que pudieran existir en una Empresa Corredora de Seguros.

En el área de Tecnologías de Información muchas veces identificado también como área de Sistemas, se reconocen las siguientes partes interesadas

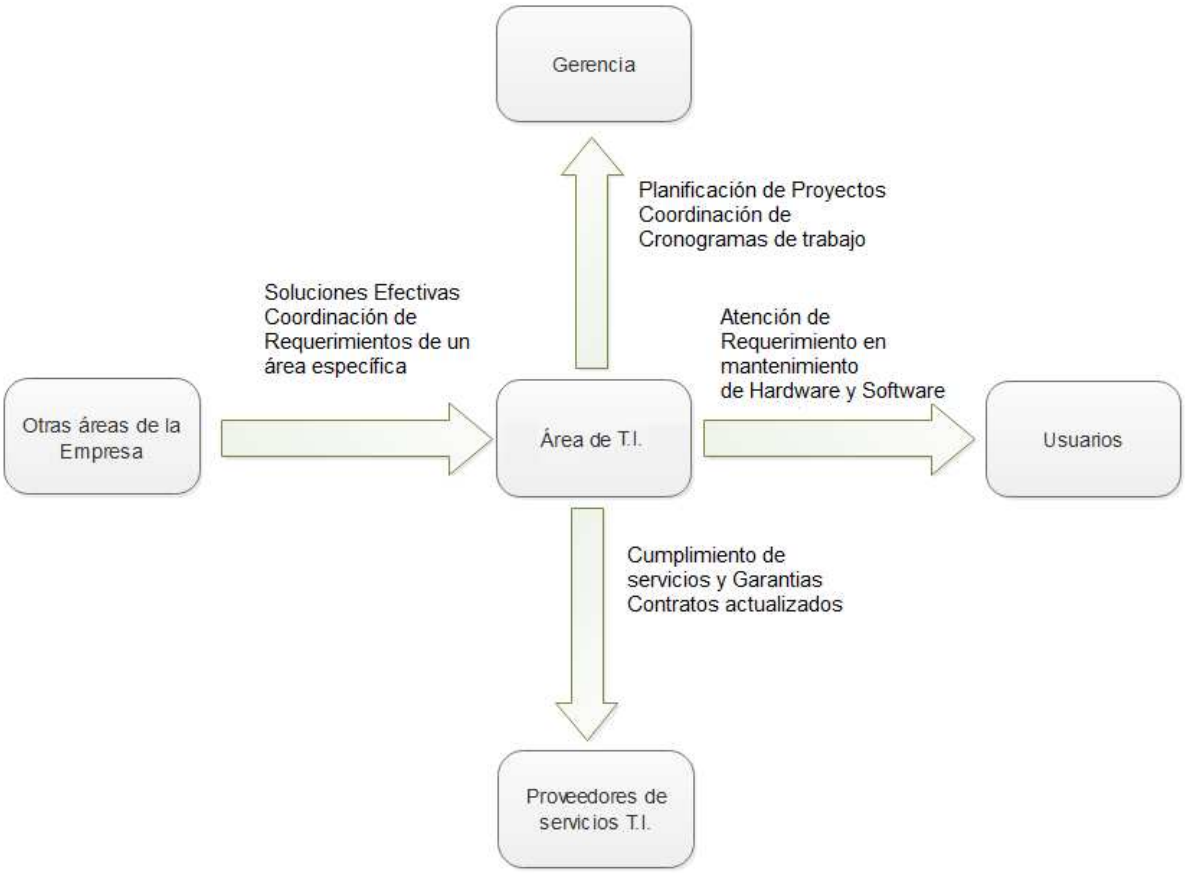


Figura 6.5 Diagrama de bloques utilizado para la Identificación de partes interesadas en el área de Sistemas

Fuente: Elaboración propia

Entre los procesos de apoyo en una Empresa Corredora de Seguros se encuentra el personal de T.I. que conforma el área de Tecnología de Información (T.I.) o área de Sistemas, se identifica los procesos estratégicos, claves y de apoyo, correspondientes a esta área.

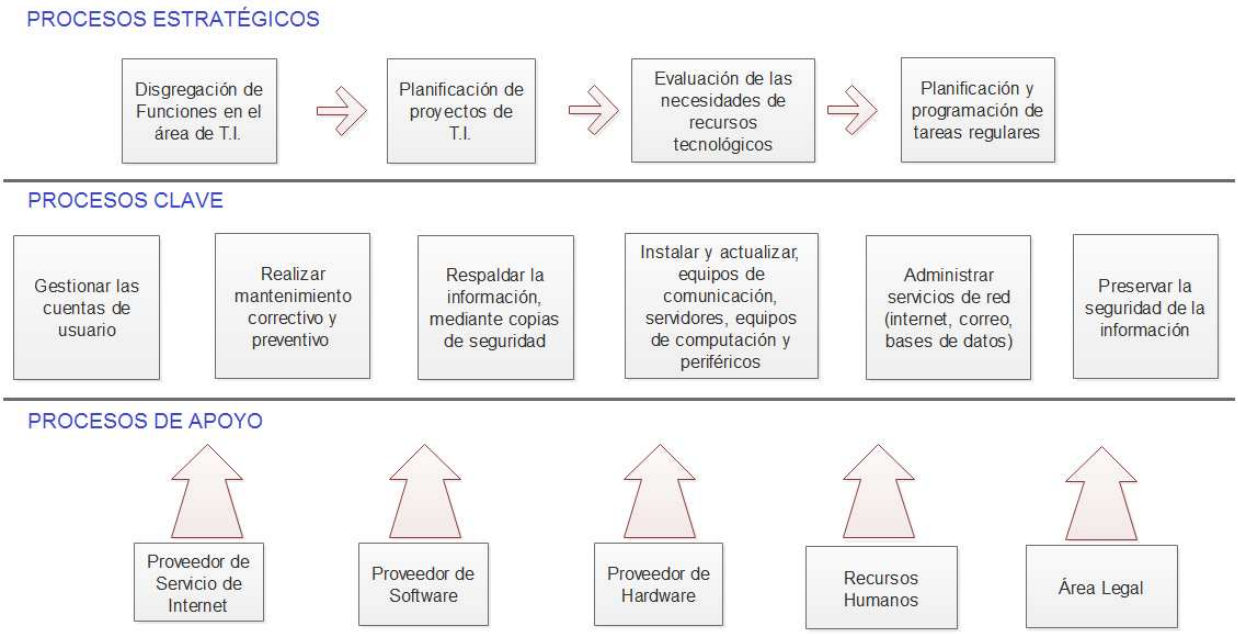


Figura 6.6 Mapa aplicado para la Identificación de procesos en el área de Tecnologías de Información en una Empresa corredora de Seguros

Fuente: Elaboración propia

Identificados los procesos estratégicos, procesos clave y procesos de apoyo, aplicado al área de Tecnologías de la Información, es utilizado para comprender gráficamente la interrelación entre procesos que permite reconocer las funciones y responsabilidades del área de TI, las áreas de apoyo que se interrelacionan con TI.

6.2 VALORACIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN

Considerando la norma NB/ISO/IEC 27005, la valoración del riesgo consta de las siguientes actividades:

Figura 6.7 Detalle de actividades utilizado para realizar la Valoración del riesgo en la seguridad de la información

Fuente: Elaboración propia basado en la norma NB/ISO/IEC 27005

El análisis de riesgo comprende dos actividades importantes que son: la identificación del riesgo y la estimación del riesgo.

En el desarrollo de la identificación del riesgo, se tienen cinco actividades que son amplias, se inicia con la identificación de los activos de información importantes para la empresa corredora, que está asociado con el cuarto control de administración de activos, analizado ya en el Capítulo 5.

La Evaluación del Riesgo, utiliza la comprensión del riesgo que se obtiene mediante el análisis del riesgo.

ANÁLISIS DEL RIESGO

6.2.1 IDENTIFICACIÓN DEL RIESGO

Antes de la identificación del riesgo, se requiere identificar los activos de información, identificar las amenazas, identificar los controles existentes, identificar las vulnerabilidades e identificar las consecuencias.

6.2.1.1 IDENTIFICACIÓN DE LOS ACTIVOS

El estudio involucra el área de T.I. de las empresas corredoras de seguros y reaseguros, por lo cual en este apartado se mencionan los activos de soporte de información. La siguiente tabla de activos no es exhaustiva, tan poco válida para siempre, ya que está sujeto a los cambios tecnológicos, es un referente para identificar los activos de información que pueden ser asociados a riesgos.

Se utilizará como base Magerit v.3 Libro II, para determinar los activos relevantes:

- Información (INF) Documentos impresos incluido registros, llenados manualmente.
- Datos (D) que materializan la información.
- Servicios (S) auxiliares que se necesitan para poder organizar el sistema.
- Las aplicaciones informáticas *(software SW)* que permiten manejar los datos.
- Los equipos informáticos *(hardware HW)* y que permiten hospedar datos, aplicaciones y servicios.
- Las redes de comunicaciones (COM) que permiten intercambiar datos.
- El equipamiento auxiliar (AUX) que complementa el material informático.
- Instalaciones (I) que implican las oficinas del área de sistemas y el ambiente destinado a Centro de Procesamiento de Datos.
- Las personas (P) que explotan u operan todos los elementos anteriormente citados.

Tipo de Activo	Detalle
INFORMACIÓN (INF)	Documentos de Políticas de Seguridad Registro de Backups Registro de Incidentes Registro de entrada al CPD
DATOS (D)	Datos de configuración Copias de Respaldo Registro de Actividad Código fuente de programa Código ejecutable de programa Datos de prueba
SERVICIOS (S)	Página Web Correo electrónico Telnet (acceso remoto) Servicio de Almacenamiento de archivos Servicio de Active Directory Servicio de VPN
SOFTWARE (SW)	Aplicación específica del negocio (sistema de contabilidad, sistema de producción) Ofimática Navegador Web Servidor de Aplicaciones Servidor de Correo Electrónico Antivirus Sistema Operativo Sistema de Gestión de Base de Datos
HARDWARE (HW)	Equipo portátil Equipo de respaldo Medios de Impresión Escáners Soporte de la Red Switch Router Firewall Punto de acceso inalámbrico Central telefónica Teléfono IP
REDES DE COMUNICACIONES (COM)	Red telefónica Red local Internet Red inalámbrica
EQUIPO AUXILIAR (AUX)	Fuentes de Alimentación Fuentes de Alimentación Ininterrumpida (UPS) Equipos de climatización Cableado de datos Cableado eléctrico

	Fibra óptica
INSTALACIONES (I)	Oficinas Canalizaciones Centro de Procesamiento de Datos
PERSONAL (P)	Usuarios Externos Usuarios Internos Administradores de Sistemas Programadores Consultores Proveedores

Tabla 6.2 Identificación de los activos de información relacionados con el área de TI de empresas corredoras, aplicando Magerit

Fuente: Elaboración propia basado en Magerit Versión 3.0 Libro II (2012)

A la *Tabla 6.2* también se le puede complementar con detalles de ubicación, propietarios u otras características necesarias para que el activo sea plenamente identificado.

Se ha considerado los activos que tienen un valor de importancia para el área de TI de la empresa corredora y que pueda causar un riesgo, la ausencia del mismo. Incluso si se trata de información pertinente al conocimiento y experiencia de las personas, serán tratadas como activo de información. En el caso de que un activo registrado como teclado o mouse, que no representa un riesgo y su disponibilidad puede ser remplazada de forma inmediata, no se considera en la lista.

6.2.1.2 IDENTIFICACIÓN DE LAS AMENAZAS

En base al ANEXO 5 identificaremos los tipos de amenazas, que según MAGERIT versión 3.0. libro II, se distinguen cuatro, cada uno estará representado por una abreviatura, tal como sigue:

- Desastres Naturales [N]
- De origen industrial [I]
- Errores y fallos no intencionados [E]
- Ataques intencionados [A]

En la siguiente tabla se identifican el origen y la amenaza asociada, de acuerdo a Magerit – Versión 3, libro II.

ORIGEN	**AMENAZA**
Desastres Naturales [N] Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.	[N.1] Fuego
	[N.2] Daños por agua
	[N.3] Desastres Naturales
De origen industrial [I] Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial.	[I.5] Avería de origen físico o lógico
	[I.6] Corte del Suministro eléctrico
	[I.7] Condiciones inadecuadas de temperatura o humedad
	[I.8] Fallo de servicios de comunicaciones
	[I.9] Interrupción de otros servicios y suministros esenciales
	[I.11] Emanaciones Electromagnéticas
Errores y fallos no intencionados [E] Fallos no intencionales causados por las personas.	[E.1] Errores de los usuarios
	[E.2] Errorres del Administrador
	[E.3] Errores de monitorización
	[E.4] Errores de Configuración
	[E.7] Deficiencias en la Organización
	[E.8] Difusión de Software Dañino
	[E.9] Errores de Re-encaminamiento
	[E.10] Errores de Secuencia
	[E.15] Alteración accidental de la Información
	[E.18] Destrucción de Información
	[E.19] Fugas de Información
	[E.20] Vulnerabilidades de los programas
	[E.21] Errores de Mantenimiento/ actualización de programas
	[E.23] Errores de Mantenimiento/actualización de equipos
	[E.24] Caída del sistema por agotamiento de recursos
	[E.25] Pérdida de equipos
Ataques intencionados [A] Fallos deliberados causados por las personas.	[A.3] Manipulación de Registros de Actividad
	[A.4] Manipulación de la configuración
	[A.5] Suplantación de la Identidad del Usuario
	[A.6] Abuso de privilegios de acceso
	[A.7] Uso no previsto
	[A.8] Difusión de Software Dañino
	[A.9] Re-encaminamiento de mensajes

	[A.11] Acceso no autorizado
	[A.12] Análisis de tráfico
	[A.13] Repudio
	[A.14] Interceptación de información
	[A.15] Modificación deliberada de la información
	[A.18] Destrucción de Información
	[A.19] Divulgación de Información
	[A.22] Manipulación de programas
	[A.23] Manipulación de los equipos
	[A.24] Denegación de Servicio
	[A.25] Robo
	[A.26] Ataque destructivo
	[A.28] Indisponibilidad del personal
	[A.29] Extorsión
	[A.30] Ingeniería social

Tabla 6.3 Identificación de Amenazas, en el entorno de las empresas corredoras, aplicando Magerit

Fuente: Elaboración propia basado en Magerit Versión 3.0 (2012)

6.2.1.3 IDENTIFICACIÓN DE LOS CONTROLES EXISTENTES

Siendo el presente estudio un modelo SGSI aplicado a empresas corredoras de seguros y reaseguros, la identificación de controles existentes ha sido realizada de forma genérica. Los controles existentes han sido identificados mediante investigación, a través de un cuestionario que ha sido respondido por personal de T.I. de las empresas Corredores de Seguros y Reaseguros. El detalle de los resultados se encuentra descrito en el Capítulo 4.

En el cuestionario, se indago sobre los controles de seguridad de la información que son aplicados actualmente, tomando en cuenta los controles que están detallados en el Anexo A de la norma NB/ISO/IEC 27001, que están alineados con los enumerados en ISO/IEC 27002.

Los resultados fueron los siguientes:

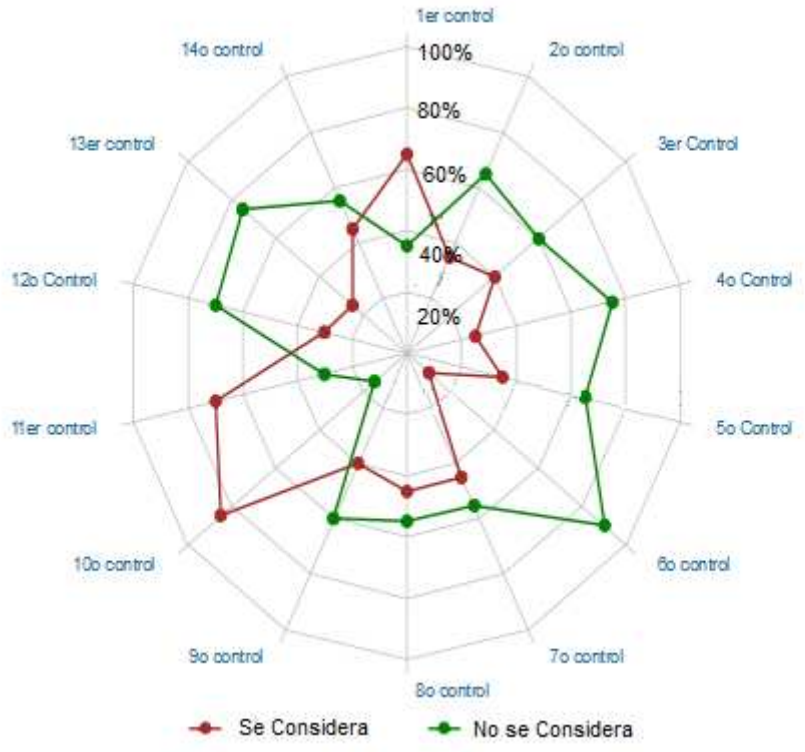


Figura 6.8 Diagrama Araña. Resultado General de los Controles de Seguridad de la Información considerados en las empresas corredoras de Seguros y Reaseguros

Fuente: Elaboración propia

Donde:

1er control. Políticas de Seguridad de la Información
2o control. Organización de la Seguridad de la Información
3er control. Seguridad ligada a los recursos humanos
4o control. Administración de activos
5o control. Control de acceso
6o control. Criptografía
7o control. Seguridad física y del ambiente
8o control. Seguridad de las operaciones
9o control. Seguridad de las comunicaciones
10o control. Adquisición, desarrollo y mantenimiento del sistema
11er décimo primer control. Relaciones con el proveedor
12o décimo segundo control. Administración de incidentes de seguridad de la información
13er Décimo tercer control. Aspectos de seguridad de la información de la administración de la continuidad del Negocio
14o Décimo cuarto control. Cumplimiento

Según la *Figura 6.8*, se puede mencionar los siguientes aspectos:

- ✓ En el 65 % de las empresas se considera aceptable el documento sobre Políticas de Seguridad de la Información
- ✓ En el 85 % de las empresas se considera que establecieron controles pertinentes en la Adquisición, desarrollo y mantenimiento de sistemas
- ✓ En el 70% de las empresas se considera que establecieron controles en las Relaciones con los proveedores

Los controles de Criptografía no son utilizados en un 90% de las empresas.

Otros controles que tienen un porcentaje alto de no ser atendidos son:

- ✓ En el 75% de las empresas no se considera que posea controles aceptables sobre la Administración de activos de información
- ✓ En el 70% de las empresas no se considera que posea controles aceptables sobre la Administración de incidentes de seguridad de la información
- ✓ En el 75 % de las empresas no se considera que posea controles aceptables sobre Aspectos de la seguridad de la información de la administración de la continuidad comercial

Los demás controles aún están en desarrollo y muchas veces desatendidos, por lo cual no serán tomados en cuenta.

Como se ha realizado una encuesta personal a través de un cuestionario, el cual tenía preguntas directamente relacionadas con los controles, se citaran los controles que tienen un porcentaje aceptable mayor al 60% en las empresas corredoras de seguros y reaseguros.

Entonces los controles que se pueden considerar son:

Controles Considerados	Detalle
Documento de políticas de seguridad	Política o procedimiento sobre el manejo de medios extraíbles (Discos duros externos, DVDs, memorias USB y otros)
	Política del manejo de la información confidencial en los equipos de computación, cuando se realiza el mantenimiento
	Política, sobre el uso aceptable de las instalaciones de comunicación
	Política sobre el uso de la mensajería, redes sociales
	Política sobre manejo de información confidencial
	Política sobre el acceso de los proveedores a la información de la empresa
	Política sobre la privacidad y protección de la información personal identificable
Adquisición, desarrollo y mantenimiento de sistemas	Existe contrato sobre adquisición, de sistemas Existe contrato de desarrollo y mantenimiento de sistemas
	Se cuenta con la documentación sobre proyectos de desarrollo de software
	Se documenta el proceso de pruebas, para adquirir un nuevo software
	Tiene conocimiento sobre clave pública y firma digital
	Se cuenta con un documento el cual establezca las reglas para el desarrollo de software y sistemas
	Se cuenta con un documento que indica los procedimientos de control de cambios en sistemas
	Cuando se cuenta con un nuevo sistema, se realizan las pruebas de aceptación
	En caso de adquirir un sistema (software) el contrato señala los derechos de propiedad de código y de propiedad intelectual
Relaciones con los	Existe una política sobre el acceso de los proveedores a la

proveedores	información de la empresa
	Existe una capacitación para el personal de la empresa que interactúa con el proveedor
	Se abordan el tema de seguridad dentro de los acuerdos con los proveedores que proporcionan componentes de infraestructura de T.I.
	En el acuerdo o contrato con los proveedores se especifican las obligaciones del proveedor para cumplir los requisitos de seguridad de la organización
	Existe una persona específica que administre las relaciones con el proveedor
	Se cuenta con los informes de servicio de los proveedores

Tabla 6.4 Detalle de los controles considerados en las empresas corredoras de seguros y reaseguros

Fuente: Elaboración propia, basado en los resultados del Capítulo 4

La tabla expuesta es genérica, producto de las respuestas al cuestionario realizado a las empresas corredoras, no es específica para una empresa.

6.2.1.4 IDENTIFICACIÓN DE LAS VULNERABILIDADES

La sola presencia de una vulnerabilidad no causa daño por sí misma, dado que es necesario que haya una amenaza presente para explotarla. Por el contrario, una amenaza que no tiene vulnerabilidad correspondiente puede no resultar un riesgo. (NB/ISO/IEC 27005, 2010)

Del Anexo D, correspondiente a la norma NB/ISO/IEC 27005 se puede citar los siguientes tipos de vulnerabilidades:

TIPOS	VULNERABILIDADES
Información	Ausencia de revisión, actualización de políticas Ausencia de datos importantes en el registro Ausencia de capacitación, para el debido llenado y manejo de registro Ausencia de control sobre el llenado del registro

Datos	Ausencia de datos de configuración Ausencia de copias de respaldo Ausencia de restricción de acceso al código fuente Ausencia de protección del código ejecutable Ausencia de protección de datos de prueba
Servicio	Software desactualizado Ausencia de capacitación del usuario sobre manejo de correo electrónico Ausencia de capacitación del usuario en el manejo de almacenamiento de archivos Desconocimiento de la configuración y administración de parte del administrador Ausencia de contrato con el proveedor del servicio
Hardware	Mantenimiento insuficiente / mala instalación Falta de condiciones de funcionamiento Ausencia de dispositivos de reemplazo Ausencia de un eficiente control de cambios en la configuración
Software	Especificaciones incompletas o no claras para los desarrolladores Gestión deficiente de las contraseñas Software nuevo o inmaduro Descarga y uso no controlados de software Configuración incorrecta de parámetros Ausencia de copias de respaldo Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario Ausencia de antivirus Ausencia de actualización Ausencia de mecanismos de identificación y autentificación, como usuario y contraseña al inicio Ausencia de control de cambios eficaz Tablas de contraseñas sin protección Asignación errada de los derechos de acceso
Red	Conexiones de red pública sin protección Conexión deficiente de los cables de datos Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento) Ausencia de identificación y autenticación de emisor y receptor
Equipo Auxiliar	Ausencia de dispositivos de reemplazo Mantenimiento insuficiente / mala instalación
Instalaciones	Ausencia de extintor Ausencia de cámaras de seguridad Ausencia de planos de instalación Instalación precaria Ausencia de control de ingreso en la entrada al CPD Ausencia de sensores de humo y temperatura
Personal	Ausencia de control sobre los accesos a la red y equipos de computación Desconocimiento de las políticas sobre seguridad de la información de la empresa Uso incorrecto de hardware y software Ausencia o desconocimiento de políticas para el uso correcto de los dispositivos de TIC

	Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo Ausencia de control sobre los accesos a la información Ausencia de control de cambios eficaces sobre los programas Ausencia de controles de acceso lógico y físico a las instalaciones Ausencia de contrato Desconocimiento de las políticas sobre seguridad de la información de la empresa a la cual presta servicio

Tabla 6.5 Elección de Vulnerabilidades aplicado a los Activos de Información en base a Norma NB/ISO/IEC 27005

Fuente. Elaboración propia aplicando el Anexo D de la Norma NB/ISO/IEC 27005

Las vulnerabilidades de tipo organizativo son consecuencia de la falta de procedimientos, procesos, políticas, registros, controles, revisiones, autorizaciones sobre las tareas vinculadas al área de tecnologías de información, citamos al respecto algunos ejemplos:

- ✓ Ausencia de proceso formal para la revisión de los derechos de acceso, lo que puede generar abuso de derechos.
- ✓ Ausencia o insuficiencia de disposiciones con respecto a la seguridad en los contratos con las terceras partes, lo que puede generar abuso de derechos.
- ✓ Ausencia de procedimientos de control de cambios en los sistemas de información.
- ✓ Ausencia de procedimiento formal para la autorización de la información disponible al público.
- ✓ Ausencia de planes de continuidad.
- ✓ Ausencia de políticas sobre el uso de correo electrónico.
- ✓ Ausencia de procedimientos para la introducción del software en los sistemas operativos.
- ✓ Ausencia de procedimientos para el manejo de información clasificada.
- ✓ Ausencia o insuficiencia en las disposiciones, con respecto a la seguridad de la información, en los contratos con los empleados.
- ✓ Ausencia de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información.
- ✓ Ausencia de políticas formales sobre la utilización de computadores portátiles.

- ✓ Ausencia o insuficiencia de política sobre limpieza de escritorio y de pantalla.
- ✓ Ausencia de autorización de los recursos de procesamiento de la información.
- ✓ Ausencia de revisiones regulares por parte de la gerencia.
- ✓ Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad

Existen métodos de prueba que ayudan a la valoración de las vulnerabilidades técnicas como ser: Herramientas automáticas de exploración de vulnerabilidades y pruebas de penetración, las cuales deben ser realizadas por personas con las competencias necesarias para esta tarea.

Los resultados de estos tipos de pruebas de seguridad ayudan a identificar otras vulnerabilidades.

6.2.1.5 IDENTIFICACIÓN DE LAS CONSECUENCIAS

Las consecuencias pueden ser de naturaleza temporal o permanente como es el caso de la destrucción de un activo de información.

Entre las consecuencias se ha identificado las siguientes:

Motivo	**Consecuencias**
Daño a la Información de carácter personal	Probablemente suponga el incumplimiento de una regulación afectando a una o muchas personas.
Incumplimiento con Obligaciones Legales	Probablemente cause un incumplimiento de una resolución o circular del ente regulador.
Daños a la Seguridad	Probablemente sea causa de un incidente de seguridad o dificulte la investigación de incidentes serios.
Daños a Intereses comerciales o económicos	De interés para la competencia, de valor comercial, causa de pérdidas económicas, causa de ganancias o ventajas para individuos u organizaciones, constituye un incumplimiento en obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros.

Interrupción del servicio	Causa de una interrupción de las actividades propias de la organización con un impacto en otras organizaciones.
Mala administración y gestión en el área de sistemas	Probablemente impediría la operación efectiva de los sistemas de información en la Empresa.
Pérdida de confianza en los sistemas de información de la Empresa (sistema de producción y sistema contable)	Probablemente causaría una publicidad negativa para el área de T.I. o área de sistemas por afectar el trabajo del personal interno de la Empresa

Tabla 6.6 Identificación de consecuencias aplicadas para valorar los activos de información

Fuente: Elaboración propia basado en Magerit Versión 3.0 Libro II (2012)

Las consecuencias descritas en la tabla son seleccionadas del modelo de Magerit Versión 3.0 Libro II son útiles para valorar los activos y van identificadas con cada tipo de activos.

6.2.2 ESTIMACIÓN DEL RIESGO

Se utilizará una estimación cualitativa para obtener una indicación general del nivel del riesgo. En base a este estudio cada empresa puede hacer el análisis de riesgo más específico y adecuado.

Para la valoración de los activos según sus dimensiones de Confidencialidad, Disponibilidad e Integridad, se consideran cinco niveles, los cuales son:

Figura 6.9 Consideración de Niveles de Valoración aplicado a los activos de Información

Fuente: Elaboración propia

La interpretación en cada una de las dimensiones se muestra en las siguientes tablas:

Confidencialidad	**Significado**
Muy bajo (MB)	Público
Bajo (B)	Uso Interno
Medio (M)	Uso Restringido
Alto (A)	Confidencial
Muy Alto (MA)	Secreto

Tabla 6.7 Criterio aplicado en la Interpretación de la Dimensión de Confidencialidad

Elaboración: Fuente propia

Disponibilidad	**Significado**
Muy bajo (MB)	De 1 día a 5 días (No puede ausentarse más de cinco días)
Bajo	De 9 a 24 horas (No puede ausentarse más de 24 horas)
Medio	De 1 a 8 horas (No puede ausentarse más de 8 horas)
Alto	De 30 a 60 minutos (No puede ausentarse más de 60 minutos)
Muy Alto	De 1 a 30 minutos (No puede ausentarse más de 30 minutos)

Tabla 6.8 Criterio aplicado en la Interpretación de la Dimensión de Disponibilidad

Elaboración: Fuente propia

Integridad	**Significado**
Muy bajo	Puede reemplazarse fácilmente
Bajo	Puede ser reemplazado
Medio	Puede ser reemplazado por otro activo similar
Alto	La calidad del activo se puede reemplazar implicando un costo
Muy Alto	No se puede volver a reemplazar con la misma calidad

Tabla 6.9 Criterio aplicado en la Interpretación de la Dimensión de Integridad

Elaboración: Fuente propia

6.2.2.1 NIVELES DE CLASIFICACIÓN

Para obtener el valor de un activo de información tomando en cuenta las dimensiones de Disponibilidad, Integridad y Confidencialidad se ha adoptado el siguiente criterio, el cual puede variar de acuerdo al punto de vista de la empresa.

ESTIMACIÓN	NIVELES DE CLASIFICACIÓN
Muy Alto	Valor de activos de información en los cuales la estimación en todas o dos de las dimensiones sea Muy Alto
Alto	Valor de activos de información en los cuales la estimación en todas o dos de las dimensiones sea Alto
Medio	Valor de activos de información en los cuales la estimación en todas o dos de las dimensiones sea Medio
Bajo	Valor de activos de información en los cuales la estimación en todas o dos de las dimensiones sea Bajo
Muy Bajo	Activos de información en los cuales la estimación en todas o dos de las dimensiones sea Muy Bajo

Tabla 6.10 Criterios de Niveles aplicado a la valoración de los activos de información
Fuente: Elaboración propia

Aplicando los criterios de niveles de valoración de la Tabla 6.10, de acuerdo a consideración personal con base en el conocimiento del área de tecnologías de información de las corredoras de seguros y reaseguros, se analiza cada activo de información en sus tres dimensiones: Confidencialidad, Disponibilidad e Integridad, para otorgarle un valor que es una estimación cualitativa. Como se muestra en la siguiente tabla:

		DIMENSIONES			***Valor***
TIPO	***ACTIVOS***	***Confidencialidad***	***Disponibilidad***	***Integridad***	***Estimación***
INF	Documento de Políticas de seguridad	M	A	A	Alto
INF	Documento Plan de	M	M	A	Medio

	Contingencias Tecnológicas				
INF	Registro de Backups	A	B	A	Alto
INF	Registro de Incidentes	MA	A	A	Alto
INF	Registro de entrada al CPD	A	M	M	Medio
D	Datos de configuración	A	MA	MA	Muy Alto
D	Copias de Respaldo	A	B	A	Alto
D	Código fuente de programa	MA	A	MA	Muy Alto
D	Código ejecutable de programa	A	A	MA	Alto
D	Datos de prueba	A	M	M	Medio
S	Página Web	MB	A	A	Alto
S	Correo electrónico	MA	MA	MA	Muy Alto
S	Telnet (acceso remoto)	A	M	A	Alto
S	Servicio de almacenamiento de archivos	M	MA	A	Medio
S	Servicio de Active Directory	A	MA	A	Alto
S	Servicio de VPN	MA	A	MA	Muy Alto
SW	Aplicación específica del negocio (sistema de contabilidad, sistema de producción)	MA	MA	MA	Muy Alto
SW	Ofimática	B	A	A	Alto
SW	Navegador Web	MB	M	M	Medio
SW	Servidor de Aplicaciones	M	A	A	Alto
SW	Servidor de Correo Electrónico	MA	MA	MA	Muy Alto
SW	Antivirus	B	B	A	Bajo
SW	Sistema Operativo	B	A	A	Alto
SW	Sistema de gestión de Base de Datos	MA	MA	MA	Muy Alto
HW	Equipo portátil	A	M	A	Alto
HW	Equipo de respaldo	A	M	A	Alto
HW	Medios de Impresión	MB	M	M	Medio
HW	Escáners	MB	A	A	Alto
HW	Switch	A	A	A	Alto
HW	Router	A	A	MA	Alto
HW	Firewall	MA	MA	MA	Muy Alto
HW	Punto de acceso inalámbrico	A	A	A	Alto
HW	Central telefónica	MA	MA	A	Muy Alto
COM	Red telefónica	M	A	A	Alto
COM	Red local	A	A	A	Alto
COM	Internet	MB	A	A	Alto
COM	Red inalámbrica	M	A	A	Alto
AUX	Fuentes de Alimentación	B	M	B	Bajo
AUX	Fuentes de Alimentación	M	A	A	Alto

	Ininterrumpida				
AUX	Equipos de Climatización	M	A	M	Medio
AUX	Cableado eléctrico	M	A	M	Medio
AUX	Cableado de datos	M	A	A	Alto
AUX	Fibra óptica	A	MA	A	Alto

Tabla 6.11 Valoración de activos de información aplicando criterios cualitativos
Fuente: Elaboración propia

Respecto a las instalaciones y el personal, no se puede manejar el mismo concepto, por lo cual para el análisis se considera con un valor ALTO.

El personal puede ser evaluado de acuerdo a sus capacidades y competencias, en este aspecto se debería coordinar con el área de recursos humanos, analizando diferentes, criterios como ser formación profesional, años de experiencia u otros.

En cuanto a las instalaciones también se pueden tener diferentes criterios para la valoración, pudiendo ser económica, técnica u otro.

Respecto al Hardware en la dimensión de integridad se puede, analizar el aspecto de que el equipo debe encontrarse completo físicamente, es decir con las condiciones necesarias para operar de manera correcta.

Valor económico de un activo

Económicamente un activo de información también se puede valorar respecto al valor en libros tomando en cuenta el valor de compra menos el valor depreciado al tiempo de vida útil.

Valoración de las amenazas

Una vez determinado que una amenaza puede perjudicar a un activo, hay que valorar su influencia en el valor del activo, en dos sentidos:

- **Degradación:** cuán perjudicado resultaría el valor del activo
- **Probabilidad:** cuán probable o improbable es que se materialice la amenaza

La degradación mide el daño causado por un incidente en el supuesto de que ocurriera.

La degradación se suele caracterizar como una fracción del valor del activo y así aparecen expresiones como que un activo se ha visto "totalmente degradado", o "degradado en una pequeña fracción". Como se puede apreciar en la siguiente tabla:

impacto		*degradación*		
		1%	10%	100%
valor	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Tabla 6.12 Estimación del Impacto

Fuente: Magerit versión 3 libro III (2012)

Entonces como referencia el valor de un activo de información puede ser MA (Muy Alto), si sufre una degradación del 1% sobre su valor se considera que el impacto será M (Medio), si sufre una degradación del 10% sobre su valor entonces el impacto será A (Alto), si sufre una degradación del 100% sobre su valor entonces el impacto será MA (Muy Alto).

Aplicando a la tabla de activos se tiene:

		IMPACTO	DEGRADACIÓN		
TIPO	***ACTIVOS***	***Valor***	**1%**	**10%**	**100%**
INF	Documento de Políticas de seguridad	Alto	B	M	A
INF	Documento Plan de Contingencias Tecnológicas	Medio	MB	B	M
INF	Registro de Backups	Alto	B	M	A
INF	Registro de Incidentes	Alto	B	M	A
INF	Registro de entrada al CPD	Medio	MB	B	M
D	Datos de configuración	Muy Alto	M	A	MA
D	Copias de Respaldo	Alto	B	M	A
D	Código fuente de programa	Muy Alto	M	A	MA
D	Código ejecutable de programa	Alto	B	M	A
D	Datos de prueba	Medio	MB	B	M

S	Página Web	Alto	B	M	A
S	Correo electrónico	Muy Alto	M	A	MA
S	Telnet (acceso remoto)	Alto	B	M	A
S	Servicio de almacenamiento de archivos	Medio	MB	B	M
S	Servicio de Active Directory	Alto	B	M	A
S	Servicio de VPN	Muy Alto	M	A	MA
SW	Aplicación específica del negocio (sistema de contabilidad, sistema de producción)	Muy Alto	M	A	MA
SW	Ofimática	Alto	B	M	A
SW	Navegador Web	Medio	MB	B	M
SW	Servidor de Aplicaciones	Alto	B	M	A
SW	Servidor de Correo Electrónico	Muy Alto	M	A	MA
SW	Antivirus	Bajo	MB	MB	B
SW	Sistema Operativo	Alto	B	M	A
SW	Sistema de gestión de Base de Datos	Muy Alto	M	A	MA
HW	Equipo portátil	Alto	B	M	A
HW	Equipo de respaldo	Alto	B	M	A
HW	Medios de Impresión	Medio	MB	B	M
HW	Escáners	Alto	B	M	A
HW	Modems	Alto	B	M	A
HW	Switch	Alto	B	M	A
HW	Router	Alto	B	M	A
HW	Firewall	Muy Alto	M	A	MA
HW	Punto de acceso inalámbrico	Alto	B	M	A
HW	Central telefónica	Muy Alto	M	A	MA
COM	Red telefónica	Alto	B	M	A
COM	Red local	Alto	B	M	A
COM	Internet	Alto	B	M	A
COM	Red inalámbrica	Alto	B	M	A
AUX	Fuentes de Alimentación	Bajo	MB	MB	B
AUX	Fuentes de Alimentación Ininterrumpida	Alto	B	M	A
AUX	Equipos de Climatización	Medio	MB	B	M
AUX	Cableado eléctrico	Medio	MB	B	M
AUX	Cableado de datos	Alto	B	M	A
AUX	Fibra óptica	Alto	B	M	A

Tabla 6.13 Impacto sobre los activos, basado en degradación de activos

Fuente: Elaboración propia

Si el activo de valor Muy Alto se degrada un 100% es decir totalmente, entonces se tiene un impacto Muy Alto. Que se lo identifica con color rojo.

Si el activo de valor Medio se degrada un 100% es decir totalmente, entonces se tiene un impacto Medio. Que se lo identifica con color amarillo.

De la tabla se puede observar que el impacto al 100%, está relacionado directamente con el valor del activo.

Ya se ha estimado el impacto en valor cualitativo, para cada uno de los activos de información. En el cálculo del riesgo, se requiere el valor cuantitativo del impacto, el cual se obtiene mediante la siguiente relación:

Impacto (valor cuantitativo)	Impacto (Valor cualitativo)
0	Muy Bajo
1	Bajo
2	Medio
3	Alto
4	Muy Alto

Tabla 6.14 Relación de valor cuantitativo y valor cualitativo del Impacto

Fuente: Elaboración propia, con base en Anexo E de la norma NB/ISO/IEC 27005

6.2.2.2 ESTIMACIÓN DE LA PROBABILIDAD

La probabilidad de un escenario de incidente está dada por una amenaza que explota una vulnerabilidad.

En base a Magerit, según el origen se encuentra un listado de amenazas, se ha seleccionado, las que pueden aplicarse en el entorno de las empresas corredoras y en la siguiente tabla se puede observar las amenazas y la dimensión afectada de acuerdo a los diferentes tipos de Activos.

ORIGEN	CÓDIGO	AMENAZA	D	I	C	INF	Dat	S	SW	HW	COM	AUX	I	P
Desastres naturales (N)	N.1	Fuego	X			X				X		X	X	
	N.2	Daños por agua	X			X				X		X	X	
	N.3	Otros Desastres Naturales	X			X				X		X	X	
De origen industrial (I)	I.5	Avería de origen fisico o lógico	X						X	X		X		
	I.6	Corte del Suministro eléctrico	X							X		X		
	I.7	Condiciones inadecuadas de temperatura o humedad	X							X		X		
	I.8	Fallo de servicios de comunicaciones	X								X			
	I.9	Interrupción de otros servicios y suministros esenciales	X									X		
	I.11	Emanaciones Electromagnéticas			X					X		X	X	
Errores y fallos no intencio-nados (E)	E.1	Errores de los usuarios	X	X	X	X		X	X					
	E.2	Errorres del Administrador	X	X	X	X	X	X	X	X	X			
	E.3	Errores de monitorización		X		X	X							
	E.4	Errores de Configuración		X						X				
	E.7	Deficiencias en la organización												X
	E.8	Difusión de Software Dañino	X	X	X				X					
	E.9	Errores de Re-encaminamiento			X			X	X		X			
	E.10	Errorres de Secuencia		X				X	X		X			
	E.15	Alteración accidental de la Información		X		X	X	X	X		X			
	E.18	Destrucción de Información	X				X	X	X		X		X	
	E.19	Fugas de Información			X		X	X	X		X		X	X
	E.20	Vulnerabilidades de los programas	X	X	X				X					
	E.21	Errores de Mantenimiento/ actualización de programas	X	X					X					
	E.23	Errores de Mantenimiento/actualización de equipos	X							X		X		
	E.24	Caida del sistema por agotamiento de recursos	X						X	X	X			
	E.25	Pérdida de equipos	X		X					X		X		
Ataques intencio-nados (A)	A.3	Manipulación de Registros de Actividad		X		X								
	A.4	Manipulación de la configuración	X	X	X				X	X				
	A.5	Suplantación de la Identidad del Usuario		X	X			X	X		X			
	A.6	Abuso de privilegios de acceso	X	X	X		X	X	X	X	X			
	A.7	Uso no previsto	X	X	X			X	X	X	X	X	X	
	A.8	Difusión de Software Dañino	X	X	X				X					
	A.9	Re-encaminamiento de mensajes			X			X	X		X			
	A.11	Acceso no autorizado		X	X		X	X	X	X	X	X	X	
	A.12	Análisis de tráfico			X						X			
	A.13	Repudio		X		X		X						
	A.14	Interceptación de información			X						X			
	A.15	Modificación deliberada de la información		X			X	X	X		X		X	
	A.18	Destrucción de Información	X				X	X	X				X	
	A.19	Divulgación de Información			X		X	X	X		X			
	A.22	Manipulación de programas	X	X	X				X					
	A.23	Manipulación de los equipos	X		X					X		X		
	A.24	Denegación de Servicio	X					X		X	X			
	A.25	Robo	X		X	X				X		X		X
	A.26	Ataque destructivo	X							X		X	X	X
	A.28	Indisponibilidad del personal												X
	A.29	Extorsión												X
	A.30	Ingeniería social												X

Tabla 6.15 Selección de Amenazas aplicado a los activos de información

Fuente: Elaboración propia basada en Magerit Versión 3.0 Libro II (2012)

Donde los tipos de Activos se representan como: Información (INF), Datos (Dat), Servicios (S), Software (SW), Hardware (HW), Redes de Comunicaciones (COM), Equipo Auxiliar (AUX), Instalaciones (I), Personal (P).

En las siguientes tablas se analiza todos los tipos de activos ya mencionados, con las vulnerabilidades y correspondientes amenazas que pueden explotarlas.

De acuerdo a la valoración cualitativa se considera que:

- Una amenaza puede ser: Alta, Media o Baja
- Una Vulnerabilidad puede ser: Alta, Media o Baja

Para cada vulnerabilidad se debe analizar la amenaza o amenazas asociadas, en este sentido la tabla es extensa, por cada tipo de activo. En la siguiente tabla se evalúa el valor de la probabilidad. Esta valoración se hace a partir de una combinación de la probabilidad de ocurrencia de la amenaza y la facilidad de explotación de la vulnerabilidad, el resultado se expresa como probabilidad de un escenario de incidente. Como se puede ver en la siguiente tabla:

Probabilidad de Amenaza	**Baja**			**Media**			**Alta**		
Niveles de Vulnerabilidad	B	M	A	B	M	A	B	M	A
Valor de la probabilidad de un escenario de incidente	0	1	2	1	2	3	2	3	4

Tabla 6.16 Determinación de probabilidad de un escenario de incidente
Fuente: Anexo E, Norma NB/ISO/IEC 27005

La interpretación de los resultados de Probabilidad de un escenario de incidente, se indican en la siguiente tabla:

Valor Cuantitativo	Valor Cualitativo	Significado
0	Muy Baja (MB)	Muy Improbable
1	Baja (B)	Improbable
2	Media (M)	Posible
3	Alta (A)	Probable
4	Muy Alta (MA)	Frecuente

Tabla 6.17 Interpretación de los resultados de probabilidad aplicados en el estudio

Fuente: Elaboración propia

El valor cualitativo de las vulnerabilidades y amenazas, mostrados en las tablas son producto de consideraciones basadas en experiencia personal de trabajo evaluando áreas de tecnologías de información de empresas corredoras de Seguros y Reaseguros, también se sustenta en los datos y resultados del Capítulo 4.

Para obtener el resultado del riesgo, se suma el valor de la probabilidad promedio más el valor del impacto. La misma consideración para cada tipo de activo, como se puede observar en las siguientes tablas.

Aplicando a los activos de Información se tiene:

ACTIVOS DE INFORMACIÓN	VULNERABILIDAD / AMENAZA	N.1 Fuego (M)	N.2 Daños por agua (B)	N.3 Otros Desastres Naturales (B)	E.1 Errores de los usuarios (A)	E.2 Errorres del Administrador (A)	E.3 Errores de monitorización (M)	E.15 Alteración accidental de la Información (M)	A.3 Manipulación de Registros de Actividad (A)	A.13 Repudio (M)	A.25 Robo (M)	Probabilidad Promedio
Documento de Políticas de seguridad	Ausencia de revisión, actualización de documento de políticas de seguridad (A)	x	x	x	4	4	3	3	4	3	3	3
Documento Plan de Contingencias tecnológicas	Ausencia del documento, falta de revisión y aprobación (A)	3	2	2	x	x	x	x	x	x	3	3
Registro de Backups	Ausencia de datos importantes en el registro (M)	x	x	x	3	3	2	2	3	2	2	2
Registro de Incidentes	Ausencia de capacitación, para el debido llenado y manejo de registro (A)	x	x	x	4	4	3	3	4	3	3	3
Registro de entrada al CPD	Ausencia de control sobre el llenado del registro (M)	x	x	x	3	3	2	2	3	2	2	2

Tabla 6.18 Resultado de estimación de la probabilidad para activos de Tipo Información, aplicando los niveles de vulnerabilidad y amenaza

Fuente: Elaboración propia

NOTA. Donde “x” significa que no se aplica.

Aplicando a los activos de Datos se tiene:

TIPO DE ACTIVOS - DATOS	VULNERABILIDAD	AMENAZAS	E.2 Errorres del Administrador (A)	E.3 Errores de monitorización (M)	E.15 Alteración accidental de la Información (M)	E.18 Destrucción de Información (A)	E.19 Fugas de Información (A)	A.6 Abuso de privilegios de acceso (M)	A.11 Acceso no autorizado (M)	A.15 Modificación deliberada de la información (M)	A.18 Destrucción de Información (A)	A.19 Divulgación de Información (M)	Probabilidad Promedio
Datos de configuración	Ausencia de datos de configuración (A)		4	3	3	4	4	3	3	3	4	3	**3**
Copias de Respaldo	Ausencia de copias de respaldo (A)		4	3	3	4	4	3	3	3	4	3	**3**
Código fuente de programa	Ausencia de restricción de acceso al código fuente (A)		4	3	3	4	4	3	3	3	4	3	**3**
Código ejecutable de programa	Ausencia de protección del código ejecutable (M)		3	2	2	3	3	2	2	2	3	2	**2**
Datos de prueba	Ausencia de protección de datos de prueba (M)		3	2	2	3	3	2	2	2	3	2	**2**

Tabla 6.19 Resultado de Estimación de la probabilidad para activos de Tipo Datos, aplicando los niveles de vulnerabilidad y amenaza

Fuente: Elaboración propia

Aplicando a los activos de Servicio se tiene:

TIPO DE ACTIVO SERVICIOS	VULNERABILIDAD	AMENAZAS	E.1 Errores de los usuarios (B)	E.2 Errorres del Administrador (A)	E.9 Errores de Re-encaminamiento (M)	E.10 Errorres de Secuencia (M)	E.15 Alteración accidental de la Información (B)	E.18 Destrucción de Información (A)	E.19 Fugas de Información (A)	A.5 Suplantación de la Identidad del Usuario (A)	A.6 Abuso de privilegios de acceso (M)	A.7 Uso no previsto (B)	A.9 Re-encaminamiento de mensajes (M)	A.11 Acceso no autorizado (M)	A.13 Repudio (M)	A.15 Modificación deliberada de la información (M)	A.18 Destrucción de Información (A)	A.19 Divulgación de Información (M)	A.24 Denegación de Servicio (A)	Probabilidad Promedio
Página Web	Software desactualizado (A)		2	4	3	3	2	4	4	4	3	2	3	3	3	3	4	3	4	**3**
Correo electrónico	Ausencia de capacitación del usuario sobre manejo de correo electrónico (A)		2	4	3	3	2	4	4	4	3	2	3	3	3	3	4	3	4	**3**
Servicio de almacenamiento de archivos	Ausencia de capacitación del usuario en el manejo de almacenamiento de archivos (M)		1	3	2	2	1	3	3	3	2	1	2	2	2	2	3	2	3	**2**
Servicio de Active Directory	Desconocimiento de la configuración y administración de parte del administrador (A)		2	4	3	3	2	4	4	4	3	2	3	3	3	3	4	3	4	**3**
Servicio de VPN	Ausencia de contrato con el proveedor del servicio (A)		2	4	3	3	2	4	4	4	3	2	3	3	3	3	4	3	4	**3**

Tabla 6.20 Resultado de estimación de la probabilidad para activos de Tipo Servicios, aplicando los niveles de vulnerabilidad y amenaza

Fuente: Elaboración propia

Aplicando a los activos de Redes de Comunicaciones se tiene:

TIPO DE ACTIVO REDES DE COMUNICACIONES	VULNERABILIDAD / AMENAZAS	I.8 Fallo de servicios de comunicaciones (A)	E.2 Errorres del Administrador (A)	E.9 Errores de Re-encaminamiento (A)	E.10 Errorres de Secuencia (M)	E.15 Alteración accidental de la Información (M)	E.18 Destrucción de Información (A)	E.19 Fugas de Información (A)	E.24 Caida del sistema por agotamiento de recursos (A)	A.5 Suplantación de la identidad del Usuario (A)	A.6 Abuso de privilegios de acceso (M)	A.7 Uso no previsto (M)	A.9 Re-encamina-miento de mensajes (M)	A.11 Acceso no autorizado (M)	A.12 Análisis de tráfico (M)	A.14 Interceptación de información (M)	A.15 Modificación deliberada de la información (M)	A.19 Divulgación de Información (M)	A.24 Denegación de Servicio (A)	**Probabilidad Promedio**
Red telefónica	Conexiones de red pública sin protección (M)	3	3	3	2	2	3	3	3	3	2	2	2	2	2	2	x	2	3	2
Red local	Conexión deficiente de los cables de datos (M)	3	3	3	2	x	x	3	3	3	2	2	2	2	2	2	2	2	3	2
Internet	Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento) (A)	4	4	4	3	3	4	4	4	4	3	3	3	3	3	3	3	3	4	3
Red inalámbrica	Ausencia de identificación y autenticación de emisor y receptor (M)	3	3	3	2	2	3	3	3	3	2	2	2	2	2	2	2	2	3	2

Tabla 6.21 Resultado de estimación de probabilidad para activos de tipo Redes de Comunicaciones, aplicando los niveles de vulnerabilidad y amenaza

Fuente: Elaboración propia

Aplicando a los activos de Software se tiene:

TIPO DE ACTIVO SOFTWARE	VULNERABILIDAD / AMENAZAS	I.5 Avería de origen físico o lógico (A)	E.1 Errores de los usuarios (M)	E.2 Errores del Administrador (A)	E.8 Difusión no intencionada de Software Dañino (M)	E.9 Errores de Re-encaminamiento (M)	E.10 Errores de Secuencia (M)	E.15 Alteración accidental de la Información (M)	E.18 Destrucción no intencionada de Información (M)	E.19 Fugas de Información (M)	E.20 Vulnerabilidades de los programas (M)	E.21 Errores de Mantenimiento/ actualización de programas (A)	E.24 Caida del sistema por agotamiento de recursos (A)	A.4 Manipulación de la configuración (A)	A.5 Suplantación de la Identidad del Usuario (A)	A.6 Abuso de privilegios de acceso (A)	A.7 Uso no previsto (M)	A.8 Difusión intencionada de Software Dañino (A)	A.9 Re-encaminamiento de mensajes (A)	A.11 Acceso no autorizado (A)	A.15 Modificación deliberada de la información (A)	A.18 Destrucción intencionada de Información (A)	A.19 Divulgación de Información (M)	A.22 Manipulación de programas (M)	Semi total Probabilidad Promedio	**Total Probabilidad Promedio**
Aplicación específica del negocio (sistema de contabilidad, sistema de producción)	Especificaciones incompletas o no claras para los desarrolladores (A)	4	3	4	3	3	3	3	3	3	3	4	4	4	4	4	3	4	4	4	4	4	3	3	4	**4**
	Gestión deficiente de las contraseñas (A)	4	3	4	3	3	3	3	3	3	3	4	x	4	4	4	3	4	4	4	4	4	3	3	4	
	Software nuevo o inmaduro (A)	4	3	4	x	3	3	3	3	3	3	4	4	4	4	4	3	4	4	4	4	4	3	3	4	
Ofimática	Descarga y uso no controlados de software (M)	3	2	3	2	2	2	2	2	2	2	3	3	3	3	3	2	3	3	3	3	3	2	2	3	**2**
Navegador Web	Configuración incorrecta de parámetros (M)	3	2	3	2	2	2	2	2	2	2	3	3	3	3	3	2	3	3	3	3	3	2	2	3	**3**
Servidor de Aplicaciones	Ausencia de copias de respaldo (M)	3	2	3	2	x	x	x	2	x	x	3	3	3	x	3	2	3	x	3	3	3	x	x	3	**3**
Servidor de Correo Electrónico	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario (A)	4	3	4	3	3	3	3	3	3	x	4	x	4	4	4	3	4	4	4	4	4	3	3	4	**4**
	Ausencia de copias de respaldo (A)	4	3	3	3	x	x	x	3	3	x	4	4	4	x	4	3	4	x	4	4	4	x	x	4	
Antivirus	Ausencia de software antivirus (A)	4	3	4	3	3	3	3	3	3	3	4	4	x	x	x	x	4	4	x	4	4	3	3	3	**3**
	Ausencia de actualización (M)	3	2	3	2	2	2	2	2	2	2	3	3	x	x	x	x	3	3	x	3	3	2	2	3	
Sistema Operativo	Ausencia de mecanismos de identificación y autentificación, como usuario y contraseña al inicio (M)	x	2	3	2	x	x	2	2	2	2	x	x	3	3	3	2	3	3	3	3	3	2	2	3	**2**
Sistema de gestión de Base de Datos	Ausencia de control de cambios eficaz (A)	4	3	4	3	3	3	3	3	3	3	4	4	4	4	4	3	4	4	4	4	4	3	3	4	**4**
	Tablas de contraseñas sin protección (A)	4	3	4	x	x	x	3	3	3	x	4	x	4	4	4	x	x	x	4	4	4	3	x	4	
	Asignación errada de los derechos de acceso (A)	4	3	4	x	x	x	3	3	3	x	4	x	4	4	4	x	x	x	4	4	4	3	3	4	

Tabla 6.22 Resultado de estimación de probabilidad para activos de tipo software, aplicando los niveles de vulnerabilidad y amenaza

Fuente: Elaboración propia

Nota. Donde “x” significa que no aplica.

Aplicando a los activos de Hardware se tiene:

TIPO DE ACTIVO HARDWARE	VULNERABILIDAD / AMENAZAS	I.5 Avería de origen físico o lógico (M)	E.2 Errorres del Administrador (A)	E.4 Errores de Configuración (A)	E.23 Errores de Mantenimiento/actualización de equipos (A)	E.24 Caida del sistema por agotamiento de recursos (M)	E.25 Pérdida de equipos (M)	A.4 Manipulación de la configuración (A)	A.6 Abuso de privilegios de acceso (M)	A.7 Uso no previsto (M)	A.11 Acceso no autorizado (M)	A.23 Manipulación de los equipos (M)	A.24 Denegación de Servicio (M)	A.25 Robo (A)	A.26 Ataque destructivo (M)	**Probabilidad Promedio**
Equipo portátil	Mantenimiento insuficiente / mala instalación (M)	2	3	3	3	2	x	3	2	2	2	2	2	x	2	**2**
Equipo de respaldo	Falta de condiciones de funcionamiento (M)	2	3	3	3	2	x	3	2	x	x	2	2	x	x	**2**
Medios de Impresión y escaners	Mantenimiento insuficiente / mala instalación (M)	2	3	3	3	2	x	3	2	2	2	2	2	x	2	**2**
Switch	Ausencia de dispositivos de reemplazo (M)	2	3	3	3	2	2	3	2	2	2	x	x	3	2	**2**
Router	Ausencia de un eficiente control de cambios en la configuración (A)	3	4	4	4	3	x	4	3	x	3	3	3	x	3	**3**
Firewall	Ausencia de un eficiente control de cambios en la configuración (A)	3	4	4	4	3	x	4	3	3	3	3	3	x	3	**3**
Punto de acceso inalámbrico	Mantenimiento insuficiente / mala instalación (M)	2	3	3	3	2	2	3	2	2	2	2	2	x	2	**2**
Central telefónica	Mantenimiento insuficiente / mala instalación (A)	3	4	4	4	3	x	4	3	3	3	3	3	x	x	**3**

Tabla 6.23 Resultado de estimación de probabilidad para activos de tipo hardware, aplicando niveles de vulnerabilidad y amenaza

Fuente: Elaboración propia

Nota. Donde “x” significa que no aplica.

Aplicando a los activos de Equipamiento Auxiliar se tiene:

TIPO DE ACTIVO EQUIPAMIENTO AUXILIAR	AMENAZAS / VULNERABILIDAD	I.5 Avería de origen físico o lógico (M)	I.6 Corte del Suministro eléctrico (M)	I.7 Condiciones inadecuadas de temperatura o humedad (M)	I.9 Interrupción de otros servicios y suministros esenciales (M)	I.11 Emanaciones Electromagnéticas (M)	E.23 Errores de Mantenimiento/actualización de equipos (M)	E.25 Pérdida de equipos (M)	A.7 Uso no previsto (M)	A.11 Acceso no autorizado (B)	A.23 Manipulación de los equipos (B)	A.25 Robo (M)	A.26 Ataque destructivo (M)	**Promedio Probabilidad**
Fuentes de Alimentación	Ausencia de dispositivos de reemplazo (M)	2	2	2	x	x	2	2	x	1	1	2	2	**2**
Fuentes de Alimentación Ininterrumpida	Mantenimiento insuficiente / mala instalación (A)	3	3	3	x	x	3	x	x	2	x	x	3	**3**
Equipos de Climatización	Mantenimiento insuficiente / mala instalación (A)	3	3	3	3	x	3	x	x	2	2	x	3	**3**
Cableado eléctrico	Mantenimiento insuficiente / mala instalación (M)	2	2	2	x	2	2	2	2	x	x	x	2	**2**
Cableado de datos	Mantenimiento insuficiente / mala instalación (M)	2	x	2	x	2	2	2	2	1	x	x	2	**2**
Fibra óptica	Mantenimiento insuficiente / mala instalación (M)	2	x	2	x	x	2	2	x	1	1	x	2	**2**

Tabla 6.24 Resultado de estimación de probabilidad para activos de Equipamiento Auxiliar, aplicando niveles de vulnerabilidad y amenazas

Fuente: Elaboración propia

Aplicando a los activos de Instalaciones se tiene:

TIPO DE ACTIVO INSTALACIONES	AMENAZAS / VULNERABILIDAD	N.1 Fuego (A)	N.2 Inundaciones (M)	N.3 Otros Desastres Naturales (M)	I.11 Emanaciones Electromagnéticas (M)	E.18 Destrucción no intencionada de Información (M)	E.19 Fugas de Información (A)	A.7 Uso no previsto (M)	A.11 Acceso no autorizado (A)	A.15 Modificación deliberada de la información (A)	A.18 Destrucción intencionada de información (A)	A.26 Ataque destructivo (A)	**Semitotal Probabilidad Promedio**	**Total Probabilidad Promedio**
Oficinas	Ausencia de extintor (M)	3	x	2	x	x	x	2	x	x	3	3	**2**	**2**
	Ausencia de cámaras de seguridad (M)	3	x	2	x	2	3	2	3	3	3	3	**3**	
Canalizaciones	Ausencia de planos de instalación (M)	x	x	2	2	2	3	2	3	x	3	3	**2**	**2**
	Instalación precaria (M)	3	x	2	2	2	3	2	3	x	3	3	**2**	
Centro de Procesamiento de Datos (CPD)	Ausencia de control de ingreso en la entrada al CPD (M)	x	x	x	x	2	3	2	3	3	3	3	**3**	**3**
	Ausencia de sensores de humo y temperatura (A)	4	X	3	x	x	x	x	x	x	4	4	**4**	

Tabla 6.25 Resultado de estimación de probabilidad para activos de Instalaciones aplicando niveles de vulnerabilidad y amenazas

Fuente: Elaboración propia

Nota. Donde “x” significa que no aplica.

Aplicando a los activos de personal se tiene:

TIPO DE ACTIVO PERSONAL	AMENAZAS / VULNERABILIDAD	E.7 Fugas de Información (M)	E.19 Deficiencias en la organización (A)	A.25 Robo (A)	A.26 Ataque destructivo (A)	A.28 Indisponibilidad del personal (A)	A.29 Extorsión (M)	A.30 Ingeniería social (M)	Semitotal Probabilidad Promedio	**Total Probabilidad Promedio**
Usuarios Externos	Ausencia de control sobre los accesos a la red y equipos de computación (A)	3	4	4	4	x	3	3	3	**3**
	Desconocimiento de las políticas sobre seguridad de la información de la empresa (M)	2	3	3	3	x	2	2	3	
Usuarios Internos	Uso incorrecto de hardware y software (M)	2	3	3	3	x	x	2	3	**3**
	Ausencia o desconocimiento de políticas para el uso correcto de los dispositivos de TIC (M)	2	3	3	3	x	2	2	3	
	Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo (M)	2	3	x	3	3	2	2	3	
Administradores de Sistemas	Ausencia de control sobre los accesos a la información (A)	3	4	4	4	x	3	3	4	**4**
Programadores	Ausencia de control de cambios eficaces sobre los programas (A)	3	4	4	4	x	3	3	4	**4**
Consultores	Ausencia de controles de acceso lógico y fisico a las intalaciones (A)	3	4	4	4	x	3	3	4	**4**
Proveedores	Ausencia de contrato (A)	3	4	4	4	4	3	3	4	**3**
	Desconocimiento de las políticas sobre seguridad de la información de la empresa a la cual presta servicio (M)	2	3	3	3	x	2	2	3	

Tabla 6.26 Resultado de estimación de probabilidad para Personal aplicando niveles de vulnerabilidad y amenazas

Fuente: Elaboración propia

Nota. Donde “x” significa que no aplica.

6.2.2.3 NIVEL DE ESTIMACIÓN DEL RIESGO

La estimación del riesgo asigna valores a la probabilidad y al impacto.

La siguiente tabla indica la probabilidad frente al impacto, relacionado con el escenario de incidente.

	Probabilidad del escenario de incidente	**0**	**1**	**2**	**3**	**4**
Impacto	Niveles	Muy Baja	Baja	Media	Alta	Muy Alta
0	Muy Bajo	0	1	2	3	4
1	Bajo	1	2	3	4	5
2	Medio	2	3	4	5	6
3	Alto	3	4	5	6	7
4	Muy Alto	4	5	6	7	8

Tabla 6.27 Estimación del riesgo
Fuente: Anexo E Norma NB/ISO/IEC 27005

El riesgo resultante se mide en una escala de 0 a 8, teniendo en cuenta la siguiente clasificación:

- Riesgo bajo: 0 – 2 (color blanco)
- Riesgo medio: 3 – 5 (color amarillo)
- Riesgo alto: 6 – 8 (color rojo)

Para el impacto se asume la degradación del 100% del activo, ver la Tabla 6.13

La siguiente tabla representa la Matriz de Riesgo donde se observa el resultado del riesgo basado en la probabilidad y el impacto de la Tabla 6.27

TIPO	**ACTIVOS**	**AMENAZAS**	**VULNERABILIDADES**	**IMPACTO**	**PROBA-BILIDAD**	**RIESGO**
INF	Documento de Políticas de seguridad	7 amenazas (E.1 , E.2 , E. 3 , E.15 A.3 , A.13 , A.25)	Ausencia de revisión, actualización de documento de políticas de seguridad	3	3	6 (Alto)

INF	Documento Plan de Contingencias tecnológicas	4 amenazas (N.1 , N.2 , N.3 , A.25)	Ausencia del documento, falta de revisión y aprobación	2	3	5 (Medio)
INF	Registro de Backups	7 amenazas (E.1 , E.2 , E.3 , E.15 , A.3 , A.13 , A.25)	Ausencia de datos importantes en el registro	3	2	5 (Medio)
INF	Registro de Incidentes	7 amenazas (E.1 , E.2 , E.3 ,E.15 ,A.3 ,A.13 ,A.25)	Ausencia de capacitación, para el debido llenado y manejo del registro	3	3	6 (Alto)
INF	Registro de entrada al CPD	7 amenazas (E.1 ,E.2 , E.3 , E.15 A.3 , A.13 , A.25)	Ausencia de control sobre el llenado del registro	2	2	5 (Medio)
D	Datos de configuración	10 amenazas (E.2 , E.3 , E.15 , E.18 ,E.19 , A.6 , A.11 , A.15 A.18, A.19)	Ausencia de datos de configuración	4	3	7 (Alto)
D	Copias de Respaldo	10 amenazas (E.2 , E.3 , E.15 E.18 , E.19 , A.6 , A.11 , A.15 , A.18 , A.19)	Ausencia de copias de respaldo	3	3	6 (Alto)
D	Código fuente de programa	10 amenazas (E.2 E.3 E.15 E.18 E.19 A.6 A.11 A.15 A.18 A.19)	Ausencia de restricción de acceso al código fuente	4	3	7 (Alto)
D	Código ejecutable de programa	10 amenazas (E.2 E.3 E.15 E.18 E.19 A.6 A.11 A.15 A.18 A.19)	Ausencia de protección del código ejecutable	3	2	5 (Medio)
D	Datos de prueba	10 amenazas (E.2 , E.3 , E.15 , E.18 , E.19 , A.6 , A.11 , A.15 , A.18 , A.19)	Ausencia de protección de datos de prueba	2	2	4 (Medio)
S	Página Web	17 amenazas (E.1 , E.2 , E.9 , E.10 , E.15 , E.18 , E.19 , A.5 A.6 , A.7 , A.9 , A.11 , A.13 , A.15 A.18 , A.19 , A.24)	Software desactualizado	3	3	6 (Alto)
S	Correo electrónico	17 amenazas (E.1 , E.2 , E.9 , E.10 , E.15 , E.18 , E.19 , A.5 , A.6, A.7 , A.9 , A.11 , A.13 , A.15 , A.18 , A.19 , A.24)	Ausencia de capacitación del usuario sobre manejo de correo electrónico	4	3	7 (Alto)

S	Servicio de almacenamiento de archivos	17 amenazas (E.1 ,E.2 , E.9 , E.10 , E.15 , E.18 , E.19 , A.5 , A.6 A.7 , A.9 , A.11 , A.13 , A.15 , A.18 , A.19 , A.24)	Ausencia de capacitación del usuario en el manejo de almacenamiento de archivos	2	2	4 (Medio)
S	Servicio de Active Directory	17 amenazas (E.1 , E.2 , E.9 , E.10 , E.15 ,E.18 , E.19 , A.5 , A.6 , A.7 , A.9 , A.11 , A.13 , A.15 , A.18 , A.19 , A.24)	Desconocimiento de la configuración y administración de parte del administrador	3	3	6 (Alto)
S	Servicio de VPN	17 amenazas (E.1 , E.2 , E.9 , E.10 , E.15 , E.18 , E.19 , A.5 , A.6 A.7 , A.9 , A.11 , A.13 , A.15 , A.18 , A.19 , A.24)	Ausencia de contrato con el proveedor del servicio	4	3	7 (Alto)
SW	Aplicación específica del negocio (sistema de contabilidad, sistema de producción)	23 amenazas (I.5 , E.1 , E.2 , E.8 E.9 , E.10 , E.15 , E.18 , E.19 , E.20 , E.21 , E.24 , A.4 , A.5 , A.6 , A.7 , A.8 , A.9 , A.11 , A.15 A.18 , A.19 , A.22)	Especificaciones incompletas o no claras para los desarrolladores Gestión deficiente de las contraseñas Software nuevo o inmaduro	4	4	8 (Alto)
SW	Ofimática	23 amenazas (I.5 , E.1 , E.2 , E.8 E.9 , E.10 , E.15 , E.18 , E.19 , E.20 , E.21 , E.24 , A.4 , A.5 , A.6 , A.7 , A.8 , A.9 , A.11 , A.15 A.18 , A.19 , A.22)	Descarga y uso no controlados de software	3	2	5 (Medio)
SW	Navegador Web	23 amenazas (I.5 , E.1 , E.2 , E.8 E.9 , E.10 , E.15 , E.18 , E.19 , E.20 , E.21 , E.24 , A.4 , A.5 , A.6 , A.7 , A.8 , A.9 , A.11 , A.15 A.18 , A.19 , A.22)	Configuración incorrecta de parámetros	2	3	5 (Medio)
SW	Servidor de Aplicaciones	14 amenazas (I.5 , E.1 , E.2 , E.8 E.18 , E.21 , E.24 , A.4 , A.6 , A.7 A.8 , A.11 , A.15 , A.18)	Ausencia de copias de respaldo	3	3	6 (Alto)

SW	Servidor de Correo Electrónico	22 amenazas (I.5 , E.1 , E.2 , E.8 E.9 , E.10 , E.15 , E.18 , E.19 , E.21 , E.24 , A.4 , A.5 , A.6 , A.7 , A.8 , A.9 , A.11 , A.15 , A.18 , A.19 , A.22)	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario Ausencia de copias de respaldo	4	4	8 (Alto)
SW	Antivirus	18 amenazas (I.5 , E.1 , E.2 , E.8 , E.9 , E.10 , E.15 , E.18 , E.19 , E.20 , E.21 , E.24 , A.8 , A.9 , A.15 , A.18 , A.19 , A.22)	Ausencia de software antivirus Ausencia de actualización	1	3	4 (Medio)
SW	Sistema Operativo	18 amenazas (E.1 , E.2 , E.8 , E.15 , E.18 , E.19 , E.20 , A.4 , A.5 , A.6 , A.7 , A.8 , A.9 , A.11 , A.15 , A.18 , A.19 , A.22)	Ausencia de mecanismos de identificación y autentificación, como usuario y contraseña al inicio	3	2	5 (Medio)
SW	Sistema de gestión de Base de Datos	23 amenazas (I.5 , E.1 , E.2 , E.8 , E.9 , E.10 , E.15 , E.18 , E.19 , E.20 , E.21 , E.24 , A.4 , A.5 , A.6 , A.7 , A.8 , A.9 , A.11 , A.15 , A.18 , A.19 , A.22)	Ausencia de control de cambios eficaz Tablas de contraseñas sin protección Asignación errada de los derechos de acceso	4	4	8 (Alto)
HW	Equipo portátil	12 amenazas (I.5 , E.2 , E.4 , E.23 , E.24 , A.4 , A.6 , A.7 , A.11 , A.23 , A.24 , A.26)	Mantenimiento insuficiente / mala instalación	3	2	5 (Medio)
HW	Equipo de respaldo	9 amenazas (I.5 , E.2 , E.4 , E.23 , E.24 , A.4 , A.6 , A.23 , A.24)	Falta de condiciones de funcionamiento	3	2	5 (Medio)
HW	Medios de Impresión y escáners	12 amenazas (I.5 , E.2 , E.4 ,E.23 , E.24 , A.4 , A.6 , A.7 , A.11 , A.23 , A.24 , A.26)	Mantenimiento insuficiente / mala instalación	2	2	4 (Medio)
HW	Switch	12 amenazas (I.5 , E.2 , E.4, E.23 , E.24 , E.25 , A.4 , A.6 , A.7, A.11 , A.25 , A.26)	Ausencia de dispositivos de reemplazo	3	2	5 (Medio)
HW	Router	11 amenazas (I.5 , E.2 , E.4 , E.23 , E.24 , A.4 , A.6 , A.11 , A.23 , A.24 , A.26)	Ausencia de un eficiente control de cambios en la configuración	3	3	6 (Alto)

HW	Firewall	12 amenazas (I.5 , E.2 , E.4 , E.23 , E.24 , A.4 , A.6 , A.7 , A.11 , A.23 , A.24 , A.26)	Ausencia de un eficiente control de cambios en la configuración	4	3	7 (Alto)
HW	Punto de acceso inalámbrico	13 amenazas (I.5 , E.2 , E.4 , E.23 , E.24 , E.25 , A.4 , A.6 , A.7 , A.11 , A.23 , A.24 , A.26)	Mantenimiento insuficiente / mala instalación	3	2	5 (Medio)
HW	Central telefónica	11 amenazas (I.5 , E.2 , E.4 , E.23 , E.24 , A.4 , A.6 , A.7 , A.11 , A.23 , A.24)	Mantenimiento insuficiente / mala instalación	4	3	7 (Alto)
COM	Red telefónica	17 amenazas (I.8 , E.2 , E.9 , E.10 , E.15 , E.18 , E.19 , E.24 , A.5 , A.6 A.7 , A.9 , A.11 , A.12 , A.14 , A.19 , A.24)	Conexiones de red pública sin protección	3	2	5 (Medio)
COM	Red local	16 amenazas (I.8 , E.2 , E.9 , E.10 , E.19 , E.24 , A.5 , A.6 A.7 , A.9 , A.11 , A.12 , A.14 A.15 , A.19 , A.24)	Conexión deficiente de los cables de datos	3	2	5 (Medio)
COM	Internet	18 amenazas (I.8 , E.2 , E.9 , E.10 , E.15 E.18 , E.19 , E.24 , A.5 , A.6 A.7 , A.9 , A.11 , A.12 , A.14 A.15 , A.19 , A.24)	Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento)	3	3	6 (Alto)
COM	Red inalámbrica	18 amenazas (I.8 , E.2 , E.9 , E.10 , E.15 , E.18 , E.19 , E.24 , A.5 , A.6 A.7 , A.9 , A.11 , A.12 , A.14 A.15 , A.19 , A.24)	Ausencia de identificación y autenticación de emisor y receptor	3	2	5 (Medio)
AUX	Fuentes de Alimentación	9 amenazas (I.5 , I.6 , I.7 , E.23 E.25 , A.11 , A.23 , A.25 , A.26)	Ausencia de dispositivos de reemplazo	1	2	3 (Medio)
AUX	Fuentes de Alimentación Ininterrumpida	6 amenazas (I.5 , I.6 , I.7 , E.23 , A.11 , A.26)	Mantenimiento insuficiente / mala instalación	3	3	6 (Alto)
AUX	Equipos de Climatización	8 amenazas (I.5 , I.6 , I.7 , I.9 , E.23 , A.11 , A.23 , A.26)	Mantenimiento insuficiente / mala instalación	2	3	5 (Medio)

AUX	Cableado eléctrico	8 amenazas (I.5 , I.6 , I.7 , I.11 E.23 , E.25 , A.7 , A.26)	Mantenimiento insuficiente / mala instalación	2	2	4 (Medio)
AUX	Cableado de datos	8 amenazas (I.5 , I.7 , I.11 , E.23 , E.25 , A.7 , A.11 , A.26)	Mantenimiento insuficiente / mala instalación	3	2	5 (Medio)
AUX	Fibra óptica	7 amenazas (I.5 , I.7 , E.23 , E.25 , A.11 , A.23 , A.26)	Mantenimiento insuficiente / mala instalación	3	2	5 (Medio)
I	Oficinas	5 amenazas (N.1 , N.3 , A.7 , A.18 , A.26)	Ausencia de extintor Ausencia de cámaras de seguridad	3	3	6 (Alto)
I	Canalizaciones	9 amenazas (N.1 , N.3 , I.11 , E.18 , E.19 , A.7 , A.11 , A.18 , A.26)	Ausencia de planos de instalación precaria	3	2	5 (Medio)
I	Centro de Procesamiento de Datos	9 amenazas (N.1 , N.3 , E.18 , E.19 , A.7 , A.11 , A.15 , A.18 , A.26)	Ausencia de control de ingreso en la entrada al CPD Ausencia de sensores de humo y temperatura	4	3	7 (Alto)
P	Usuarios Externos	6 amenazas (E.7 , E.19 , A.25 , A.26 , A.29 , A.30)	Ausencia de control sobre los accesos a la red y equipos de computación Desconocimiento de las políticas sobre seguridad de la información de la empresa	3	3	6 (Alto)
P	Usuarios Internos	7 amenazas (E.7 , E.19 , A.25 , A.26 , A.28 , A.29 , A.30)	Uso incorrecto de hardware y software Ausencia o desconocimiento de políticas para el uso correcto de los dispositivos de TIC Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo	3	3	6 (Alto)
P	Administradores de Sistemas	6 amenazas (E.7 , E.19 , A.25 , A.26 , A.29 , A.30)	Ausencia de control sobre los accesos a la información	3	4	7 (Alto)
P	Programadores	6 amenazas (E.7 , E.19 , A.25 , A.26 , A.29 , A.30)	Ausencia de control de cambios eficaces sobre los programas	3	4	7 (Alto)

P	Consultores	6 amenazas (E.7 , E.19 , A.25 , A.26 , A.29 , A.30)	Ausencia de controles de acceso lógico y físico a las instalaciones	3	4	7 (Alto)
P	Proveedores	7 amenazas (E.7 , E.19 , A.25 , A.26 , A.28 , A.29 , A.30)	Ausencia de contrato Desconocimiento de las políticas sobre seguridad de la información de la empresa a la cual presta servicio	3	3	6 (Alto)

Tabla 6.28 Matriz de Riesgo aplicando resultados de la probabilidad estimada y el impacto
Elaboración: Fuente propia

En la *Tabla 6.28* se encuentran identificados con color rojo los riesgos altos y con amarillo los riesgos medios, dependiendo de un análisis más profundo y específico para cada empresa, estos resultados cambiaran, la presente tabla, es un modelo, el cual es aplicable para realizar la estimación del riesgo.

Todos los riesgos altos que han sido identificados están asociados con los controles que ya han sido analizados en los Capítulos 4 y 5. Se analizará cada una de las vulnerabilidades para asociar al respectivo control.

- ✓ La Ausencia de revisión, actualización de documento de políticas de seguridad representa un riesgo alto. Asociado al 1er Control
- ✓ La Ausencia de capacitación, para el debido llenado y manejo de registros de incidentes representa un riesgo alto. Asociado al 12o Control
- ✓ La ausencia de datos de configuración de equipos sensibles representa un riesgo alto. Asociado al 8º Control
- ✓ La Ausencia de copias de respaldo de equipos sensibles. Asociado al 8º Control
- ✓ La Ausencia de restricción de acceso al código fuente. Asociado al 5º Control
- ✓ Software desactualizado en la página Web. Asociado al 8º Control
- ✓ Ausencia de capacitación del usuario sobre manejo de correo electrónico. Asociado al 3er Control
- ✓ Ausencia de contrato con el proveedor del servicio de VPN. Asociado al 11º Control

- ✓ Aplicación específica del negocio (sistema de contabilidad, sistema de producción). Especificaciones incompletas o no claras para los desarrolladores, gestión deficiente de las contraseñas, Software nuevo o inmaduro. Asociado al 10º Control
- ✓ Ausencia de copias de respaldo del Servidor de Aplicaciones. Asociado al 8º Control
- ✓ Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario. Asociado al 5º Control
- ✓ Ausencia de copias de respaldo. Del servidor de correo electrónico. Asociado al 8º Control
- ✓ Ausencia de control de cambios eficaz. Tablas de contraseñas sin protección Asignación errada de los derechos de acceso en la Gestión de base de datos. Asociado al 5º Control
- ✓ Ausencia de un eficiente control de cambios en la configuración en el router y en el firewall. Asociado al 8º Control
- ✓ Mantenimiento insuficiente / mala instalación de la central telefónica. Asociado al 9º Control
- ✓ Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento) de Internet. Asociado al 9º Control
- ✓ Mantenimiento insuficiente / mala instalación de la UPS. Asociado al 7º Control
- ✓ Ausencia de extintor, Ausencia de cámaras de seguridad en las oficinas. Asociado al 7º Control
- ✓ Ausencia de control de ingreso en la entrada al CPD. Asociado al 7º Control
- ✓ Ausencia de sensores de humo y temperatura en el Centro de Procesamiento de Datos. Asociado al 7º Control
- ✓ Ausencia de control sobre los accesos a la red y equipos de computación. Asociado al 5º Control
- ✓ Desconocimiento de las políticas sobre seguridad de la información de la empresa de los usuarios externos. Asociado al 1er Control
- ✓ Uso incorrecto de hardware y software de usuarios internos. Asociado al 3er Control

- ✓ Ausencia o desconocimiento de políticas para el uso correcto de los dispositivos de TIC. Asociados al 1er Control y al 14o control
- ✓ Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo de los usuarios internos. Asociado al 5º Control
- ✓ Ausencia de control sobre los accesos a la información, de los Administradores de sistemas. Asociado al 5º Control
- ✓ Ausencia de control de cambios eficaces sobre los programas de los programadores. Asociado al 10º Control
- ✓ Ausencia de controles de acceso lógico y físico a las instalaciones de los consultores. Asociado al 5º Control
- ✓ Ausencia de contrato de los proveedores. Asociado al 11º Control
- ✓ Desconocimiento de las políticas sobre seguridad de la información de la empresa a la cual presta servicio de los proveedores. Asociado al 11º Control

Por tanto se tiene como resultado que los controles necesarios que deben ser priorizados con detalle, atendiendo las vulnerabilidades identificadas, para evitar las amenazas asociadas, para mitigar riesgos altos corresponde a los controles:

- ✓ 1er control Políticas de Seguridad de la Información
- ✓ 3er control Seguridad ligada a los recursos humanos
- ✓ 5º control Control de acceso
- ✓ 7º control Seguridad física y del ambiente
- ✓ 8º control Seguridad de las operaciones
- ✓ 9º control Seguridad de las comunicaciones
- ✓ 10º control Adquisición, desarrollo y mantenimiento del sistema
- ✓ 11er control Relaciones con el proveedor
- ✓ 12º control Administración de incidentes de seguridad de la información
- ✓ 14º control Cumplimiento

6.2.3 EVALUACIÓN DEL RIESGO

Con el fin de evaluar los riesgos descritos en la matriz de riesgo, las Empresas corredoras de seguros y reaseguros deberían tomar en consideración su contexto, el

objetivo de la empresa, puntos de vista de las partes interesadas, considerar las consecuencias y tratarlos según corresponda, en este punto existirá gran diferencia en los resultados, entre empresas corredoras.

La evaluación del riesgo utiliza la comprensión del riesgo que se obtiene mediante el análisis del riesgo para tomar decisiones sobre acciones futuras. Las decisiones deberían incluir: prioridades para el tratamiento de los riesgos considerando los valores estimados.

PRIORIZACIÓN DEL RIESGO

En la Matriz de Riesgo de la *Tabla 6.28* se obtuvo como resultado, riesgo medio y riesgo alto, por criterios personales, de acuerdo al conocimiento que mi persona posee en el área de Tecnologías de Información, con relación a los escenarios de incidentes que llevan a los riesgos identificados, se puede establecer el tipo de tratamiento, como se puede apreciar en la siguiente tabla, donde se propone la forma en la que pueden ser tratados :

Nivel de riesgo	Tipo de Tratamiento
Alto	Reducir
Alto	Evitar
Alto	Transferir
Alto	Aceptar
Medio	Reducir

Tabla 6.29 Priorización de Riesgos aplicando criterio técnico personal
Fuente: Elaboración propia

Siendo la decisión propia de la Empresa Corredora el de Reducir, Evitar, Transferir o Aceptar el riesgo, de acuerdo a las prioridades y posibilidades presupuestarias que posean se puede advertir que en este punto existen varios criterios, en muchos casos los riesgos serán aceptados y en otros casos se consideraran medidas para reducir o

evitar el riesgo, que es el más probable, por este motivo se hace una propuesta que ayudará a reducir los riesgos identificados como Altos.

6.3 TRATAMIENTO DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN

Se deberían seleccionar controles para reducir, retener, evitar o transferir los riesgos y se debería definir un plan para tratamiento del riesgo. (NB/ISO/IEC 27005, 2010)

Cuando se pueden obtener reducciones grandes en los riesgos con un costo relativamente bajo, se deberían implementar esas opciones. Las opciones adicionales para las mejoras pueden no ser económicas y es necesario estudiarlas para determinar si se justifican o no.

Es responsabilidad de la Gerencia decidir el equilibrio entre los costos de la implementación de los controles y la asignación del presupuesto. Una vez que se conoce el nivel de riesgo que está asociado con los activos en estudio, se pueden adoptar decisiones en base a las siguientes consideraciones:

- **Reducción del Riesgo.** Se debería reducir mediante la selección de controles, de manera tal que el riesgo residual se pueda revaluar como aceptable.
- **Retención del riesgo.** Si el nivel del riesgo satisface los criterios para su aceptación, no es necesario implementar controles adicionales y el riesgo se puede retener.
- **Evitación del riesgo.** Se debería evitar la actividad o la acción que da origen al riesgo particular.
- **Transferencia del riesgo.** El riesgo se debería transferir a otra parte que pueda gestionar de manera eficaz el riesgo particular dependiendo de la evaluación del riesgo.

En este sentido, se tiene una propuesta para realizar un plan de tratamiento en el cual se busca reducir los riesgos de nivel Alto, mediante controles adecuados, tal como se observa en la siguiente tabla:

PLANIFICACIÓN PARA ABORDAR EL RIESGO ALTO								SEGUIMIENTO	
N°	**Riesgo Tratado**	**Actividad**	**Respon-sable**	**Plazo**	**Recursos**	**Resultado Esperado**	**Considera-ciones adicionales**	**Frecuen-cia**	**Respon-sable**
1	Ausencia de Documento de Políticas de seguridad	Elaboración y actualización del Documento de políticas de seguridad	Área de sistemas	3 meses	Financieros (Evaluar % a utilizar del capital de inversión para activos)	Documento de políticas de seguridad revisado y de acuerdo a las necesidades de la empresa	Considerar implementar algún reconocimiento al personal que lo eleabore	Mensual	Gerencia
2	Ausencia o mal manejo de un Registro de Incidentes	Capacitación al personal sobre la utilización de los registros de incidente	Recursos Humanos y área de sistemas	2 meses	Presupuesto	Personal capacitado y motivado	Considerar la entrega de certificados de participación	Mensual	Gerencia
3	Ausencia de documenta-ción sobre Datos de configuración	Elaborar el documento de procedimientos, donde incluyan los principales datos de configuración, tomano en cuenta a los equipos de computación y equipos de comunicación	Área de sistemas	3 mes	Tiempo extra	Documento de procedimientos de configuración de equipos	Considerar tiempo extra para la actividad	Mensual	Gerencia
4	Ausencia de Copias de Respaldo	Realizar las copias de respaldo de los sistemas sensibles con el registro correspondiente	Área de sistemas	1 mes	Medios de almacenamien to	Copias de respaldo probados y almacenados	Considerar los casos de servidores y otros equipos	Semanal	Alta Dirección

5	Exposición del Código fuente de programa	En el documento de políticas de seguridad incorporar el tema de restricción al código fuente del programa, tomando en cuenta los dispositivos que tengan almacenado el código fuente.	Área de sistemas	3 meses	Tiempo extra	Documento que detalle las restricciones al código fuente del programa		Mensual	Gerencia
6	Página Web con software desactuali-zado	Realizar el mantenimiento a la página web, con la actualización de software correspondiente	Área de sistemas	3 meses	Contrato con personal externo que realiza soporte de página web	Página actualizada, que este disponible siempre	Revisar vulnerabilidades de la página web	Mensual	Gerencia
7	Uso inapropiado de Correo electrónico	Capacitación al personal técnico y usuarios en general sobre manejo de correo electrónico	Recursos Humanos y área de sistemas	3 meses	Presupuesto	Usuarios que puedan utilizar eficientement e el correo	Contratación de profesionales especialistas para hacer la capacitación	Mensual	Gerencia
8	Administració n deficiente del Servicio de Active Directory	Capacitación al personal del área de sistemas, sobre la administración de Active Directory	Recursos Humanos	1 año	Presupuesto	Buena administració n del Serviico de Active Directory	Elegir al personal, vinculado con la seguridad de la información	Semestral	Gerencia
9	Ausencia de contrato por Servicio de VPN	Revisar y actualizar contratos con el proveedor de VPN. Solicitando	Área administrati va	6 meses		Contrato sujeto a necesidades de la empresa		Trimestral	Gerencia

		características técnicas detalladas.							
10	Aplicación específica del negocio (sistema de contabilidad, sistema de producción)	Revisión de funcionamiento del sistema de producción, verificar la eficiencia, consultando a los usuarios clave.	Área de sistemas	1 año	Presupuesto	Informe de Evaluación del sistema de Producción	Dependiendo de la empresa está actividad puede ser realizada por Auditoria interna	Semestral	Gerencia
11	Ausencia de copias de respaldo del Servidor de Aplicaciones	Realizar copias de respaldo	Área de sistemas	3 meses	Dispositivos de almacenamiento	Copias de respaldo probados y almacenados		Mensual	Gerencia
12	Ausencia de procedimientos de reglas de autenticación en el Servidor de Correo Electrónico	Elaborar reglas de autenticación, con los respectivos procedimientos, procesos y controles con los niveles de seguridad apropiados	Área de sistemas	3 meses	Presupuesto curso de capacitación para personal de sistemas que se encarga de administración del servidor de correo electrónico	Documento actualizado con los respectivos procedimientos, procesos y controles de reglas de autenticación para el servidor de correo de electrónico		Mensual	Gerencia de sistemas

13	Ausencia de documentos formales, que inidiquen los cambios realizados en el Sistema de gestión de Base de Datos	Elaborar documento con procedimientos, procesos y controles para realizar los cambios de manera eficiente, en la gestión de Base de Datos	Área de sistemas	3 meses	Tiempo extra del personal de sistemas	Documento actualizado con procedimientos, procesos y controles para realizar los cambios de manera eficiente		Mensual	Gerencia de Sistemas
14	Ausencia de registro de control de cambios en la configuración del Router	Elaborar un registro de Control de cambios en la configuración	Área de Sistemas	3 meses	Tiempo extra del personal de sistemas	Registro con los datos más importantes sobre los cambios de configuración		Mensual	Gerencia de Sistemas
15	Firewall	Elaborar un registro de Control de cambios en la configuración	Área de sistemas	3 meses	Tiempo extra del personal de sistemas	Registro con los datos más importantes sobre los cambios de configuración		Mensual	Gerencia de Sistemas
16	Fallas en Central telefónica	Realizar el mantenimiento de la central telefónica, y elaborar el cronograma	Área de sistemas	3 meses	Contratación de personal externo	Central telefónica en buen funcionamiento		Mensual	Gerencia General
17	Deficiente servicio de Internet	Monitorización de la velocidad y conexión de la red de Internet	Área de sistemas	3 meses	Tiempo extra	Registro de los resultados de monitorización y tolerancia a fallos		Mensual	Gerencia General

18	Fallas en las Fuentes de Alimentación Ininterrumpida	Realizar el mantenimiento con las respectivas pruebas de funcionamiento	Área de sistemas	3 meses	Contratación de personal externo	Informe de mantenimiento	Las pruebas deben ser realizadas en horarios fuera de oficina	Mensual	Gerencia General
19	Oficinas sin extintor ni cámaras de seguridad	Compra de Extintor de fuego e instalación de cámaras de seguridad, previo estudio de factibilidad técnico económico.	Área de sistemas	6 meses	Presupuesto, para compra	Instalación de cámaras de seguridad y extintor de fuego		Trimestral	Gerencia General
20	Falta de control, en el ingreso al Centro de Procesamien-to de Datos (CPD)	Controlar el ingreso al CPD, mediante un identificador y una contraseña, monitorización mediante cámaras y un registro de entrada	Área de sistemas	6 meses	Presupuesto	Control efectivo sobre el ingreso al CPD	Elaborar el estudio de factibilidad técnica económica	Trimestral	Gerencia General
21	Usuarios Externos sin restricciones de acceso	Restringir el acceso a la red y sus recursos a usuarios externos. Solamente dar autorización a aplicaciones especificas, siguiendo procedimientos.	Área de sistemas	3 meses		Registro de usuarios externos, con detalle de accesos.	Identificar a los usuarios externos	Mensual	Gerencia de sistemas

22	Desconoci-miento sobre seguridad de la información por parte de Usuarios Internos	Capacitar a los usuarios sobre políticas de seguridad de la información de la empresa	Recursos Humanos y área de sistemas	3 meses	Tiempo extra	Usuarios comprometidos con la seguridad de la información	Incentivar a los usuarios, mediante entrga de certificados de participación	Mensual	Gerencia General
23	Administradores de Sistemas sin control alguno	Realizar los controles de los administradores sobre los accesos a la información (A)	Auditoria Interna	anual		Informe de los accesos del administrador	Informe de Auditoria Externa	Trimestral	Gerencia General
24	Ausencia de informes de control de cambios de los Progra-madores	Elaborar informes de control de cambios eficaces sobre los programas	Área de sistemas	semestral	Tiempo extra	Informes de control de cambios		Trimestral	Gerencia General
25	Consultores sin restricciones de accesos	Implementar controles de acceso lógico y fisico a las instalaciones	Área de sistemas	3 Meses	Tiempo extra	Implementación de Controles efectivos	Trabajar con el apoyo de recursos humanos	Mensual	Gerencia General
26	Proveedores que desconocen las políticas de seguridad de la infor-mación de la empresa	En el contrato especificar el cumplimiento de las políticas de seguridad de la información de la empresa.	Recursos Humanos y área de sistemas	3 meses	Coordinación entre áreas	Contratos adecuados para cubrir los requerimientos de seguridad de la información	Actualizar los contratos	Mensual	Gerencia General

Tabla 6.30 Modelo de Planificación para aplicar en el tratamiento del riesgo alto

Elaboración: Fuente propia

Está propuesta no está limitada al criterio que debe seguir una empresa determinada, es de tipo genérico, y sirve para tratar de reducir el riesgo asociado, en muchos casos serán suficientes y en otros casos no, ya que las situaciones serán diferentes, sin embargo es un cuadro que nos sirve de modelo para realizar un tratamiento de riesgo para los activos de información.

6.4 ACEPTACIÓN DEL RIESGO

Aun considerando las medidas de control quedarán los riesgos residuales, los cuales deberán ser reconocidos, esto puede suceder por varios factores siendo el primero que la medida de control no se esté aplicando de manera correcta o que su implementación tarde mucho y ya no cumpla con los requerimientos, en tal efecto se deberá realizar otra vez un ajuste al plan de tratamiento. Una vez que se haya probado la eficiencia de los controles implementados y aún existe un riesgo residual, deberá ser analizado, para que este riesgo sea aceptable. En el entendido que la seguridad absoluta no existe, por lo que hay que aceptar algunos riesgos, basados en todo el proceso de riesgo, que ha sido analizado.

6.5 COMUNICACIÓN DE LOS RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN

La comunicación del riesgo es una actividad para lograr un acuerdo sobre la manera de gestionar los riesgos al intercambiar, compartir la información acerca de los riesgos, entre quienes toman las decisiones y las otras partes involucradas.

6.6 MONITOREO Y REVISIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN

Los riesgos no son estáticos. Las amenazas, las vulnerabilidades, la probabilidad o las consecuencias pueden cambiar abruptamente sin ninguna indicación. Por ende, es necesario el monitoreo constante para detectar esos cambios. Esta actividad puede estar soportada por servicios externos que brinden información con respecto a nuevas amenazas o vulnerabilidades.

CAPÍTULO 7

7. ANÁLISIS DE RESULTADOS Y CONCLUSIONES

Del presente estudio se extrae el Análisis de resultados de los Capítulos 3, 4, 5 y 6. Finalmente se encuentran las conclusiones y recomendaciones.

7.1 ANÁLISIS DE RESULTADOS Y APLICACIÓN

El estudio ha sido desarrollado en cuatro capítulos, para una mejor comprensión se cita la aplicación y análisis de resultados separados por el título de capitulo.

7.1.1 SEGURIDAD DE LA INFORMACIÓN EN BOLIVIA Y PAÍSES VECINOS

- No se cuenta con una institución dedicada exclusivamente a las tareas de Gestión de seguridad de la Información, recién en el año 2015, Bolivia crea entidades como el AGETIC y el CTIC – EPB, que entre sus funciones está generar lineamientos en el tema de seguridad de la información, es así que el CTIC – EPB está empezando a solicitar la elaboración e implementación de los Planes Institucionales de Seguridad de la Información (P.I.S.I.) de las entidades del sector público. Por lo cual se está en un nivel inicial, de implementar medidas de seguridad de la información, en el sector público.
- En el sector privado específicamente las entidades financieras, que son reguladas por la ASFI, ya en el año 2003 se menciona la necesidad de introducir una cultura de seguridad informática con la circular SB/436/2003, que está dividido en cinco secciones, posteriormente está circular se fue modificando, actualmente la última circular es la ASFI 505/2017 que ya está comprendida por 14 secciones, que están fundamentadas en la familia de normas ISO 27000. En el caso de las empresas corredoras de Seguros y Reaseguros que están reguladas por la APS, en el año 2017 se emiten las circulares APS/DS/JCF/ 153 -2017 dirigido a corredores de Seguros y Reaseguros y APS/DS/JCF 154-2017

dirigido a Entidades Aseguradoras y Reaseguradoras, en la Resolución Administrativa APS/DJ/DS/Nº 39/2016 en la cual ya se menciona que los controles de los sistemas informáticos y de procesamiento de datos adoptados y/o desarrollados deberán realizarse de acuerdo a la norma NB/ISO/IEC 27001. De acuerdo al avance y desarrollo que se ha observado en el ASFI, en cuanto a la emisión de circulares y resoluciones, se contempla que la APS seguirá el mismo rumbo, por lo cual las corredoras de seguros y reaseguros deberían prepararse para asumir el tema de la Gestión de Seguridad de la Información.

- En Bolivia se puede distinguir dos sectores: el sector público y el sector privado, siendo el sector privado, que muestra más avances en el área de Seguridad de la Información, sin embargo todavía no se puede distinguir el tema de la Gestión de Seguridad de la Información en un entorno en el cual no existe la debida atención al tema de Seguridad de la información. Por lo que queda un trabajo amplio y complejo, en la elaboración de proyectos de análisis e implementación sobre la seguridad de la información con los respectivos procedimientos y procesos de Gestión vinculados.
- En el aspecto de Análisis de Gestión de Seguridad de la Información en otros Países, se han elegido para el presente estudio seis países de Sudamérica, de los cuales cinco países comparten frontera con Bolivia: Argentina, Brasil, Chile, Paraguay y Perú, también se menciona a Colombia que es un País con mucha experiencia en el tema de Seguridad de la Información, para este propósito se ha revisado el *Informe de Ciberseguridad 2016 presentado por la BID y la OEA,* se seleccionaron los indicadores que pueden ayudar a conocer los aspectos y comportamiento en temas de seguridad de la información que son: Cultura Cibernética y sociedad, Tecnologías y Educación, al respecto analizando los indicadores se puede decir que:
  - ✓ En el indicador de Cultura Cibernética y sociedad, en Bolivia se presenta un nivel inicial que indica la inexistencia de mentalidad de seguridad cibernética en la sociedad, resultado que no es de extrañarse. Por tanto se concluye que debería darse importancia al resultado de este indicador, trabajando en

programas de información y educación sobre la seguridad cibernética, dirigido a la sociedad en general, ya que la ausencia de conocimiento se convierte en un punto de vulnerabilidad ante las amenazas que se generan por el uso inapropiado de las tecnologías.

- ✓ En el indicador de Tecnologías en el factor de Adhesión a las normas y como sub-factor la Aplicación de las normas y prácticas mínimas aceptables, en los siete países de estudio: Argentina, Bolivia, Brasil, Chile, Colombia, Paraguay y Perú se tiene un nivel "Formativo" que indica que hay una aplicación mínima de las normas nacionales e internacionales.
- ✓ En el indicador de Tecnologías en la *Capacidad de Respuesta a Incidentes,* seis países Argentina, Bolivia, Chile, Colombia, Paraguay y Perú tienen un nivel Formativo, el cual indica la existencia de equipos de respuesta ante incidentes y su actividad se concentra en la detección y respuesta a incidentes cibernéticos específicos de la organización. Brasil tiene un nivel Estratégico, lo que significa que se comparten los recursos y la información a través de una mayor coordinación y colaboración con los equipos locales, regionales e internacionales de respuesta a incidentes. En el indicador de Infraestructura Tecnológica, Bolivia, Paraguay y Perú tienen un nivel formativo el que indica que existe la tecnología desplegada pero sin proyecciones y estrategias. En la organización de respuestas a incidentes en Bolivia, Chile, Colombia y Perú presentan un nivel formativo indica que han sido identificadas y contactadas las organizaciones del sector privado que son clave para la seguridad cibernética nacional, sin que haya mecanismos de coordinación o de intercambio de información con el sector público formal. En la coordinación de respuestas a incidentes Brasil es el único País donde se ha establecido y publicado una respuesta nacional a incidentes coordinada.
- ✓ Si bien Bolivia tiene un nivel inicial, en el que indica que a nivel nacional no existen controles respecto a la seguridad de la información y en algunos aspectos recién se está empezando a generar algunos planes al respecto, se

puede observar que en el entorno de los países vecinos tan poco existe un alto nivel de seguridad de la información, que cumpla con los aspectos necesarios para ser considerados como tal.

- ✓ El indicador de educación muestra que en Argentina, Brasil y Colombia existen ofertas educativas en seguridad cibernética a nivel nacional e institucional. En Bolivia, Chile y Perú indican un nivel de madurez formativo, es decir existe mercado para la educación y la formación en seguridad de la información con evidencia de asimilación; Paraguay indica un nivel de madurez inicial, significa que no hay oferta educativa en seguridad de la información, o existe una oferta mínima.
- ✓ En el indicador de Disponibilidad Nacional de la Educación y formación cibernéticas, Argentina, Bolivia, Chile, Colombia, Paraguay y Perú indican que existe capacitación en seguridad de la información, pero es sin coordinación, en cuanto a formación, hay disponibles seminarios y recursos en línea para grupos demográficos específicos, pero no existen medidas de efectividad.
- ✓ En el indicador de Desarrollo nacional de la educación de seguridad cibernética Argentina, Bolivia, Chile, Paraguay y Perú tienen un nivel Inicial lo que indica que no se cuenta con un programa para capacitar a las personas sobre seguridad de la información y las propuestas iniciales sobre el tema están siendo consideradas en diferentes sectores (privados, públicos). Brasil y Colombia tienen un nivel Formativo, es decir existen incentivos para la formación y la educación.
- ✓ En el desarrollo nacional de la educación de seguridad cibernética, al igual que los países vecinos Bolivia se encuentra en un nivel Inicial lo que indica que no se cuenta con un programa para capacitar a las personas sobre seguridad de la información. La capacitación de los empleados en seguridad cibernética no es parte de las funciones de la empresa privada o pública. Las empresas en particular privadas tienen algún conocimiento de seguridad,

pero no son conscientes de los daños que podrían ocasionar las amenazas y ataques cibernéticos.

- ✓ La seguridad de la información en Sudamérica tiene un punto débil ya que no existen programas formales de educación sobre el tema de seguridad, lo que hace vulnerables a todos los países. A este respeto la educación tiene un papel muy importante en la enseñanza a los profesionales especializados en seguridad sobre cómo construir tecnologías seguras que sigan estándares nacionales e internacionales.

7.1.2 CERTIFICACIONES ISO 27001 EN SUDAMÉRICA

- En Sudamérica los países que cuentan con mayores certificaciones ISO 27001 son: Brasil con 170 certificaciones y Colombia con 148 certificaciones.
- No se tiene información exacta del número de certificaciones ISO 27001 que hay en Bolivia, ya que las empresas no solamente recurrieron a IBNORCA también buscaron a organismos de certificación internacionales, para obtener certificaciones ISO 27001, entre los cuales está TÜV Rheinland, no existe la centralización de la información, que indique exactamente los datos de las empresas nacionales que han sido certificadas.
- Como referencia la norma ISO 27001 es relativamente nueva que data del año 2005, según datos *de Past Surveys 2006 – 2017, Bolivia cuenta con 7 certificaciones en ISO 27001, se* indago sobre las empresas que cuentan con esta certificación ya que la información no se encuentra centralizada es así que se encontraron solamente cuatro empresas de diferentes rubros: en el sector de minería San Cristobal, empresa privada Yanapti, dedicada a la seguridad informática, empresa de telecomunicaciones Nuevatel y por último ASFI que es una institución que regula el sector financiero. Por lo expuesto se concluye que las empresas en Bolivia no son ajenas al cumplimiento de normas internacionales como lo es ISO 27001, aunque se encuentra en cuarto lugar

entre las normas que se certifican, se puede decir que se está empezando con buenas prácticas en Seguridad de la Información en diferentes rubros.

7.1.3 CONTROLES DE SEGURIDAD DE LA INFORMACIÓN QUE APLICAN LAS EMPRESAS CORREDORAS DE SEGUROS Y REASEGUROS

Se trabajó con una muestra del 87% del total de empresas corredoras de seguros y reaseguros, con oficinas principales ubicadas en la ciudad de La Paz. El cuestionario que ha sido aplicado consta de 61 preguntas, elaboradas para ajustarse al entorno del ambiente en estudio, basadas en los controles citados de la norma NB/IEC/ISO 27002, sin embargo no significa que los resultados expongan el cumplimiento de todos los controles y requerimientos de la norma indicada.

Mediante las respuestas ya codificadas y expuestas, se han obtenido las siguientes conclusiones:

- **El documento de políticas de seguridad**, el 65% puede ser considerado como un documento de políticas de seguridad, sin embargo el 35% no puede ser considerado, ya que están en fase inicial de desarrollo o no se encuentran formalmente aprobados por gerencia.

- **La Organización en el departamento o unidad de sistemas**, en este aspecto solamente se hace referencia a las empresas corredoras que cuentan con personal T.I. en planta, lo que refiere al 50% del total de las empresas en estudio, de los cuales el 65 % no se puede considerar la existencia de organización donde existe la segregación de deberes. En consecuencia existe el problema de sobrecarga de responsabilidades y funciones a una sola persona, lo que dificulta el avance y generación de proyectos en el área de T.I.

- **Recursos humanos,** en este caso, se considera que el 40% está tomando medidas de seguridad de información ligada a los recursos humanos, ya que el

personal relacionado a T.I. interno o externo, que realiza soporte de hardware y software, firma un contrato de confidencialidad, además se realiza una capacitación anual sobre temas de seguridad de la información al personal.

- **Administración de Activos, e**l 25% considera en los inventarios, a los activos de información, como ser software con licencia, instaladores y programas de aplicación. El 75 % no considera en los inventarios los activos de información, entonces se desconoce su existencia. Lo que dificulta una administración eficiente de recursos tecnológicos y la documentación generada por estos.

- Control de acceso, el 35 % puede considerarse que tiene algún control de acceso a las computadoras y la Gerencia tiene conocimiento. El 75 % no se considera ya que no existen los mínimos controles de acceso a las computadoras. No se ha realizado una investigación a profundidad, ya que esto va en contra de la confidencialidad de la empresa. Por tanto este resultado es un esbozo general.

- Criptografía, al respecto el 90 % de las empresas no utiliza aún métodos de criptografía, en algunos casos el tema es desconocido. El 10% utiliza la criptografía, en el almacenamiento de la obtención de backups, se los guardan encriptados.

- Seguridad física y del Ambiente**,** en el 45% de las empresas se considera que se siguen controles sobre la seguridad física y del ambiente independientemente entre los que tienen un ambiente como CPD o los que no tienen. El 55% no se considera que tenga controles relacionados a la seguridad física y del ambiente. Pues cuentan con UPS, Extintor, pero no se les realiza el mantenimiento respectivo, cuentan con cableado estructurado pero no está certificado, cuenta

con un cronograma de mantenimiento de equipos de computación pero no tienen registros, por tal motivo no se considera la seguridad física y del Ambiente.

- **Seguridad de las operaciones,** donde se puede apreciar que el 45%, ha tomado medidas de seguridad de las operaciones, entre las que se encuentran empresas corredoras con personal de T.I. y también las que cuentan con personal de T.I. externo.

- **Seguridad de las Comunicaciones,** se puede considerar que el 40%, ha establecido algunos lineamientos en el control de seguridad de las Comunicaciones, cabe destacar que dentro de este porcentaje se encuentran indistintamente las corredoras que cuentan con personal de T.I. de planta, y las corredoras con personal T.I. externo. Ya que cuentan con el contrato de servicio de Internet, existen políticas sobre el uso aceptable de las instalaciones de comunicación, los usuarios están capacitados sobre el envió de información confidencial en las redes de comunicación, el uso de mensajería y el uso de redes sociales.

- **Adquisición, desarrollo y mantenimiento de sistemas, s**e puede considerar que el 85%, ha establecido lineamientos en la adquisición, desarrollo y mantenimiento de sistemas, el 15% representa a las empresas corredoras que no tienen sistemas. En algunas empresas donde el personal de T.I. es externo, el software de producción es obsoleto (año 2009), y ya no brinda el apoyo que requieren los funcionarios, por lo cual utilizan hojas Excel, bastante elaboradas, con fórmulas que ayudan a obtener los reportes, si bien es una buena forma de obtener los informes requeridos, el problema radica en que no se cuenta con una base de datos, que permite ver los históricos de manera eficiente, por tanto no se puede realizar trazabilidad y no se cumplen con otros aspectos de control de seguridad.

- **Relaciones con los proveedores**, este control independientemente si las empresas corredoras cuentan con personal de T.I. interno o externo, es un parámetro muy importante ya que todas las empresas corredoras, tienen algún proveedor, ya sea de hardware o software y en muchos casos ambos.

  Se considera que el 70% de las empresas corredoras han establecido relaciones con los proveedores de servicios basados en parámetros de la seguridad de la información. Entre los parámetros generales, según los resultados del cuestionario se puede indicar que existe una capacitación para el personal de la empresa que interactúa con el proveedor, en el acuerdo o contrato con los proveedores se especifican las obligaciones del proveedor para cumplir los requisitos de seguridad de la empresa, existe una persona específica que administre las relaciones con el proveedor y se cuenta con los informes de servicio de los proveedores.

- Administración de incidentes de seguridad de la información, como resultado se ha determinado que el 70% de las empresas no ha adoptado tareas vinculadas a la administración de incidentes de Seguridad de la Información, por varias razones entre las cuales están la falta de conocimiento, falta de presupuesto y en algunos casos indican que por el hecho de ser empresas pequeñas que tienen un personal de 5 personas, no lo consideran necesario.
    - No se cuenta con un documento aprobado por gerencia sobre los procedimientos para la respuesta rápida, eficaz y ordenada a los incidentes que puedan presentarse.
    - La unidad de TI no cuenta con los procedimientos para monitorear, detectar, analizar e informar sobre eventos e incidentes de seguridad.
    - No se capacito al personal sobre como reconocer incidentes y eventos de seguridad de la información como ser fallas en software, accesos no autorizados, errores humanos y otros.

- También cabe mencionar que se cuentan con dos empresas que tienen certificación ISO 9001, lo que les permitió generar documentación en toda la unidad de T.I., sin embargo eso no significa que posea todos los procedimientos necesarios para cumplir con la norma NB/ISO/IEC 27001, pero tienen una buena base, la cual podría ser muy útil, en el caso de requerir una certificación en dicha norma.

En el análisis del control Administración de incidentes de seguridad de la información, se debe mencionar que aunque existen procedimientos para el manejo y reconocimiento de incidentes, estos no se encuentran documentados, es así que en las entrevistas al respecto, consideraron que sería un buen punto referencial para empezar a documentar los procedimientos que en muchos casos se los tiene sobreentendido con algunas disposiciones de la empresa.

En nuestro entorno de Tecnologías de la Información, aún no se ha desarrollado el tema de procedimientos y documentación de incidentes de seguridad de la información, siendo una falencia a nivel general.

- Aspectos de la seguridad de la información de la administración de la continuidad del negocio o comercial, el plan de continuidad del negocio, es aún más relevante, ya que es un estudio minucioso especializado el cual requiere de bastante tiempo de desarrollo, que muy pocas empresas pueden darse el lujo de elaborarlo. De acuerdo a los resultado obtenidos el 75% no se considera que hayan previsto el aspecto de la seguridad de la información de la administración de la Continuidad del Negocio, este es un aspecto que en nuestro entorno está empezando a desarrollarse, en este ámbito las entidades financieras tienen mayor experiencia. El 25% se puede considerar que han previsto el aspecto de la seguridad de la información de la administración de la Continuidad Comercial.
- Cumplimiento, el 45% se considera que ha tomado algunos parámetros, sobre el control de cumplimiento, en referencia a las políticas de seguridad de la

información, que han sido elaboradas por la empresa. Todas las empresas corredoras cumplen con los requerimientos del Ente Regulador.

La gran falencia en general es la falta de generación de documentación en el área de T.I. que es parte de la administración, es decir registros, formularios, procedimientos, manuales los cuales puedan reflejar el cumplimiento de controles de seguridad de la información. Tomando como referencia que la norma ISO 27001, no solamente trata de la existencia de seguridad de la información si no de la Gestión es decir de la administración de la seguridad.

Se puede destacar las fortalezas que se han encontrado en los tres controles que son considerados:

- ✓ Políticas de Seguridad de la Información
- ✓ Adquisición, desarrollo y mantenimiento del sistema
- ✓ Relaciones con el proveedor

En referencia a los restantes once controles, se encuentran en fase inicial de desarrollo no se los considera ya que en los resultados del cuestionario, se puede observar que no existen los controles o en su defecto tienen falencias en los lineamientos generales, de seguridad de la información.

7.1.4 RESULTADOS DEL ANÁLISIS DE APLICABILIDAD DE LOS CONTROLES DE LA NORMA NB/ISO/IEC 27001:2013

Se analizó la aplicabilidad de cada control de la norma NB/ISO/IEC 27001:2013 en las Empresas Corredores de Seguros y Reaseguros, se obtuvieron los siguientes resultados:

PRIMER CONTROL. POLÍTICAS DE SEGURIDAD DE INFORMACIÓN

Por muy pequeña que sea la empresa debería tener un Documento de Políticas de Seguridad de la Información basado en el enfoque organizacional de acuerdo al

entorno en el que se encuentra. Dicho documento debería ser revisado, por Gerencia, jefatura de personal de T.I. si corresponde, Auditoria Interna y Auditoria Externa.

El documento de políticas de Seguridad de la Información, es muy importante ya que es la base fundamental, una guía que rige las buenas prácticas de seguridad del personal interno y externo, así como los cuidados que deberían tener con la manipulación de los activos de información y aspectos propios que la empresa considera necesario, para mantener la disponibilidad, confidencialidad e integridad de su información. Se considera Aplicable y es la base para el resto de los controles.

SEGUNDO CONTROL. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La asignación específica de personal de seguridad de la información, en el entorno de estudio de las empresas corredoras, donde el personal de T.I. puede ser de planta o externo, no es factible. En este aspecto como resultado de la entrevista se puede indicar que la unidad o área de Tecnologías de Información está compuesta por un máximo de cinco personas. Observando que el 50% de las empresas cuentan con personal de T.I. de planta y el otro 50% cuenta con personal de T.I. externo, las responsabilidades de organización de la seguridad de la información recaerían en la Jefatura de T.I. y en el caso de las empresas que cuentan con personal de T.I. externo recaería sobre Gerencia. Por tanto este control puede Aplicarse de forma parcial, indicando que la asignación específica de personal de seguridad de la información, no es factible, según el contexto de las Empresas Corredoras.

TERCER CONTROL. SEGURIDAD DE RECURSOS HUMANOS

Se requiere coordinar con el personal de recursos humanos para considerar los roles y responsabilidades de seguridad de la información del personal antes, durante el empleo, en la desvinculación y cambio de empleo. De manera general, incluyendo a todo el personal de la empresa, es de vital importancia, la concientización, educación y capacitación sobre la seguridad de la información. Es importante que el personal entienda el objetivo de la seguridad de la información y el posible impacto, ya sea

positivo y negativo, en la empresa y en su propio comportamiento. Se considera ***aplicable*** según el tamaño, contexto y características de la Empresa corredora.

CUARTO CONTROL. ADMINISTRACIÓN DE ACTIVOS

Asegurar que los activos de información reciban el nivel de protección adecuado de acuerdo con su importancia para la empresa. El nivel de protección debería evaluarse mediante el análisis de la confidencialidad, la integridad y la disponibilidad. En el documento de políticas de seguridad de la información se debería contemplar el manejo de medios, para evitar la divulgación, la modificación, el retiro o la destrucción de información almacenada en medios. En las empresas corredores que cuentan con personal de T.I. externo, el control de administración de activos es importante, ya que el servicio de soporte técnico, está relacionado con la manipulación de activos y la información de la empresa. ***Un control aplicable*** y necesario.

QUINTO CONTROL. CONTROL DE ACCESO.

Un usuario tiene acceso al Sistema operativo, Servicio de internet, correo electrónico, sistema de producción, sistema contable, archivos y recursos compartidos como impresoras. Gerencia debería establecer y conocer los niveles de privilegios que los usuarios tienen a cada uno de los servicios. Así también realizar la capacitación para el personal, sobre seguridad siendo uno de los aspectos fundamentales la información sobre el Control de Acceso.

El control de acceso a los sistemas y aplicaciones es de vital importancia, siendo un parámetro de Seguridad que debería ser considerado en todas las empresas corredores independientemente de la cantidad de personal con el que cuente. Es un control aplicable.

SEXTO CONTROL. CRIPTOGRAFÍA

La criptografía puede ser utilizado para almacenar la información de los backups de servidores, puede utilizarse un DAS o un NAS de acuerdo al tamaño de la información. En el caso específico de las empresas corredoras que utilizan discos externos para guardar los backups, sería recomendable los DAS o NAS con un método de criptografía.

La criptografía en el proceso de consultas a bases de datos, implicaría un costo en el ancho de banda de la red interna. La criptografía en la VPN es responsabilidad del proveedor, sin embargo la empresa podría recabar información respecto al código de cifrado y protocolos de encriptación de VPN. Es aplicable desde el punto de vista del almacenamiento de los backups.

SÉPTIMO CONTROL. SEGURIDAD AMBIENTAL

La seguridad física, es un control necesario, en todas las empresas corredores de seguros, siendo los controles de seguridad de los equipos bastante sencillos de cumplir y cada una está dirigida a obtener indicadores que puedan establecer lineamientos de seguridad aceptables. Para que sea factible es necesario la capacitación a todo el personal, involucrado con actividades en la empresa, haciendo hincapié en la concientización de cumplimiento con las políticas de seguridad de la información. Es un control aplicable, con las debidas consideraciones del tamaño de la empresa corredora.

OCTAVO CONTROL. SEGURIDAD DE LAS OPERACIONES

El registro de los tiempos que se planifican para realizar tareas, es conocido como, Administración de cambios para documentos, para tal efecto se debería realizar un seguimiento, con las tareas principales que son: elaborar, revisar y aprobar, cada una con el detalle de fecha de inicio y fecha en la que se completó la tarea, con la firma respectiva del personal responsable de dicha tarea.

Entre las operaciones que deberían considerarse están:

- Registro de backups, se puede observar cómo se incrementa el tamaño de los backups en ciertos periodos, permite determinar a futuro el espacio en disco que se requiere, también se puede observar algunos aspectos irregulares en el crecimiento del backup. Este registro de seguimientos establecerá indicadores que ayudaran a la toma de mejores decisiones en el área de Tecnologías de Información.
- Todos los equipos de computación y comunicación, deberían tener la misma hora de referencia. son una base importante del seguimiento de incidentes informáticos.
- Reconocer las operaciones esenciales, que son requeridas para un óptimo funcionamiento en el área de T.I. ayudará a implementar la seguridad en las operaciones.

Es un control aplicable, que debe ser analizado para su implementación.

NOVENO CONTROL. SEGURIDAD DE LAS COMUNICACIONES

Los controles en las redes están constituidos por varias herramientas la principal un Firewall o cortafuegos que puede ser físico o lógico.

Las conexiones inalámbricas que son empleadas en todas las empresas, requieren de controles especiales, para lo cual se puede adquirir algunas soluciones que ofrecen los proveedores de Antivirus, servicios como: Red Wi-fi protegida, cifrado de archivos entre otros.

En las empresas corredoras un 75% se consideran de tamaño pequeño, por tanto sus redes LAN también son pequeños, en consiguiente los procedimientos de controles de accesos y permisos, pueden alcanzar una adecuada seguridad en la transferencia de información dentro la empresa.

El uso de las técnicas de criptografía en la transferencia de información, no serían recomendables ya que podría provocar un desmedro de la capacidad en una red local de pocos equipos. En el caso particular de las VPN, este control escapa de las manos ya que el proveedor es el encargado de garantizar la seguridad en la transferencia de la información, sin embargo como característica técnica se puede obtener información sobre las técnicas de criptografía que se utiliza, además de tener un contrato que aborde los temas de seguridad en la transferencia de la información. En general este control es aplicable.

DÉCIMO CONTROL. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

El control de protección de transacciones de servicios de aplicación, no es aplicable a las empresas corredoras a nivel general ya que aún no se realizan transacciones por lo que tan poco se utilizan firmas electrónicas.

Según los resultados que se tiene en la entrevista, del 85 % de empresas que utiliza sistemas solamente un 10% de las empresas corredores tiene personal de TI que desarrollan software. El resto adquiere y utiliza aplicaciones que han sido desarrolladas por proveedores externos. En el aspecto de desarrollo externalizado, se puede mencionar los siguientes puntos:

- Los desarrolladores externos son personas independientes, y sus costos son relativamente accesibles, en muchos casos se trabaja de manera informal.

- Los desarrolladores externos son empresas legalmente constituidas que tienen costos elevados, la ventaja: se trabaja de manera formal.

En el control de desarrollo externalizado, existen varios controles que son importantes sin embargo considerando los puntos mencionados, seguir acuerdos con requerimientos como ser: “El derecho contractual para auditar procesos y controles de desarrollo” la inclusión en un contrato de este requerimiento, hace difícil un acuerdo

entre partes, lo más factible es documentar cada una de las etapas de desarrollo y solicitar la garantía correspondiente del desarrollador externo. Es un control que se puede aplicar, de acuerdo a las características específicas de las empresas corredoras, sin embargo se reconoce que algunos controles se pueden aplicar solamente al 10% de las empresas corredoras.

DÉCIMO PRIMER CONTROL. RELACIONES CON LOS PROVEEDORES

Este control implica varios aspectos entre los cuales se destaca: Política de seguridad de la información para las relaciones con los proveedores y abordar la seguridad dentro de los acuerdos con los proveedores. Controles que son necesarios aplicarlos.

Existen dos controles, aunque son necesarios, en el entorno en el cual hoy en día se realizan los acuerdos con los proveedores, es complejo obtenerlos, es el caso de:

- ✓ Revisar los aspectos de seguridad de la información de las relaciones que tiene el proveedor con sus proveedores.
- ✓ Solicitar al proveedor el plan de trabajo, para garantizar que el servicio continuará, a pesar de la ocurrencia de fallas o desastres.

Siendo muchas veces aspectos que causan susceptibilidad al proveedor, son controles que no pueden ser aplicables, porque va más allá de las posibilidades de la Empresa.

El control es Aplicable y necesario, ajustando a los medios con los que cuente la empresa corredora.

DÉCIMO SEGUNDO CONTROL. ADMINISTRACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

- Aún no se utilizan los registros de incidentes, por falta de conocimiento y la falta de administración sobre incidentes informáticos. Una de las formas de trabajar

con un registro de incidentes es permitir que el incidente sea informado por todo el personal de la Empresa, a través del llenado de un registro, para lo cual se requiere una capacitación previa. A partir de este registro personal de T.I. puede realizar el Informe de Incidentes dirigido hacia Gerencia.

Es un control que aún no puede ser aplicable, por el contexto de las Empresas Corredoras.

DÉCIMO TERCER CONTROL. ASPECTOS DE LA SEGURIDAD DE LA INFORMACIÓN DE LA ADMINISTRACIÓN DE LA CONTINUIDAD DEL NEGOCIO

- En muchos casos no se cuenta con un plan de continuidad del negocio y en otros casos, se encuentran en fases iniciales, por lo cual es difícil hablar de la continuidad de seguridad de la información en el plan de continuidad del negocio.
- La continuidad de la seguridad de la información en el plan de continuidad del negocio es un tema que aún no está desarrollado, según entrevista. Solamente un 25% se puede considerar que ha previsto el aspecto de la seguridad de la información en una fase inicial. Es un aspecto que todavía no puede ser analizado, ya que en las empresas que no se considera a la seguridad de la información como una necesidad y no existe ni un plan de contingencias tecnológico, entonces no se puede hablar aún de este tema.

No es aplicable como tal, ya que la elaboración de un documento de Continuidad del Negocio, es compleja y debe ser desarrollado por personal capacitado, con el apoyo de Gerencia, donde debe participar todo el personal. El control implica incluir los aspectos de la Seguridad de la Información en el Documento de Continuidad del Negocio.

DÉCIMO CUARTO CONTROL. CUMPLIMIENTO

- El Control de regulaciones de controles criptográficos no es aplicable a las Empresas Corredores ya que no se realizan tareas de importación o exportación de hardware y software informático para realizar funciones criptográficas.
- Siendo base el documento de políticas de seguridad de la información, es prudente aplicar y llevar el control del cumplimiento de las políticas.
- La realización de pruebas de penetración, se puede aplicar a aproximadamente el 25% de las empresas corredoras, que cuentan con sistemas robustos, y tienen las condiciones técnicas, para realizar dichas pruebas. En el resto de las empresas que son el 75% podría estudiarse otros métodos para evaluar el cumplimiento técnico del software y la red. Todas las empresas corredoras Cumplen con todos los requerimientos del Ente Regulador.

Es aplicable en los controles dirigidos al documento de políticas de seguridad, puesto que las corredoras de seguros y reaseguros son empresas privadas, que cuentan con políticas, contratos y acuerdos. Además que son fiscalizados por la APS.

7.1.5 ELABORACIÓN DE PROCEDIMIENTOS, PROCESOS, POLÍTICAS Y REGISTROS

El aporte para aplicar los controles ha sido desarrollado en el Capítulo 5, elaborando, guías de procedimientos, procesos, políticas y registros.

- ✓ En el primer control de políticas de seguridad de Información se identificaron los Aspectos que deben ser incluidos en la política de Seguridad de la Información para aplicarlos.
- ✓ En el cuarto control, administración de activos se desarrolló:
    - Guía para elaborar un registro con activos de información
    - Registro de activos con características de Confidencialidad, Integridad y Disponibilidad
- ✓ En el quinto control, que es el control de acceso se desarrolló:

- Guía de una Política de control de acceso
- Guía de pasos para la Administración de acceso a los usuarios
- Proceso de Solicitud de Acceso por parte del usuario

✓ En el octavo control, seguridad de las operaciones se desarrollaron:

- Modelo para elaborar una tabla de Control de Cambios para documentos de T.I.
- Registro de seguimiento de las copias de Backups
- Registro de eventos

✓ En el noveno control, seguridad de las comunicaciones se desarrolló una guía de Procedimiento de control de cambios del sistema

✓ En el décimo segundo control, administración de incidentes de seguridad de la información, se elaboró un Registro de incidentes

✓ En el décimo tercer control, aspectos de la seguridad de la información de la administración de la continuidad del negocio se elaboró un esquema de plan de Continuidad del Negocio

7.1.6 GESTIÓN DE RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN

Para realizar la gestión de riesgo se tomó como referencia la norma NB/ISO/IEC 27005, analizando primero el contexto de las empresas corredoras de seguros donde se identificaron los procesos estratégicos, procesos claves y procesos de apoyo. También se identificaron los procesos estratégicos, clave y de apoyo del área de Tecnologías de Información.

La gestión de riesgo está compuesta por muchas partes, se ha requerido revisar Magerit v.3 Libro II y a la vez emplear la norma NB/ISO/IEC 27005, para así combinarlos y obtener los resultados que puedan aplicarse al entorno de estudio, en consecuencia se han obtenido las siguientes consideraciones:

- ✓ La valoración del riesgo implico el análisis y la evaluación del riesgo. En el análisis del riesgo se identificó y se estimó el riesgo. Para la identificación del riesgo, se identificaron los activos de información, se identificaron las amenazas, se identificaron los controles existentes, se identificaron las vulnerabilidades y las consecuencias.
- ✓ Para la identificación de los activos de información y la identificación de amenazas se empleó Magerit v.3 Libro II, se identificaron los controles existentes en las empresas corredoras de seguros y reaseguros, basados en los resultados del Capítulo 4. Para la identificación de vulnerabilidades se recurrió como referencia al Anexo D, correspondiente a la norma NB/ISO/IEC 27005.
- ✓ Se ha utilizado una estimación del riesgo cualitativa ya que es más sencillo trabajar con cualidades como ser: Muy Alto, Alto, Medio, Bajo y Muy Bajo, estas cualidades fueron interpretadas para las tres dimensiones de Confidencialidad, Integridad y Disponibilidad. Con estas cualidades se determinó el valor cualitativo del activo, también se puede hallar el valor económico de un activo físico de información tomando en cuenta el valor de compra menos el valor depreciado al tiempo de vida útil. Sin embargo no se puede aplicar el mismo criterio para dar el valor a activos de información como los programas o las bases de datos.
- ✓ Cuando ocurre un incidente existirá un daño causado al activo de información, por lo cual el activo sufrirá una degradación, lo cual impactara en el valor del activo. Bajo ese criterio se utilizó una tabla de dos entradas donde se tiene el valor del activo y la degradación del 1%, 10% y 100%, como resultado se tiene el impacto.
- ✓ Para la estimación de la probabilidad de Amenaza, se analizó las amenazas para cada activo y en que dimensiones pueden llegar a afectar. También se identificaron las vulnerabilidades y con un criterio personal basado en las respuestas del cuestionario se valoró las vulnerabilidades y amenazas con las cualidades Alta (A), Media (M) y Baja (B). Estos criterios variaran bastante de una Empresa a otra, por lo cual se obtendrán resultados diferentes. Obteniendo

una probabilidad promedio y ya contando con el valor de impacto se calculó el riesgo para cada activo de información. Para la estimación del riesgo se obtuvo referencias en el Anexo E de la norma NB/ISO/IEC 27005. Se identificaron por colores los riesgos, es así que un riesgo con valores entre 6 y 8 se estima como riesgo alto y se lo identifica con color rojo, un riesgo con valores entre 3 y 5 se estima como riesgo medio, identificado por color amarillo. En la tabla 6.27 se puede apreciar un resumen donde se observa que los activos están sujetos a un número de amenazas por vulnerabilidad, se observa el valor del impacto por activo, la probabilidad de ocurrencia y finalmente se obtiene el valor del riesgo.

Todo este análisis y evaluación del riesgo han sido determinantes, para seleccionar los controles que son necesarios para reducir, retener, evitar o transferir los riesgos altos, entonces se concluye que se requiere de este estudio que pueda determinar el nivel de riesgo al que están expuestos los activos de información.

En el Capítulo 4 se ha podido identificar los controles de seguridad que más utilizan las empresas corredores de seguros y reaseguros, en el Capítulo 5 se ha estudiado la forma de aplicabilidad de los controles de acuerdo al entorno de las empresas que tienen características específicas como ser el tamaño pequeño, y que el 50 % de la empresa tiene personal tecnologías de información de planta y el otro 50% de las empresas cuenta con personal T.I. externo. Así mismo según el análisis de aplicabilidad, existen cuatro controles que se pueden aplicar con todas las consideraciones citadas, sin embargo los otros diez controles presentan algunas especificaciones, que no pueden cumplirse a cabalidad. Por último en el Capítulo 6 se pueden identificar mediante el análisis y evaluación del riesgo, los niveles de riesgo por activo de información y se deducen los controles necesarios para reducir, mitigar o evitar los riesgos altos.

En los capítulos 4, 5 y 6 se han determinado la existencia, la aplicabilidad y la necesidad de los siguientes controles:

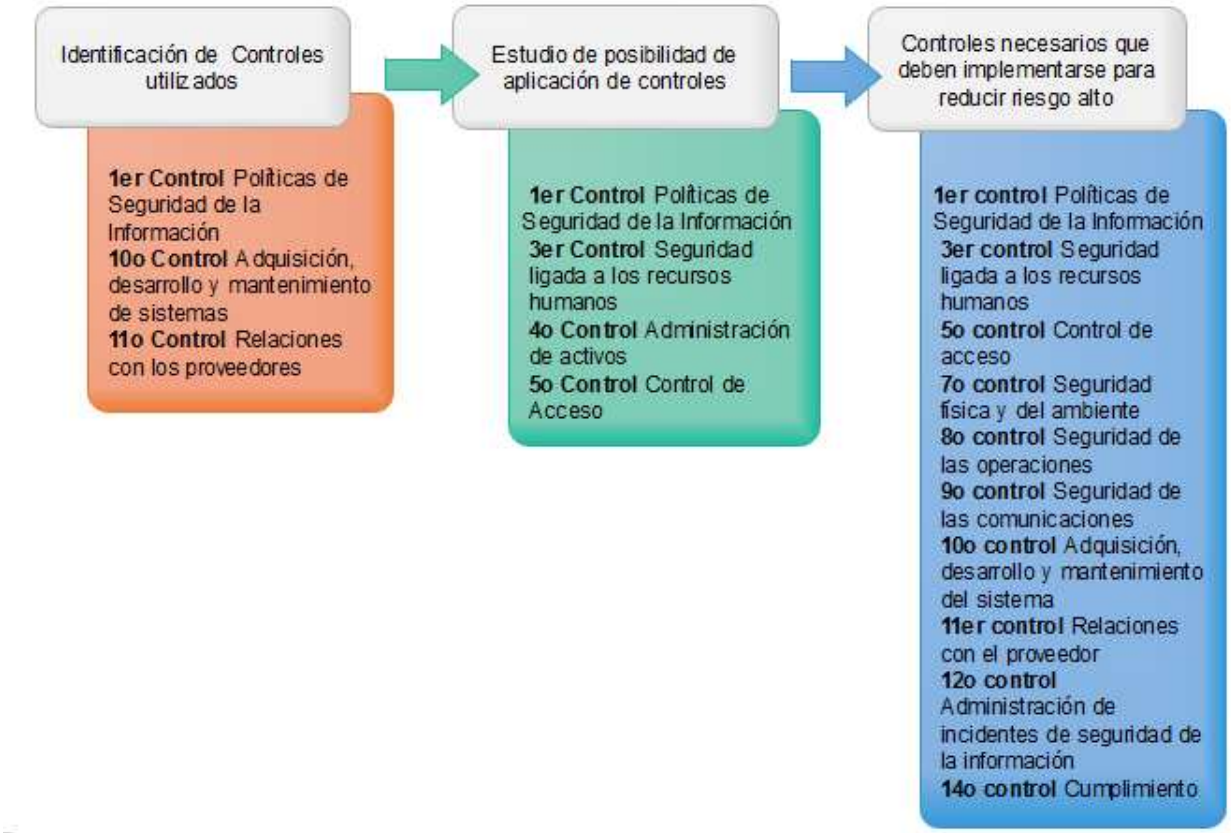


Figura 7.1 Existencia, aplicabilidad y necesidad de Controles en la seguridad de la información
Elaboración: Fuente propia

Analizando la Figura, se concluye que:

- ✓ La ausencia de los controles 2, 4 ,6 y 13 no genero un riesgo alto, en el resultado de la evaluación de riesgos para las empresas corredoras, está es la primera iteración, de acuerdo a los resultados obtenidos, se podría volver a hacer una iteración para realizar las mejoras.
- ✓ El primer control de Políticas de Seguridad de la Información se encuentra en los tres cuadros, primero se entiende que las empresas corredoras de seguros y reaseguros cuentan con políticas de seguridad de la información, segundo este control tiene posibilidad de aplicación, tercero este control es necesario para reducir los riesgos altos que se identificaron en la matriz de riesgo.

- ✓ El tercer control Seguridad ligada a los recursos humanos, se ha podido estudiar que es factible de poder aplicarse, además que en el resultado de la evaluación de riesgos se lo considera necesario para evitar riesgos altos vinculados a recursos humanos, la capacitación en seguridad de la información de todo el personal interno y todo aquel que tiene relación con la Empresa es fundamental, ya que la implementación de una estructura segura y robusta no es suficiente si el personal no es consciente del manejo seguro de la información.
- ✓ El quinto control que es el control de acceso, se ha establecido que puede ser aplicable y además también se encuentra entre los controles necesarios para mitigar riesgos altos, por lo cual es necesario implementar este control.
- ✓ El décimo control Adquisición, desarrollo y mantenimiento de sistemas que es un control utilizado por las corredoras de seguros y también se encuentra entre los controles necesarios para mitigar riesgos altos, es recomendable prestar atención a la los trece controles que los componen, y seleccionar cuales se adecuaran al entorno y contexto de una empresa específica.
- ✓ El décimo primer control relaciones con el proveedor, que es utilizado por las empresas corredoras y también se encuentra entre los controles que mitigan riesgos altos, es importante seguir desarrollando los cinco controles que lo comprenden, ya que como se ha observado todas las empresas corredoras cuentan con proveedores en el área de Tecnologías de la Información.
- ✓ Los controles restantes, ya han sido presentados, explicados y serán útiles para que las empresas corredoras puedan considerarlo tomando en cuenta que ayudan a mitigar riesgos, según se muestra en la matriz de riesgo elaborado en el Capítulo 6.
- ✓ Cada control está compuesto de más controles, no todos son aplicables, ya que se trata de empresas pequeñas y la implementación de muchos controles implicaría la retardación de algunas actividades, la generación de mucho papel, sobrecarga de trabajo a personal de T.I. y otras áreas relacionadas. Por lo que se debe tener mucho cuidado en seleccionar los controles específicos para cada

Empresa, en este estudio se han mostrado los controles generales que son necesarios, pueden ser aplicables y además ayudan a mitigar riesgos altos.

- ✓ Finalmente la implementación de controles dará lugar a la generación de registro de accesos, registros de eventos, formularios de control, documentos de procedimientos y procesos, manuales de sistemas entre otros, todos relacionados al área de T.I. que establecerán las bases para el diseño de un sistema de gestión de seguridad de la información automatizado que será capaz de generar informes y alertas consolidadas sobre la efectividad de los controles y permitirán una toma de decisiones a nivel gerencial con efectividad y además así lograr un buen nivel de seguridad de la información.

7.2 CONCLUSIONES

En muchas empresas corredores de seguros y reaseguros, en las que se conversó con Gerencia y personal de TI, manifestaron el desconocimiento de la norma NB/ISO/IEC 27001, y también manifestaron su interés en saber e informarse al respecto ya que consideran que debe existir seguridad en el manejo de su información, se puede destacar los siguientes criterios que se expresaron:

- ✓ En las entrevistas con personal de Tecnologías de Información, coincidieron que es necesario el uso de algunos formularios, como ser los procedimientos de control de cambios en sistemas. Que es parte del décimo control: adquisición, desarrollo y mantenimiento del sistema.
- ✓ En la entrevista algunos jefes de área de sistemas consideraron, las preguntas realizadas muy acertadas ya que ayudaran a tener un mejor control en el aspecto del área de seguridad, siendo la encuesta solicitada, para ver los puntos en los cuales tienen acefalia.

En el desarrollo de los capítulos se puede llegar a las siguientes conclusiones:

- ✓ Existe una escasez de literatura fidedigna en materia de seguridad de la información en Sudamérica, siendo los estudios con más aporte el Informe de

Ciberseguridad de 2016 de la OEA y la BID. Como referencia también el Survey de ISO.

- ✓ En Sudamérica Bolivia tiene el nivel más bajo de mentalidad de seguridad cibernética en la sociedad, antes de pensar en ampliar servicios de tecnología, se debe pensar en realizar programas de formación para el manejo seguro de la información. O hacerlo de forma paralela.
- ✓ Inclusión de la capacitación del personal es vital para conseguir Seguridad de la Información, ejemplo: como debe ser el trato del personal con el proveedor de servicios, cuidando el nivel de acceso del proveedor a los sistemas y la información de la empresa.
- ✓ Capacitación para personas que utilizan dispositivos móviles, los usuarios deben renunciar a la propiedad de los datos. Celular con programa especial, que permita el borrado de información confidencial, en caso de extravió.
- ✓ Adoptar un Sistema de Gestión de Seguridad de la Información (SGSI) es una decisión estratégica para la Empresa. El retorno de inversión de un proyecto de este modelo es a largo plazo.
- ✓ En Bolivia se puede distinguir dos sectores: el sector público y el sector privado, siendo el sector privado, que muestra más avances en el área de Seguridad de la Información, sin embargo todavía no se puede distinguir el tema de la Gestión de Seguridad de la Información en un entorno en el cual no existe la debida atención al tema de Seguridad de la información, entonces no se puede hablar de gestionar o administrar. Por lo que queda un trabajo amplio y complejo, para elaborar proyectos de análisis e implementación sobre la seguridad de la información con los respectivos procedimientos y procesos de Gestión.
- ✓ En el indicador de Tecnologías en el factor de Adhesión a las normas y como sub-factor la Aplicación de las normas y prácticas mínimas aceptables, en los siete países de estudio: Argentina, Bolivia, Brasil, Chile, Colombia, Paraguay y Perú se tiene un nivel “Formativo” que indica que hay una aplicación mínima de las normas nacionales e internacionales. Se puede concluir que a nivel de

Sudamérica todavía falta mucho desarrollo sobre los aspectos de aplicación de normas en seguridad de la información.

- ✓ En el indicador de Tecnologías en la *Capacidad de Respuesta a Incidentes,* seis países Argentina, Bolivia, Chile, Colombia, Paraguay y Perú tienen un nivel Formativo, el cual indica la existencia de equipos de respuesta ante incidentes, con responsabilidades definidas. Brasil tiene un nivel Estratégico.

  Es decir, que si no se tiene una capacidad de respuesta ante incidentes de seguridad de la información, no se puede colaborar ni esperar colaboración de los otros países, cuando se manifiesten los incidentes, ya que la red de redes como es Internet, no conoce de fronteras, y si no se trabaja de forma conjunta y coordinada con todos los países, todos estamos en riesgo.
- ✓ El nivel de educación y conocimiento en la seguridad de la información de los países determina el desarrollo que pueden llegar a tener los países es así que en Brasil y Colombia tienen un nivel Formativo, en el indicador de Desarrollo nacional de la educación de seguridad cibernética, es decir existen incentivos para la formación y la educación. Lo que refleja que existe desarrollo en el área de seguridad de la información, tal como se ha podido observar en los indicadores, en el número de certificaciones ISO 27001, donde se puede observar que Brasil posee 170 certificaciones y Colombia 148 correspondiente a año 2017.
- ✓ En el indicador de Infraestructura Tecnológica, Bolivia, Paraguay y Perú tienen un nivel formativo el que indica que existe la tecnología desplegada pero sin proyecciones y estrategias.
- ✓ De los siete países en estudio, cuatro países que son: Argentina, Brasil, Chile y Colombia tienen un Nivel establecido, lo que indica que la tecnología desplegada cumple con estándares y buenas prácticas de TI y el servicio de Internet cuenta con procedimientos relacionados a la seguridad de la información. Bolivia, Paraguay y Perú tienen un nivel formativo el que indica que existe la tecnología desplegada pero sin proyecciones ni estrategias.

- ✓ Según los indicadores expuestos, en Bolivia no se identifican ni catalogan incidentes a nivel nacional, encontrándose en el nivel inicial, que es el más bajo entre los países en estudio. En cuanto a la organización se ha podido observar que el sector privado ha tomado medidas en aspecto de seguridad, sin embargo todavía no hay mecanismos de coordinación con instituciones públicas.
- ✓ También se ha podido observar que aún, el País no es consciente de que la gestión de crisis (más que respuesta a incidentes) es necesaria para la seguridad nacional. Se puede observar que de los siete países citados ninguno tiene el nivel más alto que es el nivel Dinámico (implica la toma de decisiones estratégicas, incluso cuando existen cambios).
- ✓ En el desarrollo nacional de la educación de seguridad cibernética, al igual que los países vecinos Bolivia se encuentra en un nivel Inicial lo que indica que no se cuenta con un programa para capacitar a las personas sobre seguridad de la información. La capacitación de los empleados en seguridad cibernética no es parte de las funciones de la empresa privada o pública. Las empresas en particular privadas tienen algún conocimiento de seguridad, pero no son conscientes de los daños que podrían ocasionar las amenazas y ataques cibernéticos.
- ✓ Bolivia se encuentra con niveles iniciales en cuanto a Educación en seguridad cibernética también se puede decir que en el entorno en el cual se encuentra Bolivia, respecto a los países vecinos, se destaca que Brasil y Colombia presentan avances aceptables, sin embargo en todos los países, se necesita trabajar más en programas de capacitación sobre seguridad de la información de manera coordinada, las cuales puedan ser accesibles a todas las personas, ya sea a nivel de usuario, a nivel de instructor para formar, a nivel de especialidad para trabajar en instituciones privadas y públicas.
- ✓ La seguridad de la información en Sudamérica tiene un punto débil ya que no existen programas formales de educación sobre el tema de seguridad, lo que hace vulnerables a todos los países. A este respeto la educación tiene un papel muy importante en la enseñanza a los profesionales especializados en seguridad

sobre cómo construir tecnologías seguras que sigan estándares nacionales e internacionales.

- ✓ Las empresas en Bolivia no son ajenas al cumplimiento de normas internacionales como lo es ISO 27001, aunque se encuentra en cuarto lugar entre las normas que se certifican, se puede decir que se está empezando a darle importancia a las buenas prácticas de Seguridad de la Información en diferentes rubros.

CONTROLES DE SEGURIDAD DE LA INFORMACIÓN QUE APLICAN LAS EMPRESAS CORREDORAS DE SEGUROS Y REASEGUROS

- ✓ De los catorce controles de la norma NB/ISO/IEC 27001, cuatro controles tienen muy poco uso, son los siguientes: Administración de activos de información se consideró que sólo el 25% aplica, la Criptografía se consideró que solamente el 10% aplica, la Administración de incidentes de seguridad de la información se consideró que solo el 30% aplica y Aspectos de seguridad de la información en la gestión de continuidad del negocio solo se puede considerar que el 25 % aplica. Estos resultados tienen que ver con el tamaño, contexto y entorno de las empresas corredoras, también se puede mencionar que dos empresas tenían certificación ISO 9001.
- ✓ Siete controles tienen un resultado menor al 50%, por tanto no han sido considerados como controles que están siendo utilizados. Se destaca que se cumplen con muchos de los controles pero la gran falencia es la falta de generación de documentación en el área de T.I. es decir registros, formularios, procedimientos, manuales que son parte de la administración, los cuales también puedan reflejar el cumplimiento de controles de seguridad de la información.
- ✓ Se puede destacar las fortalezas que se han encontrado en los tres controles que son considerados:

- Políticas de Seguridad de la Información, el 65% puede ser considerado como un documento de políticas de seguridad y el 35% no se considera que sigan con lineamientos generales de políticas de seguridad de la Información, en este sentido se tienen dos aspectos, primero que no se cuente con ningún documento que haga referencias a seguridad de la información, segundo que exista algún documento borrador el cual no esté completo, y no cumpla con lineamientos generales, por tanto no ha sido aprobado por Gerencia.
- Adquisición, desarrollo y mantenimiento del sistema, **s**e puede considerar que el 85%, ha establecido lineamientos en la adquisición, desarrollo y mantenimiento de sistemas, el 15% representa a las empresas corredoras que no tienen sistemas.
- Relaciones con el proveedor, se considera que el 70% de las empresas corredoras han establecido relaciones con los proveedores de servicios basados en parámetros de la seguridad de la información. Entre los parámetros generales, según los resultados del cuestionario se puede indicar que existe una capacitación para el personal de la empresa que interactúa con el proveedor, en el acuerdo o contrato con los proveedores se especifican las obligaciones del proveedor para cumplir los requisitos de seguridad de la empresa, existe una persona específica que administre las relaciones con el proveedor y se cuenta con los informes de servicio de los proveedores.

✓ En el análisis del control Administración de incidentes de seguridad de la información, se debe mencionar que aunque existen procedimientos para el manejo y reconocimiento de incidentes, estos no se encuentran documentados, es así que en las entrevistas al respecto, consideraron que sería un buen punto referencial para empezar a documentar los procedimientos que en muchos casos se los tiene sobreentendido con algunas disposiciones de la empresa.

- ✓ En nuestro entorno de Tecnologías de la Información, aún no se ha desarrollado el tema de procedimientos y documentación de incidentes de seguridad de la información, siendo una falencia a nivel general.

CUADRO RESUMEN APLICABILIDAD DE LOS CONTROLES DE LA NORMA NB/ISO/IEC 27001:2013

El primer, tercer, cuarto y quinto control pueden ser aplicables considerando siempre el tamaño de la empresa. Sin embargo no se puede generalizar los restantes diez controles, ya que se necesita un estudio minucioso de cada empresa corredora según su contexto y tamaño.

	CONTROL	APLICABILIDAD	OBSERVACIONES
1er control	Políticas de Seguridad de la Información	Aplicable (dos controles)	Políticas para la seguridad de la información y la respectiva revisión.
2o control	Organización de la Seguridad de la Información	Estudiar los siete controles en el contexto y tamaño de la Empresa	Asignar personal exclusivo de seguridad de la información, no es aplicable. La responsabilidad de seguridad de la información recae en jefatua de TI. En el caso de que el personal de T.I. es externo la responsabilidad recae en Gerencia

3er control	Seguridad ligada a los recursos humanos	Aplicable (seis controles)	Considerar los roles y responsabilidades de seguridad de la información del personal antes, durante el empleo, en la desvinculación y cambio de empleo. La concientización, educación y capacitación sobre la seguridad de la información.
4o control	Administración de activos	Aplicable (diez controles)	El nivel de protección de los activos de información, debería evaluarse mediante el análisis de la confidencialidad, la integridad y la disponibilidad. En las empresas corredores que cuentan con personal de T.I. externo, el control de administración de activos es importante, ya que el servicio de soporte técnico, está relacionado con la manipulación de activos y la información de la empresa.
5o control	Control de acceso	Aplicable (catorce controles)	Un usuario tiene acceso al Sistema operativo, Servicio de internet, correo electrónico, sistema de producción, sistema contable, archivos y recursos compartidos como impresoras. Gerencia debería establecer y conocer los niveles de privilegios que los usuarios tienen a cada uno de los servicios.
6o control	Criptografía	Estudiar los dos controles en el contexto y tamaño de la Empresa	Es aplicable desde el punto de vista del almacenamiento de los backups, que tienen alta confidencialidad.

7o control	Seguridad física y del ambiente	Estudiar los quince controles en el contexto y tamaño de la Empresa y depende del resultado de la Gestión de Riesgo.	La seguridad física, es un control necesario, en todas las empresas corredores de seguros. Para que sea factible es necesario la capacitación a todo el personal, involucrado con actividades en la empresa.
8o control	Seguridad de las operaciones	Estudiar los catorce controles en el contexto y tamaño de la Empresa	Registro de backups, registro de eventos, reconocimiento de las operaciones, en el área de T.I., son esenciales para implementar la seguridad en las operaciones.
9o control	Seguridad de las comunicaciones	Estudiar los siete controles en el contexto y tamaño de la Empresa	Como referencia el 75 % de las redes LAN en las corredoras son de tamaño pequeño. Y pueden aplicar controles de seguridad, procedimientos de control de acceso en Redes LAN y servicios de red. Herramienta principal un Firewall o cortafuegos que puede ser físico o lógico. Las conexiones inalámbricas Red Wi-fi protegidas. Acuerdos de confidencialidad y de no divulgación.
10o control	Adquisición, desarrollo y mantenimiento del sistema	Estudiar los trece controles en el contexto y tamaño de la Empresa	Un 10% de las empresas tiene personal de T.I. que desarrolla software, el resto de las empresas adquiere sistemas, se puede concluir que en los dos casos son aplicables los controles de mantenimiento del sistema. El control de protección de transacciones de servicios de aplicación, no es aplicable a las empresas corredoras a nivel general.

11er décimo primer control	Relaciones con el proveedor	Estudiar los cinco controles en el contexto y tamaño de la Empresa	Existen dos controles, que son: Revisar los aspectos de seguridad de la información de las relaciones que tiene el proveedor con sus proveedores y solicitar al proveedor el plan de trabajo, para garantizar que el servicio continuará, a pesar de la ocurrencia de fallas o desastres. Estos controles, podrían ser complejos de obtenerlos y aplicarlos.
12o décimo segundo control	Administración de incidentes de seguridad de la información	Estudiar los siete controles en el contexto y tamaño de la Empresa	Es uno de los controles menos utilizados actualmente. Se puede comenzar con la aplicabilidad de la administración de incidentes, a través de registro de incidentes, el cual pueda ser llenado por todo el personal, previa capacitación. El resto de los controles dependerán de la existencia de los registros de incidentes.
13er Décimo tercer control	Aspectos de seguridad de la información de la administración de la continuidad del negocio	Estudiar los cuatro controles en el contexto y tamaño de la Empresa	El 75% no cuenta con un plan de continuidad del negocio y en otros casos, se encuentran en fases iniciales, por lo cual es difícil hablar de la continuidad de seguridad de la información en el plan de continuidad del negocio. Siendo las empresas corredoras un 75 % de tamaño pequeño, no resulta aplicable la inversión que se requiere para elaborar un plan de continuidad del negocio, incluyendo los aspectos de T.I.

14o Décimo cuarto control	Cumplimiento	Estudiar los ocho controles en el contexto y tamaño de la Empresa	El Control de regulaciones de controles criptográficos no es aplicable a las Empresas Corredores ya que no se realizan tareas de importación o exportación de hardware y software informático para realizar funciones criptográficas. Siendo base el documento de políticas de seguridad de la información, es prudente aplicar y llevar el control del cumplimiento de las políticas. Todas las empresas corredoras Cumplen con todos los requerimientos del Ente Regulador.

Tabla 7.1 Cuadro Resumen aplicabilidad de controles

Fuente: Elaboración propia

Como conclusión de la tabla expuesta se puede decir:

- ✓ El Modelo del Sistema de Gestión de Seguridad de la Información de la norma ISO/IEC 27001, es bastante amplio y riguroso para empresas de tamaño pequeño, que por diferentes situaciones principalmente económicas, se ven complicadas en adoptarlo e implementarlo.
- ✓ De los catorce controles, cuatro son aplicables a los entornos y contexto de las empresas corredoras de seguros y reaseguros, sin embargo los otros diez controles que a la vez están conformados por otros controles, deben ser evaluados y estudiados, para ser aplicados.
- ✓ En algunas actividades de control se requiere de un profesional especializado que tenga las competencias requeridas para cumplir las funciones de un Oficial de Seguridad de la Información (OSI), quien realice el monitoreo, revisión de registro de eventos, revisión de los permisos de acceso del administrador de sistemas, entre otros. Por este motivo es que algunos controles no pueden ser aplicables en empresas pequeñas.

Gestión del Riesgo

- ✓ Abordar la gestión de riesgos, es un tema amplio y complejo, en el capítulo 6, se realizó la Gestión de Riesgo basado en ISO 27005 y Magerit v.03 y libro II, el desarrollo de cada actividad depende una de otra, por tanto si existe una variación, afecta a todo el proceso, existen muchas maneras de realizar cada una de las actividades y en el presente estudio se desarrolló una metodología, que puede ser fácilmente interpretada por el área de Tecnología de Información.
- ✓ Una vez que se identificaron los controles que utilizan la empresas corredoras de seguros y reaseguros, además de estudiar la forma de aplicabilidad de los controles mediante la elaboración de modelos de políticas, procedimientos, procesos y registros, el nexo que faltaba era un justificativo de la implementación de los controles, para lo cual se realizó la Gestión de riesgo, y como resultado se obtuvo la matriz de riesgo donde se identificaron los riesgos altos, y los controles necesarios para mitigar dichos riesgos.
- ✓ Es responsabilidad de la Gerencia decidir el equilibrio entre los costos de la implementación de los controles y la asignación del presupuesto. Una vez que se conoce el nivel de riesgo que está asociado con los activos en estudio. Cuando se pueden obtener reducciones grandes en los riesgos con un costo relativamente bajo, se deberían implementar esas opciones. Las opciones adicionales para las mejoras pueden no ser económicas y es necesario estudiarlas para determinar si se justifican o no. En este sentido, se tiene una propuesta para realizar un plan de tratamiento en el cual se busca reducir los riesgos de nivel Alto, mediante controles adecuados.

7.3 RECOMENDACIONES TÉCNICAS

A nivel general, existen recomendaciones técnicas que todo personal involucrado con el área de Tecnologías de Información en las empresas corredoras, debería considerar:

- ✓ Leer la política de privacidad de un sitio web, es importante ya que en esa política indica, que información recolectan del visitante, incluido dirección IP, localización geográfica, tipo de buscador versión, sistema operativo, fuente de referencia, duración de la visita, páginas visualizadas, rutas de navegación del sitio web.
- ✓ Se debería informar mediante programas de Educación en uso de Tecnologías de Información sobre Configuración de privacidad y seguridad en el navegador Chrome de Google, términos del servicio en el Youtube, en Whatsap, en Twitter y en Facebook.
- ✓ El uso de un servidor de almacenamiento en red, como un NAS, requiere de un buen ancho de banda en la red local, ya que se transmitirán grandes volúmenes de información, recomendable para redes gigabit Ethernet, un cableado categoría 5e de 100 Mbps puede llegar a una velocidad máxima de 1000 Mbps, y está diseñado para transmisión a frecuencias de 100 MHz., actualmente se pueden encontrar muchas redes cableadas en Categoria 6 que trabajan a 1000 Mbps y a una frecuencia de hasta 250 MHz, a una distancia menor de 50 m, pueden alcanzar hasta una velocidad de 10 Gbps, según especificaciones técnicas del fabricante.
- ✓ El uso de encriptación en una base de datos, debe ser analizada ya que puede bajar el rendimiento de respuesta, por el aumento de los procesos, debido a la encriptación, se debe tener un buen justificativo para realizar el encriptado en una base de datos.
- ✓ La seguridad de una VPN, depende del protocolo y el tipo de cifrado, lo cual involucra pérdida de rendimiento en velocidad de la conexión, dependiendo del proveedor que pueda ofrecer la seguridad requerida.
- ✓ Existen muchas soluciones sobre el tema de encriptación, que son ofrecidos por diferentes marcas y proveedores tanto en equipos de hardware como software, sin embargo sus requisitos técnicos siempre están basados, en la infraestructura física de la red de área local, ya que debe cumplir con parámetros de certificación, garantizar la velocidad de transmisión en la red, ejemplo para una

red gigabit Ethernet, todos los dispositivos conectados en la red deben soportar la velocidad de 1 Gbps, para lo cual las computadoras y los dispositivos de comunicación deben tener tarjetas de red gigabit Ethernet, así también los switches, routers y en general todos los componentes de la red de área local.

- ✓ En conclusión la encriptación tiene un costo, en cuanto a respuesta en rendimiento y velocidad, sin embargo es la mejor forma de obtener alta confidencialidad, tanto en los datos que se transmiten en la red interna, datos que se guardan en bases de datos, y comunicaciones vía VPN.
- ✓ Algunos gerentes desconocen sobre las clausulas referentes a seguridad de la información, las cuales deben estar en el contrato con los proveedores externos. En el entendido que son dos tipos de proveedores externos: los que brindan soporte y mantenimiento de equipos de computación y los proveedores de sistemas informáticos como el sistema de producción y contabilidad.
- ✓ Para incorporar el tema de continuidad de la seguridad de la información, en el documento de continuidad del negocio, se deberá consultar con especialistas.
- ✓ Para el manejo de evidencia para un incidente de seguridad de la información consultar con especialistas en el área.

8. REVISIÓN DE LITERATURA

Se revisaron las siguientes normas, resoluciones y circulares de los entes reguladores:

- NB/ISO/IEC 27000 (Octubre 2010) Tecnología de la Información - Técnicas de Seguridad – Sistemas de Gestión de Seguridad de la Información – Visión General y Vocabulario
- NB/ISO/IEC 27001 (31 diciembre 2013) Tecnología de la Información - Técnicas de Seguridad – Sistemas de Gestión de Seguridad – Requisitos
- NB/ISO/IEC 27005 (Junio 2010) Tecnología de la Información - Técnicas de Seguridad – Gestión del Riesgo en la Seguridad de la Información

- NB/ISO/IEC 27002 (27 de febrero 2014) Tecnología de la Información - Técnicas de Seguridad – Código de Prácticas para los controles de Seguridad de la Información
- Circular ASFI /505 / 2017 del 4 de diciembre de 2017
- Resolución ASFI No 604/ 2013 del 16 de septiembre de 2013
- Circular APS/DS/JCF/ 153 – 2017 del 6 de noviembre de 2017
- Circular APS/DS/JCF/ 154 – 2017 del 6 de noviembre de 2017
- Resolución Administrativa APS/DJ/DS/No 39 -2016 del 12 de enero de 2016
- Resolución Administrativa IS No 1025 del 18 de noviembre de 2005
- Resolución SB Nº 066/2003 del 4 de julio de 2003

9. BIBLIOGRAFÍA

✓ Agencia para el Desarrollo de la Sociedad de la Información en Bolivia [ADSIB]. (2019). Quiénes Somos. Noviembre 2019. Bolivia Recuperado el 10 de noviembre de 2019 de: https://adsib.gob.bo/portal_frontend/

✓ Alexander Seger (2015) Economía digital y seguridad en América Latina y el Caribe. WEF FORO ECONÓMICO MUNDIAL. Consejo sobre la Agenda Global en Seguridad Cibernética. CoE Consejo de Europa. Recuperado el 15 de noviembre de 2019 de : https://publications.iadb.org/publications/spanish/document/Ciberseguridad-%C2%BFEstamos-preparados-en-Am%C3%A9rica-Latina-y-el-Caribe.pdf

✓ APS (2019) Quienes Somos. Bolivia. Recuperado el 14 de octubre de 2019 de: https://www.aps.gob.bo/index.php/institucional/acerca-de-la-aps/quienes-somos

- ✓ APS (2019). Registro del Mercado Asegurador. Autoridad de Fiscalización y Control de Pensiones y Seguros. Bolivia. Recuperado 14 de noviembre de 2019 de: https://www.aps.gob.bo/index.php/enlace-entidades-fiscalizadas#seguros

- ✓ APS (2019). Entidades Fiscalizadas Seguros. Bolivia. Recuperado 5 de enero de 2020 de: https://www.aps.gob.bo/index.php/seguros/entidades-fiscalizadas

- ✓ Appvizer Revista, 2019. España. Definición de CRM: características, beneficios y mejores herramientas, por Rina Peña Recuperado 10 de enero 2020 de: https://www.appvizer.es/revista/relacion-cliente/software-crm/crm-definicion

- ✓ Argentina.gob.ar , 2019. Argentina. Recuperado el 23 de noviembre de 2019 de: https://www.argentina.gob.ar/noticias/recibimos-la-certificacion-iso-27001-que-fortalece-el-sistema-de-gestion-de-seguridad

- ✓ Autoridad de Supervisión del Sistema Financiero [ASFI] (16 de septiembre 2013). Recuperado el 11 de junio de 2019, de: **https://bolivia.infoleyes.com/norma/4559/circular-asfi-2013-193**

- ✓ ASFI (2019) Por un sistema financiero sólido, solvente e inclusivo. Bolivia. Recuperado el 4 de octubre de 2019 de: https://www.asfi.gob.bo/index.php/asfi/acerca-de-nosotros/que-es-asfi.html

- ✓ Banco Mundial, 2019. Banco de Datos. 2019 Grupo del Banco Mundial. Reservados todos los derechos. Distrito de Columbia. Washington D.C. EE.UU. Recuperado 20 de noviembre de 2019 de: http://databank.bancomundial.org/data/home.aspx

- ✓ Banco Fassil (2015) Programa de Educación Financiera. ¿Qué es la ASFI?. Bolivia. Recuperado el 10 de octubre de 2019 de: https://www.fassil.com.bo/educaci%C3%B3n-financiera/programa-de-educaci%C3%B3n-financiera.html

- ✓ CSIRT Bolivia (2015), Equipo de Respuesta ante Incidentes de Seguridad Informática. La Paz. Bolivia. Recuperado el 5 de noviembre de 2019 de: http://www.bdo3c.f-sc.org/Dossier%20archive%20consolid%C3%A9%20et%20d%C3%A9finitif%20%C3%A0%20la%20date%20du%2001.12.2015/3322.pdf

- ✓ Ciberseguridad (2016) ¿Estamos preparados en América Latina y el Caribe? Informe Ciberseguridad 2016 Copyright © 2016 Banco Interamericano de Desarrollo. Esta obra se encuentra sujeta a una licencia Creative Commons IGO 3.0 Reconocimiento-NoComercial-SinObrasDerivadas (CC-IGO 3.0 BY-NC-ND) (http://creativecommons.org/licenses/by-ncnd/3.0/igo/legalcode) Recuperado 15 de noviembre de 2019 de : https://publications.iadb.org/publications/spanish/document/Ciberseguridad-%C2%BFEstamos-preparados-en-Am%C3%A9rica-Latina-y-el-Caribe.pdf

- ✓ Cisco, 2008. Cómo funcionan las redes privadas virtuales. ID del documento:14106. Recuperado 20 de diciembre de 2019 de: https://www.cisco.com/c/es_mx/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html

- ✓ CONACYT (s.f.) Consejo Nacional de Ciencia y Tecnología. Asunción. Paraguay, ¿Qué es ONA? Recuperado 6 de mayo de 2020 de: https://www.conacyt.gov.py/que-es-ona

- ✓ CTMA Consultores (2018). España. ¿Qué son los certificados ISO y para qué sirven? Todos sus tipos y características Recuperado el 4 de enero de 2020 de: https://ctmaconsultores.com/certificados-iso/

- ✓ Consultores de Seguros S.A. (s.f.) Misión. Bolivia. Recuperado 20 de enero de 2020 de: http://www.consegsa.com/#close

- ✓ Consejo para las Tecnologías de Información y Comunicación [CTIC] del Estado Plurinacional de Bolivia. (s.f.) Seguridad. Bolivia Recuperado el 20 de septiembre 2019 de https://www.ctic.gob.bo/

- ✓ Convention on Cybercrime (2001), Council of Europe, Estrasburgo. Francia. Non – Official languajes, Spanish. Recuperado el 20 de diciembre de 2019 de: https://www.coe.int/en/web/conventions/full-list/-/conventions/webContent/8601684

- ✓ Decreto Supremo 2514 (2015). 2019. Pertenece al Grupo Mostajo. Costa Rica. Sociedad boliviana Infoleyes Bolivia Ltda. Recuperado el 5 de noviembre de 2019 de : https://bolivia.infoleyes.com/norma/5658/decreto-supremo-2514

- ✓ Energy Press Titulada Guía empresas certificadas y acreditadas 2018. Marcelo Vasquez Lema. Santa Cruz, Bolivia. DA No 9 001 1043/2000, ISSN 1680 0788 ENERGY PRESS, ISSN 1609 6843 www.energypress.com.bo Gerente General Carmen Hurtado. Miembro de la Asociación Nacional de la Prensa. Recuperada

el 25 de noviembre de 2019 de: https://es.calameo.com/read/00464206473f054f04bd8

- ✓ Estado Plurinacional de Bolivia – Ministerio de la Presidencia AGETIC (s.f.) Recuperado el 20 de septiembre de 2019 de: https://www.agetic.gob.bo/#/

- ✓ Federación Latinoamericana para la Calidad (s.f.) Libros por Título. Herramientas para el Análisis, Cuantitativo y Cualitativo, Aplicables a sistemas de gestión de la calidad. Argentina. Ciencia y Técnica Administrativa – CyTA ejournal Técnica Administrativa - ISSN 1666-1680. Recuperado el 20 de agosto de 2019 de: http://www.cyta.com.ar/biblioteca/bddoc/bdlibros/herramientas_calidad/causaefecto.htm

- ✓ Hernández, Fernández y Baptista (2014), Metodología de la Investigación, 6ta Edición. McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V. México D.F. ISBN: 978-1-4562-2396-0

- ✓ IAAC (2020). Cooperación Interamericana de Acreditación. Introducción. México. Recuperado el 8 de agosto de 2020 de: https://www.iaac.org.mx/index.php/es/acerca-de-iaac/introduccion

- ✓ Instituto Boliviano de Metrología [IBMETRO](2018) Decreto Supremo 29519 para Organismos de Certificación e Inspección. La Paz. Bolivia. Recuperado 30 de noviembre de 2019 de: http://www.ibmetro.gob.bo/web/node/225

- ✓ Instituto Boliviano de Metrología (2018). Quienes Somos. La Paz. Bolivia. Recuperado 30 de noviembre de 2019 de:

http://www.ibmetro.gob.bo/web/node/156

- ✓ IBNORCA. (s.f.) IBNORED. La Paz. Bolivia. Recuperado 20 de noviembre de 2019 de : http://www.ibnorca.org/es/empresas/12

- ✓ IBNORCA Acreditada. (s.f.) Certificación Sistemas de Gestión. La Paz. Bolivia. Recuperado 10 de enero de 2020 de: https://www.ibnorca.org/sites/default/files/inline-files/CERTIFICADO%20DTA%20TCS.pdf

- ✓ Instituto Boliviano de Normalización y Calidad [IBNORCA] (s.f.) Sobre Nosotros. Bolivia. Recuperado el 25 de julio de 2019, de: http://www.ibnorca.org/es/nosotros

- ✓ INSTITUTO NACIONAL DE ESTADÍSTICAS [INE] (18 de mayo de 2018) La población en Bolivia llega a 11.216.000 habitantes. La Paz, Bolivia. Recuperado el 23 de noviembre de 2019 de: https://www.ine.gob.bo/index.php/prensa/notas-de-prensa/item/3149-la-poblacion-en-bolivia-llega-a-11-216-000 habitantes#:~:targetText=INE%20%2D%20La%20Paz%2C%2018%20de,Nacional%20de%20Estad%C3%ADstica%20(INE).

- ✓ INN (2016), Instituto Nacional de Normalización [INN]. Chile. Recuperado 4 de enero 2020 de: https://www.inn.cl/

- ✓ INACAL Instituto Nacional de Calidad (2016). Organismos de Certificación de Sistemas de Gestión. Lima. Perú. Recuperado 10 de mayo de 2020 de: https://www.inacal.gob.pe/principal/categoria/odcdp

- ✓ INACAL (2016). Información Institucional. Perú. Recuperado el 5 de enero de 2020 de: https://www.inacal.gob.pe/principal/categoria/acerca-de-inacal

- ✓ Inmetro (2018). Habilidades. Brasil. Recuperado el 5 de enero de 2020 de: https://www4.inmetro.gov.br/

- ✓ IRAM (s.f.) Instituto Argentino de Normalización y Certificación. Argentina. Buenos Aires. Recuperado 9 de enero de 2020 de : http://www.iram.org.ar/

- ✓ INTN (2016). Organismo Nacional de Certificación. Paraguay. Recuperado 8 de enero de 2020 de: https://www.intn.gov.py/index.php/organismos/organismo-nacional-de-certificacion

- ✓ ISO (2015). ISO/IEC 17021-1:2015. Ginebra. Suiza. Recuperado 5 de enero de 2020 de: https://www.iso.org/obp/ui#iso:std:iso-iec:17021:-1:ed-1:v1:es

- ✓ ISOTools Excellence (28 de septiembre 2017) Blog especializado en Sistemas de Gestión de Seguridad de la Información. Chile. ¿Cuál es la situación de la norma ISO 27001 en Sudamérica? Recuperado el 15 de agosto de 2019 de: https://www.pmg-ssi.com/2017/09/situacion-norma-iso-27001-sudamerica/

- ✓ ISO/IEC 27001 - Information Technology - Security Techniques - Information Security Management Systems – Requirements Data from 2006 to 2017.(Septiembre, 2019). España. Recuperado el 24 de noviembre de 2019 de: https://isotc.iso.org/livelink/livelink?func=ll&objId=20719433&objAction=browse&viewType=1 archivo Excel:

03. ISO/IEC 27001 - data per country and sector 2006 to 2017 : ISO/IEC 27001 - Central / South America

- ISO survey 2018. The ISO Survey of Management System Standard Certifications 2018 (Septiembre, 2019) THE ISO SURVEY OF MANAGEMENT SYSTEM STANDARD CERTIFICATIONS – 2018 – EXPLANATORY NOTE. Septiembre 2019. España. Recuperado el 26 de noviembre de 2019 de: https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1 https://isotc.iso.org/livelink/livelink/fetch/-8853493/8853511/8853520/18808772/0._Explanatory_note_on_ISO_Survey_2018_results.pdf?nodeid=20719021&vernum=-2

- ITU. Ciberseguridad, abril 2008. International Communications Union. Recomendación UIT-T X.1205, 2008. Serie X: Redes de Datos, Comunicaciones de Sistemas Abiertos y Seguridad. SEGURIDAD EN EL CIBERESPACIO – CIBERSEGURIDAD. Recuperado: 28 de noviembre de 2019 de: https://www.itu.int/rec/T-REC-X.1205-200804-I

- Ley No 164 (2011), La Paz. Bolivia. Reglamento a la Ley Nº 164, de 8 de agosto de 2011, para el Desarrollo de Tecnologías de Información y Comunicación, 13 de noviembre de 2013. Recuperado el 4 de noviembre de 2019 de: https://www.lexivox.org/norms/BO-RE-DSN1793.xhtml

- Ley No 164 (2011), Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación. Recuperado 2 de noviembre de 2019 de: https://www.minedu.gob.bo/files/documentos-normativos/leyes/ley_164___ley_general_de_telecomunicaciones_tecnologias_de_informacin_y_comunicacion.pdf

- ✓ Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público (2017). Estado Plurinacional de Bolivia. Seg-001. CTIC Consejo para las Tecnologías de Información y Comunicación. Recuperado 4 de agosto de 2019 de: https://www.cgii.gob.bo/sites/default/files/2017-12/Documento_Seguridad_SEG-001.pdf

- ✓ Lista de empresas certificadas, 2013. Instituto Boliviano de Normalización y Calidad. La Paz-Bolivia. Código de documento DAT-TCB-04 Recuperado el 20 de noviembre de 2019 de: https://docplayer.es/1047963-Lista-de-empresas-certificadas.html

- ✓ Magerit v.3.0 libro I. Metodología de análisis y gestión de Riesgos de los Sistemas de Información.Métodos. Octubre 2012. Madrid. España. Recuperado 24 de enero de 2020 de: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

- ✓ Magerit v.3.0 libro II. Metodología de Análisis y gestión de Riesgos de los Sistemas de Información. Catálogo de elementos. Madrid. España. Recuperado 24 de enero de 2020 de: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

- ✓ Magerit v.3.0 libro II. Metodología de Análisis y gestión de Riesgos de los Sistemas de Información. Guía de Técnicas. Madrid. España. Recuperado 24 de enero de 2020 de:

https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

- ✓ Mañas José A. (2004). PILAR. HERRAMIENTAS PARA EL ANÁLISIS Y LA GESTIÓN DE RIESGOS. Madrid, España. Recuperado el 11 de agosto de 2019: https://administracionelectronica.gob.es/buscador-gsa/buscadorAvanzado.htm?q=analisis+de+riesgo&busqueda=true&ticket=#.XWRk8ONKjIU

- ✓ McGraw-Hill y Distriforma. (s.f.). Unidad 2. Controladores de Dominios en Redes Windows España. Recuperado 13 de enero de 2020 de: https://www.mheducation.es/bcv/guide/capitulo/8448183940.pdf

- ✓ Microsoft Azure (2019). España. Roles de administrador de suscripciones clásico de RBAC de Azure y de administrador de Azure AD. Recuperado 13 de enero de 2020 de: https://docs.microsoft.com/es-es/azure/role-based-access-control/rbac-and-directory-admin-roles#azure-rbac-roles

- ✓ Ministerio de Economía y Finanzas Públicas [MEFP] (14 diciembre 2018). Noticias del Ministerio Recuperado el 15 de junio de 2019 de: https://www.economiayfinanzas.gob.bo/index.php?opcion=com_prensa&ver=prensa&id=4215&categoria=6&seccion=308

- ✓ Ministerio de Economía y Finanzas Públicas [MEFP] (14 diciembre 2018). Noticias del Ministerio. ASFI recibió certificación ISO/IEC 27001:2013 de seguridad de la información. Recuperado el 15 de junio de 2019 de: https://www.economiayfinanzas.gob.bo/index.php?opcion=com_prensa&ver=prensa&id_item=124&id=4215&seccion=306&categoria=5

- ✓ Mendoza T., Julio César (2008). DEMOSTRACIÓN DE CIFRADO SIMETRICO Y ASIMETRICO. Ingenius. Revista de Ciencia y Tecnología, Universidad Politécnica Salesiana Cuenca, Ecuador. Número (3), pág. 46-53. ISSN: 1390-650X. Recuperado el 2 de Enero de 2020 de: https://www.redalyc.org/articulo.oa?id=5055/505554806007

- ✓ Nueva Economía. La Paz, Bolivia (2013). Certificaciones de Calidad. Depósito Legal Nº 4-3-18-00 Recuperado 21 de noviembre de 2019 de: http://nuevaeconomia.com.bo/wp-content/uploads/2014/09/CERTIFICACIONES-DE-CALIDAD-2.pdf

- ✓ NIST [National Institute of Standards and Technology]. (s.f.) Peter Mell, Tim Grance, Information Technology Laboratory. Gaithersburg. Estados Unidos. Effectively and Securely Using the Cloud Computing Paradigm. Recuperado el 22 de diciembre de 2019 de : https://csrc.nist.gov/CSRC/media/Presentations/Effectively-and-Securely-Using-the-Cloud-Computing/images-media/fissea09-pmell-day3_cloud-computing.pdf

- ✓ OAA Organismo Argentino de Acreditación. (s.f.) Buenos Aires. Argentina. ¿Qué es la acreditación? Recuperado el 10 de junio de 2020 de: https://oaa.org.ar/acreditacion/que-es-la-acreditacion/

- ✓ ONAC (2018). Último Reconocimiento Internacional IAF para ONAC. Bogotá. D.C. Colombia. Recuperado 7 de enero de 2020 de: https://onac.org.co/links-noticias/186-nuevo-reconocimiento-internacional-iaf

- ✓ ONAC (s.f). Presentación. Bogotá. D.C. Colombia. Recuperado 7 de enero de 2020 de: https://onac.org.co/presentacion

- ✓ Organización Internacional de Normalización (2012) El portal de ISO 27001 en español. España. Recuperado el 20 de agosto de 2019, de: http://www.iso27000.es/sgsi.html

- ✓ Página SIETE, domingo, 16 de febrero de 2014. Certifican a empresa boliviana en seguridad de información. La Paz. Bolivia Recuperado el 27 de noviembre de 2019 de: https://www.paginasiete.bo/sociedad/2014/2/17/certifican-empresa-boliviana-seguridad-informacion-14153.html

- ✓ Panda (12 septiembre 2018) ¿En qué se diferencian el sandboxing y los honeypots? Bizkaia (España). Recuperado el 20 de diciembre de 2019 de: https://www.pandasecurity.com/spain/mediacenter/seguridad/diferencias-sandboxing-honeypot/

- ✓ Plan de implementación de Gobierno Electrónico 2016 – 2025. (Julio, 2016) Documento revisado y corregido por el COPLUTIC (Comité Plurinacional de Tecnologías de la Información y Comunicación). La Paz – Bolivia. Recuperado el 10 de julio de 2019 de: https://coplutic.gob.bo/IMG/pdf/pige_versionfinal_corregida.pdf

- ✓ Política y procedimiento preliminar de control de acceso 2012. Intendencia Regional de Atacama. Chile. Recuperado 3 de enero de 2020 de: http://www.intendenciaatacama.gov.cl/filesapp/Control%20de%20Acceso%20Preliminar.pdf

- ✓ Profesional Review (2011 – 2019). Málaga. España. Miguel Angel Navas (Administrador y Analista de Hardware) Recuperado 20 de diciembre de 2019 de: https://www.profesionalreview.com/mejores-nas-del-mercado/

- ✓ REALNET Copyright Realnet 2016 México. Recuperado el 20 de septiembre de 2019 de: https://www.realnet.com.mx/noticias/notas/nota.php?t=la-seguridad-informtica-en-latinoamrica&id=1436

- ✓ Reglamento a la Ley Nº 164 (2013), para el Desarrollo de Tecnologías de Información y Comunicación, 13 de noviembre de 2013. REGLAMENTO PARA EL DESARROLLO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. LexiVox 2011. La Paz, Bolivia. Recuperado el 4 de noviembre de 2019 de: https://www.lexivox.org/norms/BO-RE-DSN1793.xhtml

- ✓ *Salvador E. Vásquez Moctezuma (julio, 2015). México.* e-Ciencias de la Información. *Tecnologías de almacenamiento de información en el ambiente digital.* Volumen 5, número 2, Revisión bibliográfica 1, Jul-Dic 2015 . Recuperado el 20 de diciembre de 2019 de : http://dx.doi.org/10.15517/eci.v5i2.19762

- ✓ Seguridad de la Información, 2018. REVISTA SEGURIDAD. Universidad Nacional Autónoma de México. DGTIC. Consideraciones para el uso de cifrado en las Bases de Datos. Johnny Villalobos Murillo. Recuperado el 2 de enero de 2020 de: https://revista.seguridad.unam.mx/numero22/consideraciones-para-el-uso-de-cifrado-en-las-bases-de-datos

- ✓ SG (2009). Control de Acceso Basado en Roles. México. Gartner Magic Quadrant for Web Access Management, 2H07 Novalys Whitepaper: Role Based Access Control for .NET applications visual-guard.com. Recuperado 6 de enero de 2020 de: https://sg.com.mx/content/view/707

- ✓ Sudamericana Corredores & Asesores de Seguros. (s.f.) Bolivia. Recuperado 20 de enero de 2020 de : http://www.sudseguros.com/index.php?lang=es

- ✓ Techlandia (2001 – 2019), ¿Cómo funciona el AES?. Santa Mónica. California. Estados Unidos Recuperado el 22 de diciembre de 2019 de: https://techlandia.com/funciona-aes-info_215975/

- ✓ Tim Mocan. 2019. Europa. Moldavia. Cifrado de VPN (Todo lo Que Necesita Saber). Recuperado 4 de enero de 2020 de: https://www.cactusvpn.com/es/la-guia-para-principiantes-de-vpn/cifrado-de-vpn/

- ✓ VISA-Negocios. Artículos de Interés. ¿Qué es la seguridad Cibernética? México. Recuperado 27 de noviembre de 2019 de : https://visaempresarial.com/mx/noticias/que-es-la-seguridad-cibernetica_1542

- ✓ VPNmentor (2019). ¿Es WireGuard el futuro de los protocolos VPN? Noticia sobre seguridad de 2019. James Milin-Ashmore. Recuperado 2 de enero de 2020 de: https://es.vpnmentor.com/blog/es-wireguard-el-futuro-de-los-protocolos-vpn-noticia-sobre-seguridad-de/

  World Stats Usage and Population Statistics (18 de noviembre de 2019) Bogota, Colombia. The Internet World Stats web site was created on March 25, 2002 by Enrique de Argaez, MBA, PE, who is the editor, webmaster and owner. He speaks fluent English and Spanish. Copyright © 2019, Miniwatts Marketing Group. All rights reserved worldwide. Page updated November 18, 2019 Recuperado de: https://www.internetworldstats.com/stats2.htm

- ✓ Zhao, G. (2006). Research on Digital Library Data Storage Program. Shanxi Library Journal, 3, 31- 34.

10. TÉRMINOS Y DEFINICIONES

Basado en los términos y definiciones que se encuentran en las normas NB/ISO/IEC 27000 **e** ISO/IEC 17021-1:2015, se citan aquellos que son utilizados en el presente estudio.

TÉRMINOS Y DEFINICIONES BASADO EN NORMA BOLIVIANA NB/ISO/IEC 27000

Se mencionaran los términos y definiciones, basado en la norma NB/ISO/IEC 27000, las cuales son:

Activo. Aquello que tenga valor para la organización, hay muchos tipos de activos, incluidos:

- ✓ Información
- ✓ Software
- ✓ Físicos, como una computadora
- ✓ Servicios
- ✓ Personas y sus calificaciones, habilidades y experiencia
- ✓ Intangible, tal como reputación

Amenaza. Causa potencial de un incidente no deseado, que puede dar lugar a daños en un sistema o en una organización.

Autenticación. Asegurar que una supuesta característica de una entidad es correcta.

Confidencialidad. Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Control. Medio de gestionar el riesgo. Incluyendo políticas, procedimientos, guías, prácticas o estructuras organizativas, que pueden ser de naturaleza administrativa, técnica, de gestión, o legal.

Disponibilidad. Propiedad de ser accesible y utilizable por solicitud de una entidad autorizada.

Evento. Ocurrencia de un conjunto particular de circunstancias.

Guía. Recomendación sobre lo que se espera que se haga para lograr un objetivo.

Impacto. Cambio adverso en el nivel logrado de los objetivos de negocio.

Integridad. Propiedad de salvaguardar la exactitud y completitud de los activos.

No repudio. Capacidad para demostrar la existencia de un supuesto evento o acción y las entidades que los originaron, a fin de resolver las controversias sobre la ocurrencia o no del evento o la acción y la participación de entidades del evento.

Procedimiento. Forma especificada para llevar a cabo una actividad o un proceso.

Proceso. Conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entrada en resultados

Políticas. Intenciones globales y orientación tal como se expresan formalmente por la dirección.

Riesgo. Combinación de la probabilidad de un evento y de su consecuencia.

Vulnerabilidad. Debilidad de un activo o control que puede ser explotado por una amenaza.

OTROS TÉRMINOS Y DEFINICIONES BASADO EN ISO/IEC 17021-1:2015

Cliente certificado. Organización cuyo sistema de gestión ha sido certificado

Imparcialidad. Presencia de objetividad.

Nota 1 a la entrada: Objetividad significa que no existen conflictos de intereses o que éstos se resuelven sin afectar de forma adversa a las actividades subsiguientes del organismo de certificación.

Nota 2 a la entrada: Otros términos que sirven para transmitir el elemento de imparcialidad son: independencia, ausencia de conflictos de intereses, ausencia de sesgos, carencia de prejuicios, neutralidad, justicia, actitud abierta, ecuanimidad, actitud desinteresada, equilibrio.

Consultoría de sistema de gestión, participación en el establecimiento, la implementación o el mantenimiento de un sistema de gestión.

EJEMPLO 1: Preparar o elaborar manuales o procedimientos.

EJEMPLO 2: Asesorar, dar instrucciones o soluciones específicas para el desarrollo e implementación de un sistema de gestión.

Nota 1 a la entrada: Organizar actividades de formación y participar como instructor no se considera consultoría siempre que, cuando estos cursos se refieran a sistemas de gestión o auditorías, se limiten a proporcionar información genérica; es decir, que el instructor no debería proporcionar soluciones específicas para el cliente.

Nota 2 a la entrada: No se considera consultoría el suministro de información genérica sin soluciones específicas para el cliente dirigidas a la mejora de procesos o sistemas. Esta información puede incluir:

— explicar el significado y la intención de los criterios de certificación;

— identificar oportunidades de mejora;

— explicar las teorías, metodologías, técnicas o herramientas asociadas;

— compartir información no confidencial sobre las mejores prácticas relacionadas;

— otros aspectos de gestión que no están cubiertos por el sistema de gestión auditado.

Auditoría de certificación. Auditoría realizada por una organización auditora independiente del cliente y de las partes que confían en la certificación, con el fin de certificar el sistema de gestión del cliente.

Nota 1 a la entrada: En las definiciones siguientes, el término “auditoría” se utiliza para simplificar cuándo se hace referencia a la auditoría de certificación de tercera parte.

Nota 2 a la entrada: Las auditorías de certificación incluyen las auditorías inicial, de seguimiento, de renovación de la certificación y también pueden incluir auditorías especiales.

Nota 3 a la entrada: Las auditorías de certificación las llevan a cabo generalmente los equipos auditores de los organismos que proporcionan la certificación de conformidad con los requisitos de las normas de sistemas de gestión.

Nota 4 a la entrada: Cuando dos o más organizaciones auditoras colaboran en la auditoría de un mismo cliente, ésta se denomina “auditoría conjunta”.

Nota 5 a la entrada: Cuando un cliente es auditado con respecto a los requisitos de dos o más normas de sistemas de gestión a la vez, la auditoría se denomina “auditoría combinada”.

Nota 6 a la entrada: Cuando un cliente ha integrado la aplicación de los requisitos de dos o más normas de sistemas de gestión en un único sistema de gestión y es auditado con respecto a más de una norma, la auditoría se denomina “auditoría integrada”.

Cliente. Organización cuyo sistema de gestión se audita con fines de certificación.

Auditor. Persona que lleva a cabo una auditoría.

Competencia. Capacidad para aplicar conocimientos y habilidades para lograr los resultados previstos.

Guía. Persona designada por el cliente para asistir al equipo auditor

Observador. Persona que acompaña al equipo auditor, pero que no audita

Área técnica. Área caracterizada por los elementos comunes de los procesos pertinentes a un tipo específico de sistema de gestión y a sus resultados previstos.

No conformidad. Incumplimiento de un requisito

No conformidad mayor. No conformidad que afecta a la capacidad del sistema de gestión para lograr los resultados previstos

Nota 1 a la entrada: Las no conformidades pueden ser clasificadas como mayores en las siguientes circunstancias:

— si existe una duda significativa de que se haya implementado un control eficaz de proceso, o de que los productos o servicios cumplan los requisitos especificados;

— una cantidad de no conformidades menores asociadas al mismo requisito o cuestión podría demostrar una desviación sistemática y por tanto, constituye una no conformidad mayor.

No conformidad menor. No conformidad que no afecta la capacidad del sistema de gestión para lograr los resultados previstos

Experto técnico. Persona que proporciona conocimiento o experiencia específicos al equipo auditor

Nota 1 a la entrada: Conocimiento o pericia específicos son aquellos que se relacionan con la organización, el proceso o la actividad que se va a auditar.

Esquema de certificación. Sistema de evaluación de la conformidad relacionado con sistemas de gestión a los que se aplican los mismos requisitos especificados, reglas y procedimientos específicos

Tiempo de la auditoría. Tiempo requerido para planificar y realizar una auditoría completa y eficaz del sistema de gestión de la organización del cliente.

Duración de las auditorías de certificación de sistemas de gestión. Parte del tiempo de la auditoría empleado en actividades de auditoría, desde la reunión de apertura hasta la reunión de cierre, inclusive.

Nota 1 a la entrada: Las actividades de auditoría incluyen normalmente:

— llevar a cabo la reunión de apertura;

— llevar a cabo la revisión de documentos mientras se realiza la auditoría;

— comunicarse durante la auditoría;

— asignar roles y responsabilidades a guías y observadores;

— recopilar y verificar información;

— generar hallazgos de auditoría;

— preparar conclusiones de la auditoría;

— llevar a cabo la reunión de cierre.

ANEXO 1

CUESTIONARIO

CUESTIONARIO UTILIZADO EN LA ENTREVISTA CON CORREDORAS DE SEGUROS Y REASEGUROS

1	Existe un documento llamado políticas de Seguridad de la Información? SI NO	Con que frecuencia son revisadas las políticas de seguridad de la información? (Semestralmente, anualmente)	
2	Existe el área de sistemas? SI NO Por cuanto personal está integrado? 1 2 3 4 5 más de cinco	Existe alguna persona específica con tareas de seguridad de la informacion? SI NO	
3	La empresa incentiva el trabajo que realiza el área o encargado de sistemas? SI NO	El encargado de sistemas firma algún acuerdo de confidencialidad con la Empresa? SI NO	Se ha realizado alguna capacitación sobre seguridad de la información? SI NO
4	Se cuenta con un inventario de activos físicos? SI NO En el inventario se incluyen los activos intangibles? SI NO	Se cuenta con algún registro manual o registro por sistema, que indique características del activo, como nombre del propietario, versión y otros? SI NO	Existe alguna política o procedimiento sobre el manejo de medios extraibles (Discos duros externos, DVDs, memorias USB y otros) SI NO
5	El acceso a la computadora es mediante contraseña? SI NO Después de cuánto tiempo la computadora se bloquea, y solicita contraseña? 5min 10 min 15 min	Existe algún requisito para elegir contraseña? SI NO	La máxima autoridad de la empresa tiene conocimiento sobre los niveles de acceso que tiene cada usuario? SI NO
	Que controles de acceso fisico se tienen en el acceso al CPD? Entrada huella digital. Registro a la entrada. Cámaras de Seguridad.	Que controles de acceso lógico se tienen en el acceso al CPD? Firewall. VLAN. ACL. VPN. Otros	
6	Conoce algoritmos de cifrado para criptografia? SI NO	Se aplica la criptografia, en algún sistema? SI NO	La información almacenada, caso backup, utiliza criptografía ? SI NO
7	Se cuenta con un Centro de Procesamiento de Datos (CPD)? SI NO Existe un medidor de temperatura y humedad en el CPD? SI NO	En el CPD Se cuenta con UPS? SI NO Se han realizado pruebas de funcionamiento? SI NO Se realiza el mantenimiento? SI NO	Se cuenta con extintor? SI NO Se realiza el mantenimiento? SI NO Se cuenta con ventilador o aire acondicionado? SI NO Se le realiza el mantenimiento? SI NO

	Se cuenta con cableado estructurado? SI NO Se cuenta con los informes de certificación del cableado estructurado? SI NO	Cuenta con un cronograma de mantenimiento de equipos de computación? SI NO Existe algún registro del mantenimiento de equipos de computación? SI NO	
8	Se cuenta con documentos de procedimientos operativos? SI NO Como ser Descripción de como realizar respaldos. Uso de correo electrónico.	Existe restricción en el ancho de banda, en la red, en Internet, para los usuarios? SI NO	Se realiza el desarrollo de software, para necesidades de la empresa? SI NO
	Se cuenta con la instalación y actualización de software de detección de malware? SI NO	Los usuarios saben que hacer en caso de presentarse un malware? SI NO	Se obtienen los backups de los equipos más sensibles? SI NO Los Backups son probados? SI NO
	Existen registros de la obtención de backups? SI NO Se registran las ejecuciones de pruebas de los backups? SI NO	Se cuenta con un documento que identifique las vulnerabilidades técnicas, de equipos sensibles como los servidores? SI NO	Existen políticas que rigen la instalación de software por parte de los usuarios? SI NO
9	Cual de los siguientes servicios es más importante, para la empresa? Correo, Internet, sistema de producción, otro sistema	Existe la separación de unidad de redes e informática? SI NO	Se cuenta con algún documento o política sobre el uso de la mensajeria, redes sociales? SI NO
	Se cuenta con Contrato del proveedor de Internet? SI NO Se cuenta con contrato de servicios de red? (Provisión de conexiones, servicio de redes privadas, firewalls u otros) SI NO	Existe un servidor de dominio? SI NO Existe alguna segmentación lógica como uso de VLAN? SI NO	Existe alguna política, sobre el uso aceptable de las instalaciones de comunicación? SI NO
	Se informo a los usuarios sobre las precauciones de envio de información confidencial, en las redes de comunicación? SI NO		

10	Existe algún contrato sobre adquisición, de sistemas? SI NO Existe algún contrato de desarrollo y mantenimiento de sistemas? SI NO	Se cuenta con la documentación sobre proyectos de desarrollo de software? SI NO	Se documenta el proceso de pruebas, para adquirir un nuevo software? SI NO
	Tiene conocimiento sobre clave pública y firma digital? SI NO	En que aplicación se utiliza clave pública?..... En que aplicación se utiliza la firma digital?.....	Se cuenta con un documento el cual establezca las reglas para el desarrollo de software y sistemas? SI NO Los proveedores son empresas: nacionales o internacionales
	Se cuenta con un documento que indique los procedimientos de control de cambios en sistemas? SI NO	Cuando se cuenta con un nuevo sistema,se realizan las pruebas de aceptación? SI NO	En caso de adquirir un sistema (software) ¿El contrato señala los derechos de propiedad de código y de propiedad intelectual? SI NO
11	Existe una política sobre el acceso de los proveedores a la información de la empresa? SI NO	Existe una capacitación para el personal de la empresa que interactua con el proveedor? SI NO	Se abordan el tema de seguridad dentro de los acuerdos con los proveedores que proporcionan componentes de infraestructura de TI? SI NO
	En el acuerdo o contrato con los proveedores se especifican las obligaciones del proveedor para cumplir los requisitos de seguridad de la organización? SI NO	Existe una persona específica que administre las relaciones con el proveedor? SI NO	Se cuenta con los informes de servicio de los proveedores? SI NO
12	Se cuenta con un documento aprobado por gerencia sobre los procedimientos para la respuesta rápida, eficaz y ordenada a los incidentes que puedan presentarse? SI NO	La unidad de TI cuenta con los procedimientos para monitorear, detectar, analizar e informar sobre eventos e incidentes de seguridad? SI NO	Se capacito al personal sobre como reconocer incidentes y eventos de seguridad de la información? (fallas en software, accesos no autorizados, errores humanos) SI NO
13	Se cuenta con un plan documentado sobre la continuidad del negocio. SI NO	Si se cuenta con este documento, se ha previsto la continuidad de la seguridad en la información? SI NO	Se tiene un plan de contingencias tecnológico? SI NO De que año es? ……..

14	Se cuenta con una matriz de riesgo a nivel de Tecnología, en seguridad de la Información? SI NO	Cumple con todos los requerimientos del Ente Regulador? SI NO	El documento de las políticas de seguridad de la información son revisadas por: Auditoria interna, Auditoria externa, Jefatura de TI Otros
	Existe una política sobre la privacidad y protección de la información personal identificable? SI NO		

ANEXO 2

POLÍTICA DE CONTROL DE ACCESO

CÓDIGO
POL-CON-01-01

POLÍTICA DE CONTROL DE ACCESO

INTRODUCCION

La Política de control de acceso, garantiza el control y el límite de acceso a la información y a las instalaciones de procesamiento de la información, mediante la aplicación de controles y restricciones definidas por la empresa corredora que garantiza la confidencialidad, integridad y disponibilidad de los activos de la información.

OBJETIVO

La unidad de Tecnologías de Información establece como Política de control de Acceso el controlar el acceso a la información y a las instalaciones de procesamiento de la información.

ALCANCE

Está política se aplica a todo el personal, consultores y terceras partes que tengan derechos de acceso a la información que puedan afectar los activos de información de la empresa corredora y a todas sus relaciones con terceros que impliquen el acceso a sus datos.

MARCO REFERENCIAL

Se consideran los controles de la norma NB/ISO/IEC 27002 Tecnologías de la Información – Técnicas de Seguridad – Código de prácticas para los Controles de Seguridad de la Información.

CONTROL DE ACCESOS

Se deberá asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas de información. Se utilizará el Registro RECA01 con el

nombre del sistema, nombre de usuario, contraseña temporal, Permisos y fecha de creación. El cual será un documento confidencial de la Unidad de T.I.

REGISTRO DE CONTROL DE ACCESOS (RECA01)					
Nombre del Sistema	Nombre del Usuario	Contraseña Temporal	Permisos	Fecha de Creación	Nombre del que creo la cuenta

Se controlará el acceso a los servicios de red tanto internos como externos.

Las reglas de acceso a través de los puertos, estarán basados en la premisa: “Todo está restringido, a menos que este expresamente permitido”.

Se contempla como servicio de conexión externa a la VPN, al respecto se considera:

> Es de responsabilidad del funcionario con privilegios VPN, asegurarse que ninguna otra persona utilice su cuenta de acceso, entendiendo que es de uso exclusivo para quienes se les ha asignado dichos privilegios.
>
> El uso del sistema VPN debe ser controlado utilizando una contraseña de autenticación fuerte.

El personal de T.I. controlará e identificará los equipos conectados a su red, mediante el uso de controladores de dominio o asignación manual de IP, según corresponda.

Los puertos que permitan realizar mantenimiento y soporte remoto a los equipos de red, servidores y equipos de usuario final, será restringido al administrador de red, que es personal de T.I.

Los usuarios finales deberán permitir tomar el control remoto de sus equipos para realizar el soporte, no desatender el equipo mientrás se tenga el control del equipo por un tercero.

La unidad de T.I.. utilizará dispositivos de seguridad “Firewalls”, para controlar el acceso de una red a otra.

Control de Conexiones de las redes

- ✓ La capacidad de descarga del usuario final será de 10 Mb (Se puede colocar el adecuado)
- ✓ La seguridad para las conexiones Wifi, será WPA2 o superior

Dentro de la red de datos se restringira el acceso a:

- ✓ Mensajería instantánea
- ✓ Correo electrónico comercial no autorizado
- ✓ Descarga de archivos peer to peer
- ✓ Conexiones a sitios streaming no autorizado
- ✓ Acceso a sitios de pornografía
- ✓ Servicios de escritorio remoto a través de Internet
- ✓ Cualquier otro servicio que vulnere la seguridad de la red o degrade el desempeño de la misma

Control de acceso a Internet

La unidad de T.I. proveerá a través de sus ISPs (Proveedor de Servicios de Internet) el servicio de Internet en la empresa siendo el único servicio de Internet autorizado.

Control de Acceso al Sistema Operativo

El acceso al sistema operativo estará protegido por contraseña, que contemplará la siguientes condiciones:

- ✓ Limitar el número de intentos fallidos de conexión auditando los intentos no exitosos.
- ✓ No mostrar las contraseñas digitadas.
- ✓ No transmitir la contraseña en texto claro.

Gestión de contraseñas

La asignación de contraseñas se deberá controlar a través de un proceso formal de gestión a cargo del personal de T.I. las recomendaciones son:

- ✓ Cambiar la contraseña temporal, entregada por personal de T.I.
- ✓ No escribirlas en papeles de fácil acceso, ni en archivos sin cifrar.
- ✓ No habilitar la opción “Recordar clave en este equipo”, función que ofrecen los programas.
- ✓ No enviarla por correo electrónico
- ✓ Las contraseñas se deben mantener confidenciales en todo momento
- ✓ No compartir las contraseñas con otros usuarios.
- ✓ Cambiar la contraseña si se sospecha que alguien más la conoce y si han tratado de dar mal uso de ella
- ✓ Seleccionar contraseñas que no sean fáciles de adivinar, con un mínimo de diez caracteres alfanuméricos.
- ✓ No grabar la contraseña en una tecla de función.
- ✓ Cambiar la contraseña regularmente, puede ser dos veces al año
- ✓ No utilizar la opción de almacenar contraseñas en Internet
- ✓ Ningún usuario podrá tener privilegios de usuario administrador

Los usuarios deberán proceder a bloquear sus sesiones, cuando deban abandonar temporalmente su puesto de trabajo. Las estaciones de trabajo deberán quedar apagados al finalizar la jornada laboral.

Control de Acceso a la Información

El control de acceso a la información a través de una aplicación, se realizará a través de roles que administren los privilegios de los usuarios dentro del sistema de información.

El control de acceso a información física o digital, se realizará teniendo en cuenta los niveles de clasificación de activos.

Equipos de Cómputo portable

El uso de equipos de cómputo portable, está restringido únicamente a los provistos por la institución y deberán contemplar las siguientes directrices:

- Uso de usuario y contraseña
- Uso de software antivirus, provisto por la Empresa
- Restricción de privilegios de usuario administrador
- Realización de copias de seguridad periódicas
- No dejar desatendidos los equipos
- Mantener cifrada la información clasificada
- No conectarse a redes Wifi públicas
- Informar de inmediato al personal de T.I. en caso de pérdida o hurto del equipo, quien procederá al bloqueo del usuario

GLOSARIO

Terceras partes: Persona u organismo reconocido como independiente de las partes implicadas en lo que se refiere a la materia en cuestión. Para este procedimiento, se entenderá como terceras partes a: Proveedores de servicios y de red.

- Proveedores de productos de software y servicios de información.
- Outsourcing de instalaciones y operaciones.
- Servicios de asesoría de seguridad.
- Auditores externos.

Estación de Trabajo: En una red de computadores, una estación de trabajo es un computador que facilita a los usuarios el acceso a los servidores y periféricos de la red.

Documento de políticas de control de acceso basado en: Política y procedimiento preliminar de control de acceso 2012. Intendencia Regional de Atacama. Chile.

ANEXO 3

CONTROL PARA PROTECCION DE LOS REGISTROS QUE SE GENERAN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

CONTROL PARA PROTECCION DE LOS REGISTROS QUE SE GENERAN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Toda la información de este registro es Confidencial

IDENTIFI-CACIÓN	DOCU-MENTOS	MEDIO DE ALMACE-NAMIENTO	TIEMPO DE RETEN-CIÓN	ELABO-RADO POR Y LA FECHA	REVI-SADO POR Y LA FECHA	APRO-BADO POR Y LA FECHA
REG-SEG-01-1	Registro de Eventos de Seguridad de la Información	Papel	2 Años			
INF-SEG-01-1	Informe de seguridad de la información, basado en el registro REG-SEG-01-01	Papel	2 Años			
POL-CON-01-1	Política de control de acceso	Papel	5 Años			
DOC-SEG-01-1	Documento de procedimientos para la recopilación de evidencia	Papel	2 Años			
PLA-CON-01-1	Plan de Continuidad del Negocio	Papel	2 años			

CONTROL DE CAMBIOS

CONTROLES PARA PROTEGER REGISTROS QUE SE GENERAN	
Versión 1.0	

GESTIÓN DEL DOCUMENTO

Elaborado Por:	Revisado Por:	Aprobado Por:
Fecha:	Fecha	Fecha

Donde:

REG-SEG-01-1 Registro de Seguridad Número 01 Versión 1

INF-SEG-01-1 Informe de Seguridad Número 01 Versión 1

POL-CON-01-1 Política de Control Número 01 Versión 1

DOC-SEG-01-1 Documento de Seguridad Número 01 Versión 1

PLA-CON-01-1 Plan de Continuidad del Negocio Número 01 Versión 1

ANEXO 4

PLAN DE CONTINUIDAD DEL NEGOCIO

CÓDIGO
PLA-CON-01-01

Plan de Continuidad del Negocio

Antecedentes. Descripción de la Empresa y los servicios que presta.

Objetivos. Como principal objetivo será el de establecer los procesos y procedimientos de reacción ante una situación adversa que permita reducir el impacto sobre la actividad del negocio.

Metodología. Se debería mencionar bajo que lineamientos se trabajara y los métodos que se utilizaran para lograr el objetivo.

Desarrollo. Se determinaran los procesos y procedimientos críticos, escenarios de contingencia, las funciones principales, las funciones secundarias, analizando los siguientes puntos:

- ✓ Análisis del impacto en el negocio
- ✓ Matriz de riesgo
- ✓ Continuidad de Seguridad de la Información
- ✓ Plan de Contingencia

La Matriz de riesgo, desarrollada en la Capítulo 6, puede ser una propuesta, recomendada para incluirlo en este Plan de Continuidad del Negocio.

CONTROL DE CAMBIOS

PLAN DE CONTINUIDAD DEL NEGOCIO	
Versión 1.0	

GESTIÓN DEL DOCUMENTO

Elaborado Por:	Revisado Por:	Aprobado Por:
Fecha:	Fecha	Fecha

ANEXO 5

AMENAZAS SOBRE LOS ACTIVOS DE INFORMACIÓN

Magerit v.3.0 libro II.
Metodología de Análisis y gestión de Riesgos de los Sistemas de Información

DESASTRES NATURALES [N]

Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.

N1. Fuego, Incendios, posibilidad de que el fuego acabe con recursos del sistema.

N.2 Daños por agua, Inundaciones, posibilidad de que el agua acabe con recursos del sistema.

N.3 Otros desastres naturales, otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, etc.

DE ORIGEN INDUSTRIAL [I]

Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas puede darse de forma accidental o deliberada.

I.5 Avería de origen físico o lógico, fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.

I.6 Corte del suministro eléctrico, Cese de la alimentación de potencia.

I.7 Condiciones inadecuadas de temperatura y/o humedad. deficiencias en la aclimatación de los lugares donde se encuentran equipos sensibles.

I.8 Fallo de servicios de comunicaciones. cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente.

I.9 Interrupción de otros servicios y suministros esenciales. otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, toner, refrigerante, ...

I.11 Emanaciones electromagnéticas. Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información.

ERRORES Y FALLOS NO INTENCIONADOS [E]

Fallos no intencionales causados por las personas.

La numeración no es consecutiva, sino que está alineada con los ataques deliberados, muchas veces de naturaleza similar a los errores no intencionados, difiriendo únicamente en el propósito del sujeto.

[E.1] Errores de los usuarios, equivocaciones de las personas cuando usan los servicios, datos, etc.

[E.2] Errores del administrador, equivocaciones de personas con responsabilidades de instalación y operación.

[E.3] Errores de monitorización, inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos, ...

[E.4] Errores de configuración, introducción de datos de configuración erróneos.

[E.7] Deficiencias en la organización, cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión.

[E.8] Difusión de software dañino, propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.

[E.9] Errores de re-encaminamiento, envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando la información en manos de quien no se espera.

[E.10] Errores de secuencia, alteración accidental del orden de los mensajes transmitidos.

[E.15] Alteración accidental de la información, esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.

E.18] Destrucción de información, esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.

[E.19] Fugas de información, revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel, etc.

[E.20] Vulnerabilidades de los programas (software), defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.

[E.21] Errores de mantenimiento / actualización de programas (software), defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.

[E.23] Errores de mantenimiento / actualización de equipos (hardware), defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.

[E.24] Caída del sistema por agotamiento de recursos, la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

[E.25] Pérdida de equipos, provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad.

ATAQUES INTENCIONADOS

Fallos deliberados causados por las personas.

[A.3] Manipulación de los registros de actividad (log)

[A.4] Manipulación de la configuración, prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.

[A.5] Suplantación de la identidad del usuario, cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente.

[A.6] Abuso de privilegios de acceso, cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.

[A.7] Uso no previsto, utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.

[A.8] Difusión de software dañino, propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.

[A.9] Re-encaminamiento de mensajes, envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a donde o por donde no es

debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Un atacante puede forzar un mensaje para circular a través de un nodo determinado de la red donde puede ser interceptado. Es particularmente destacable el caso de que el ataque de encaminamiento lleve a una entrega fraudulenta, acabando la información en manos de quien no debe.

[A.11] Acceso no autorizado, el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.

[A.12] Análisis de tráfico, el atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios. A veces se denomina "monitorización de tráfico".

[A.13] Repudio, negación a posteriori de actuaciones o compromisos adquiridos en el pasado. Repudio de origen: negación de ser el remitente u origen de un mensaje o comunicación. Repudio de recepción: negación de haber recibido un mensaje o comunicación. Repudio de entrega: negación de haber recibido un mensaje para su entrega a otro.

[A.14] Interceptación de información (escucha), el atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada.

[A.15] Modificación deliberada de la información, alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.

[A.18] Destrucción de información, eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.

[A.19] Divulgación de información, revelación de información.

[A.22] Manipulación de programas, alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.

[A.23] Manipulación de los equipos, alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.

[A.24] Denegación de servicio, la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

[A.25] Robo, la sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad.

En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información

[A.26] Ataque destructivo, Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal.

[A.28] Indisponibilidad del personal, ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos, ...

[A.29] Extorsión, presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido

[A.30] Ingeniería social, abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.