UNIVERSIDAD MAYOR DE SAN ANDRÉS

FACULTAD DE CIENCIAS PURAS Y NATURALES

CARRERA DE INFORMÁTICA

TESIS DE GRADO

"DISEÑO DE UN MODELO DE SEGURIDAD PARA DATA CENTER BASADO EN NB/ISO/IEC 27001:2013 Y NB/ISO/IEC 27002:2014"

Para optar al Título de Licenciatura en Informática

Mención: Ingeniería de Sistemas Informáticos

POSTULANTE: Constantino Lopez Quispe

TUTOR METODOLOGICO: M. SC. Miguel Cotaña Mier

ASESOR: M. SC. Franz Cuevas Quiroz

LA PAZ – BOLIVIA

2020

UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE CIENCIAS PURAS Y NATURALES
CARRERA DE INFORMÁTICA

LA CARRERA DE INFORMÁTICA DE LA FACULTAD DE CIENCIAS PURAS Y NATURALES PERTENECIENTE A 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 referencia correspondiente respetando normas de redacción e investigación.

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

DEDICATORIA

A Dios, porque con él todo es posible.
A mis padres, que me guiaron en el camino correcto.
A mi familia en general, por haberme apoyado en todo momento, por tenerme paciencia en cada momento.

AGRADECIMIENTOS

Doy gracias a Dios por darme fuerza, el tiempo y las condiciones físicas y mentales para el desarrollo de este trabajo.

A mi madre en particular desde que aprendí a escribir y leer a su lado fue la que más me impulso con su humildad, fortaleza, tenacidad, honradez y sus sabias palabras.

A mi familia quienes son una parte muy importante de mi vida. En esta última etapa fueron vital para la conclusión de este trabajo.

A mis amigos, porque me han dado las lecciones más importantes de mi vida y siempre me alentaron y apoyaron para llegar a la conclusión de esta etapa. A quien le pido una foto para el recuerdo, pero me dice que la mejor manera es llevarlo en los recuerdos y el corazón.

Con mucha gratitud a los maestros: a mi tutor M. SC. Miguel Cotaña Mier por compartir sus conocimientos y aportes al presente trabajo, a mi asesor M. SC Franz Cuevas Quiroz, por la dedicación y colaboración en el desarrollo de la presente tesis.

Al Lic. Teófilo Villegas Apaza por haberme permitido aplicar el desarrollo del modelo en el departamento de computación de la Facultad de Tecnología.

A todos los docentes que me alentaron en forma constante, a ellos va mi eterna gratitud.

De la misma manera agradecer a todas las personas que fueron parte de mi vida universitaria, amigos y amigas inolvidables, gracias por su bella amistad y todo su apoyo incondicional.

Constantino Lopez Quispe

RESUMEN

La información es un activo crucial en una organización, resguardar la misma es vital ante posibles alteraciones, mal uso, pérdida, robo, phishing, denegación de servicio, entre otros eventos; es por lo cual se pretende coadyuvar con el presente trabajo mejoras con un modelo de Sistema de Gestión de la seguridad de la información para un centro de datos de una organización. Colaborando a que la seguridad de la información sea gestionada correctamente por medio de un proceso metódico, argumentado y conocido por todas las áreas de la organización.

La metodología seleccionada para el diseño de un modelo de Sistema de Gestión de la seguridad de la información se basa en la NB/ISO/IEC 27001:2013 y como directriz NB/ISO/IEC 27002:2013 los cuales permitirán aplicar una cadena de procedimientos rigurosos y comprensivos en la organización, ya sea esta pequeña o mediana. Los resultados serán mejoras en la gestión de un centro de datos y su entorno.

Palabras clave: Información, denegación de servicio, centro de datos.

ABSTRACT

Information is a crucial asset in an organization, protecting it is vital to possible alterations, misuse, loss, theft, phishing, denial of service, among other events; This is why we intend to contribute with the present work improvements with a model of Information Security Management System for a data center of an organization. Helping to ensure that information security is managed correctly through a methodical process, argued and known by all areas of the organization.

The methodology selected for the design of an Information Security Management System model is based on NB/ISO/IEC 27001:2013 and as a guideline NB/ISO/IEC 27002:2014 which will allow to apply a chain of procedures rigorous and comprehensive in the organization, whether small or medium. The results will be improvements in the management of a data center and its environment.

Keywords: Information, denial of service, data center.

Índice

Índice de Figuras

Índice de tablas

CAPÍTULO I

Marco introductorio

En la actualidad toda organización se basa en la información para la toma de decisiones que permitan la continuidad del negocio, convirtiéndose así en un activo principal para la organización, De ahí la necesidad de protegerla y hacer extensible esa protección a los sistemas tanto físicos como tecnológicos que la administran. La seguridad de la información y los Sistemas de Gestión de la Seguridad de la Información (SGSI) son un aspecto importante para una organización dado su interés en mejorar los niveles de seguridad de las instituciones.

La actual sociedad hace que las personas consuman y produzcan datos a un ritmo nunca antes visto: internet, motores de búsqueda, aplicaciones para móviles, teléfonos inteligentes, etc. Están por todas partes y su existencia es de carácter cotidiano. La realidad es que todos los mecanismos actuales y en número cada vez mayor, dependen del almacenamiento, la distribución en red y el procesamiento de datos digitales. Una mayoría de estas operaciones se ejecutan en un centro de procesamiento de datos (CPD). Sin duda es la columna vertebral, un sector vital para una organización que ejecuta aplicaciones críticas.

Ningún CPD es igual a otro. Cada una tiene requerimientos únicos. Una organización hace el trabajo, sin importar que tan pequeño o grande sea. Un CPD se valora cuando existe un funcionamiento seguro, fiable y eficiente.

La digitalización acelerada ha activado el flujo de datos ininterrumpido en algo absolutamente esencial para el día a día.

En los albores de hoy, una organización invierte en tecnologías y sistemas de información, con el fin de satisfacer las necesidades del ente referido, tener un control de sus

operaciones y distinguirse en un mercado cada vez más competitivo y de constante evolución tecnológica.

De acuerdo a lo referido, la información, tanto digital como física, cumple una tarea muy importante, ya que actúa como activo principal y generador de valor económico real o administrativo para una entidad. Si una de estas organizaciones no administra, protege o asegura adecuadamente su información, estará expuesta a riesgos que perjudicarán la continuidad de su objetivo. Es por ello, que toda información debe ser resguardado, para que se encuentre accesible en tiempo y forma, o desde el punto de vista de la seguridad de información, conserve la triada en sus características de confidencialidad, integridad y disponibilidad.

Por otro lado, los usuarios, experimentan una nueva forma de acceder a los servicios y negocios en línea, se convierten en testigos pasivos y activos de la transformación digital. Por este motivo las organizaciones, sean estas públicas o privadas, buscan adaptar su CPD, dicho de otra manera, existe la tendencia de construir nuevos Data Center en base a estándares internacionales u optar por tercerizar su infraestructura tecnológica. Sin lugar a dudas, un CPD es la columna vertebral como se indica párrafos arriba, también diríamos es el cerebro de una organización o la parte vital.

Un CPD es único, el cual tiene una misión: proteger la información más importante y relevante de una organización. Para tal efecto se requiere implementar las mejores prácticas basadas en estándares nacionales e internacionales y adecuadas a un estado en particular. Con la finalidad que sea escalable, seguro, fácil de administrar y supervisar, además debe estar en funcionamiento todo el tiempo y tener un plan emergente de recuperación ante posibles fallas.

Todo lo referido anteriormente tiene amenazas significativas en el manejo de la información, esto conlleva a que la administración tenga un papel fundamental, partiendo de una adecuada identificación de elementos críticos y sobre todo, tener claro cuáles son los riesgos y clasificarlos, para luego diseñar estrategias y controles apropiados de mitigación en cuanto a su seguridad y poder tener una meta de tomas de decisiones adecuadas.

Debido a estos riesgos es esencial proteger esa infraestructura tecnológica. También es común que una organización tenga pocos recursos para las áreas tecnológicas, lo cual no justifica dejar de implementar e invertir en seguridad.

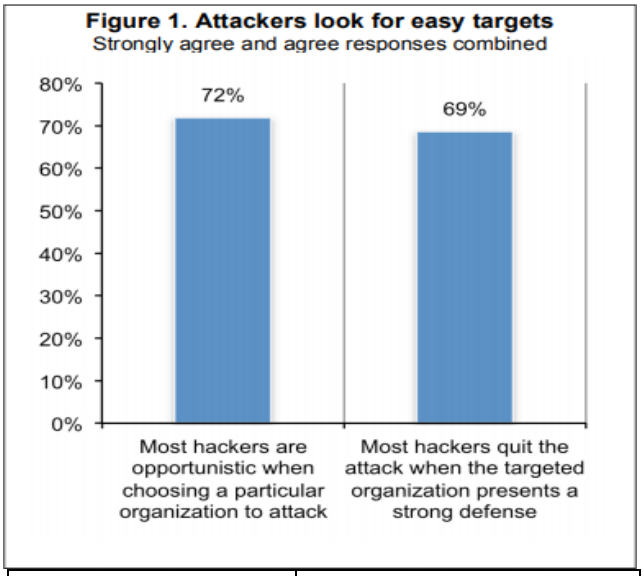
Por lo tanto, en un CPD donde los sistemas son parte de esa entidad, considerar este aspecto dentro de la planeación estratégica constituye en un factor clave para el éxito de la organización.

El presente trabajo, presenta un modelo de diseño de seguridad para CPD, basado en la NB/IEC/ISO 27001:2013 y NB/IEC/ISO 27002:2014. Para diseñar el SGSI, en su versión más reciente. Esto permite tener una metodología de gestión de la información clara y segura, además es un estándar internacional que cuenta con nuevos dominios y controles que buscan reducir el impacto o la posibilidad de ocurrencia de los distintos riesgos a los cuales se encuentra expuesta la organización.

1.1. Antecedentes y trabajos previos

El instituto Ponemon (2016), en su documento “Flipping the Economics of Attacks” llega a inferir lo siguiente: se debe tener en cuenta la motivación y el ámbito económico de los ataques y no solo tomar como coyuntura a soluciones técnicas de los problemas de seguridad,

propiamente a que los atacantes toman direcciones hacia otros objetivos, cuando quebrar la seguridad de una organización le toma más tiempo del que han previsto. Por eso aconseja crear una estrategia integral de ciberseguridad, que se centre en la triada de los componentes importantes de un programa de seguridad: personas, procesos y tecnología, así como construir un equipo fuerte de operaciones de seguridad con políticas acordes y claras en lugar de responder puntual y eficazmente a los incidentes de seguridad. En la figura 1.1 se muestra a 304 expertos en amenazas en Estados Unidos, el Reino Unido y Alemania.



La mayoría de los hackers son oportunistas cuando eligen una organización en particular para atacar.	La mayoría de los hackers abandonan el ataque cuando la organización objetivo presenta una fuerte defensa.

Figura 1.1 Incidentes de seguridad

Fuente: Ponemon Institute ,2016

El instituto Ponemon Institute (2018), en su artículo, “2018 Cost of a Data Breach Study” llega a la conclusión del costo de una violación de datos, la investigación de referencia

del estándar de oro de la industria. El estudio de este año informa que el costo promedio global de una violación de datos aumentó un 6,4 por ciento con respecto al año anterior a $ 3.86 millones. El costo promedio por cada registro perdido o robado que contenga información sensible y confidencial también aumentó en un 4.8 por ciento anual a $ 148.

Realizada una búsqueda de trabajos análogos en la carrera de Informática de la Universidad Mayor de San Andrés UMSA no existen proyectos o tesis de grado, posterior a 2013, en la que se siga un modelo o metodología para aplicar las NB/IEC/ISO 27001:2013 y NB/IEC/ISO 27002:2014.

1.2. Planteamiento del problema

A partir del avance de las tecnologías, de los servicios y de los entornos organizacionales en general, estamos de acuerdo que la información es el activo más importante con que cuentan una entidad pública y privada de Bolivia.

Para ser considerada información, debe previamente realizarse una correcta gestión de los datos, procesarlos en forma significativa y generar información precisa, íntegra, oportuna, interesante, coherente y útil que coadyuve a una correcta toma de decisiones, basadas en la Seguridad en un CPD, llamada también Data Center.

Un CPD está dotado de equipos eléctricos e informáticos que deberían funcionar continuamente. Esto quiere decir que, para evitar su deterioro, todo lo que esté en la infraestructura debe recibir revisiones, verificaciones y mantenimiento. Pueden parecer procesos tediosos, pero son caminos o pasos que sirven para evitar problemas mayores.

Por lo tanto, entre los factores más importantes que motivan la creación de un CPD se

puede destacar el garantizar la continuidad del servicio a clientes, empleados, ciudadanos, proveedores y empresas colaboradoras, pues en estos ámbitos es muy importante la protección física de los equipos informáticos o de comunicaciones implicados, así como servidores de bases de datos que puedan contener información crítica.

La seguridad constituye, por consiguiente, uno de los principales problemas en todo sistema de procesamiento de datos; la expansión de los sistemas informáticos hace que sea imprescindible la implantación de nuevos elementos de seguridad que protejan de una forma adecuada estos entornos.

La seguridad de un CPD (amenazas, medidas de protección y vulnerabilidades) también hace referencia a los riesgos que afectan a la instalación donde se encuentra el mismo y a las soluciones que han de adoptarse para su protección, con el fin de evitar ataques o catástrofes naturales que afecten la imagen institucional.

La seguridad física en la actualidad, presenta grandes problemas, los cuales no fueron previstos con anticipación o no se sujetan a estándares de redes y telecomunicaciones como los de BICSI[1], TIA-942[2], IEEE[3], entre otros. En general, no se toman en cuenta la serie de recomendaciones y directrices para el diseño e instalación de infraestructuras de CPD y sistema de cableado estructurado.

---

[1] BICSI building Industry Consulting Service International Asociación sin fines de lucro que sirve a profesionales en la comunidad de tecnologías de la información y comunicación (TIC)

[2] TIA-942 Telecomunication Industry Association publica su estándar 942 con la intención de unificar criterios en el diseño de áreas de tecnología y comunicaciones.

[3] IEEE Institute of Electrical and Electronics Engineers. El instituto de ingeniería Eléctrica y electrónica es una asociación mundial de ingenieros dedicada a la normalización y el desarrollo de áreas técnicas.

Con relación a la seguridad lógica, cualquiera que sea la forma que tome la información, o medio por el cual sea almacenada o compartida, siempre deberá estar apropiadamente protegida.

A nivel internacional, las empresas han avanzado significativamente ya que hay más volúmenes de datos a tratar, los cuales aumentan debido a la transformación digital, por lo que las empresas necesitan una solución rápida y sencilla para establecer nuevos CPD directamente donde se generan.

Un gran número de organizaciones están muy poco preparadas para resistir frente a este tipo de ataques y se da principalmente a:

- Debilidades de cultura y conciencia organizacional.
- Debilidades en sus sistemas de gestión de riesgos tecnológicos.
- Debilidades de diseño en cuanto a seguridad de los sistemas de información.
- Debilidades en la gestión de crisis.
- Ausencia de recursos suficientes de personal capacitados y entrenados.
- Debilidades de recursos tecnológicos necesarios y suficientes para prevenir, controlar, hacer frente y recuperarse ante ciberataques.
- Debilidades de información detallada relacionada con los impactos reales en las empresas debido al temor de afectar la imagen y reputación al divulgarse las situaciones y experiencias de las compañías atacadas, información que podría ser útil a otras compañías del sector, compañías de seguridad y autoridades, si fuesen compartidas.
- Debilidades de pruebas, ejercicios y simulación de medidas implementadas para

evaluar la efectividad de las acciones.

- Debilidades de cooperación entre sectores y de estos con las autoridades.
- La velocidad del cambio e incorporación de nuevos desarrollos de los atacantes, frente a la evolución tecnológica requerida de la seguridad.

1.3. Formulación del problema

¿Es posible la elaboración de un modelo de Sistema de Gestión de la Seguridad de la información (SGSI) para un CPD que se constituye en la adecuación de componentes, estándares, fases controles y procedimientos que minimicen el nivel de riesgo de seguridad de un CPD, en un ente público o privado en Bolivia?

1.4. Objetivos

1.4.1. Objetivo General

Plantear un modelo de SGSI para un CPD para mejorar la seguridad, que se constituya en la adecuación de componentes basado en el estándar NB/ISO/IEC 27001:2013 apoyado con NB/ISO/IEC 27002:2014.

1.4.2. Objetivos Específicos

- Indagar estándares de seguridad de la información y seguridad informática
- Identificar lineamientos de seguridad de la información y seguridad informática mediante parámetros de la norma NB/ISO/IEC 27001:2013 y NB/ISO/IEC 27002:2014.
- Integrar los conceptos de la NB/ISO/IEC 27001:2013 y NB/ISO/IEC 27002:2014.

- Desarrollar el modelo SGSI de la información basado en las normas NB/ISO/IEC 27001:2013 y NB/ISO/IEC 27002:2014 en un Centro de Procesamiento de Datos CPD.

1.5. Hipótesis

El modelo de SGSI de la información basado en las normas NB/ISO/IEC 27001:2013 y NB/ISO/IEC 27002:2014, coadyuvara a proteger los activos de la información en el proceso de adecuación de componentes, estándares, fases, controles y procedimientos, que minimizan el nivel de riesgo de seguridad informática y seguridad de la información en un Centro de Procesamiento de Datos CPD.

CAPÍTULO II
Marco teórico

En Bolivia como en otras latitudes del mundo las organizaciones consideran la información como un activo de vital importancia, otorgándole prioridad y buscando maneras de controlar los accesos de manera segura a más de buscar maneras de tenerla disponible en cualquier momento y actualizada en los distintos sistemas que puedan tener cada organización.

Debido a esto es que se busca maneras de obtener las mejores prácticas a través de una combinación entre la tecnología y la gestión de usuarios, los cuales son los encargados de enmarcar políticas de seguridad, a través de estándares propuestos por organizaciones regulatorios, que dictan recomendaciones y herramientas para llegar a tener un control eficaz y eficiente de la información, tanto para delimitar el alcance, como para permitir la comprensión total de la propuesta aquí contenida. A continuación, se explica cada uno de los conceptos empleados y desarrollados.

2.1. Datos e Información

2.1.1. Datos

Es una representación simbólica (numérica, alfabética, algorítmica, espacial) de un atributo o variable cuantitativa o cualitativa. Los datos describen hechos empíricos, sucesos y entidades. Es un valor o referente que recibe el computador por diferentes medios los datos representan la información que el programador manipula en la construcción de una solución o en el desarrollo de un algoritmo.

Los datos se caracterizan por no contener ninguna información. Un dato puede significar un número, una letra, un signo ortográfico o cualquier símbolo que represente una cantidad, una medida, una palabra o una descripción [YARLEQUE, 2018]. Los datos son representaciones simbólicas ya sea en un papel o computadora.

2.1.2. Información

La información está constituida por un grupo de datos ya supervisados y ordenados, que sirven para construir un mensaje basado en un cierto fenómeno o ente. La información permite resolver problemas y tomar decisiones, ya que su aprovechamiento racional es la base del conocimiento que constituye un mensaje sobre un determinado ente o fenómeno. Los datos se perciben, se integran y generan la información necesaria para producir el conocimiento que es el que finalmente permite tomar decisiones para realizar las acciones cotidianas que aseguran la existencia. [YARLEQUE, 2018]. Son datos agrupados las cuales se unen para formar información.

2.2. Data Management

Durante los años de 2010 a 2015 se observa en la gestión de datos, que los volúmenes de datos han sido incrementados en las organizaciones, hoy en día todos los movimientos que son registrados por los teléfonos inteligentes, sensores, logs de páginas web, coordenadas de posicionamiento y hábitos de compras. La competencia entre empresas está empezando a enfocarse más en la experiencia de los usuarios que en los productos en sí. Ante este panorama abrumador de volúmenes de datos, distintas fuentes, velocidad y formas surge el Data Management. [Sergio Tornati, 2015] Se tienen fotos, mensajes, videos, música y documentos, los cuales se incrementan de manera exponencial, ocupan espacios en los

distintos servidores. Tanto a nivel de país como mundial, esta información debe ser cuidadosamente administrada. Esta nueva disciplina es también conocida como un proceso de negocios de alto nivel.

Consiste en diferentes subprocesos:

- Planificación y ejecución de políticas, prácticas y proyectos que adquieren controlan, protegen, entregan y refinan el valor de los activos de datos e información.

La misión de esta función es dar respuesta a las necesidades de información de todos los sectores de la empresa en términos de disponibilidad, seguridad y calidad de información.

Los objetivos estratégicos de la función de Data Management son:

- Entender las necesidades de información de la empresa.
- Capturar, almacenar, proteger y asegurar la integridad los activos de información.

Continuamente mejorar la calidad de los datos e información incluyendo:

- Exactitud de los datos.
- Integridad de los datos.
- Integración de la información.
- El tiempo de captura y presentación de los datos.
- La definición de los datos.
- Asegurar la confidencialidad.
- Maximizar el valor de los activos de datos.
- Analizar cada una de estas funciones servirá para entender como esta disciplina se está

convirtiendo en estrategia, incluso la figura 2.1 del CDO (del inglés Chief Data Officer) se ganó un lugar en la mesa de directorio de las empresas más grandes.

[Sergio Tornati, 2015]. Data Management es la conjunción de las distintas funciones de manejo que propone DAMA International.

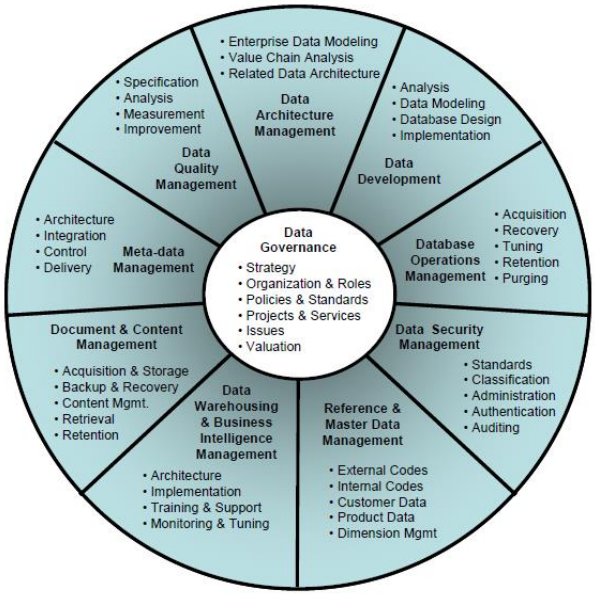


Figura 2.1 Funciones de Data Management

Fuente: (® DAMA International,2019)

2.3. Data Security

La transformación digital ha supuesto una auténtica revolución en un sinfín de aspectos, pero de forma paralela, este inédito avance también ha convertido el nuevo ecosistema tecnológico en mucho más vulnerable.

Los adelantos tecnológicos conllevan importantes problemas de seguridad y privacidad que obligan a buscar fórmulas para resistir ante un posible ataque cibernético, incrementando la demanda de seguridad informática para responder a las necesidades de consumidores y

organizaciones comerciales.

Como es lógico, la proliferación de la delincuencia informática, así como la gravedad y sofisticación de sus ataques, ha hecho que la seguridad sea una prioridad para las organizaciones, no en vano, los ciberataques suponen una seria amenaza para aspectos vitales de las organizaciones, como la economía, la seguridad de datos críticos o la reputación.

Entendiendo que la seguridad es una de las mayores preocupaciones de los responsables de sistemas de TI, la implantación de sistemas de ciberseguridad capaces de hacer frente a estos riesgos es necesaria para una exitosa adopción de la transformación digital [PowerData, 2016]. La criptografía moderna protege los datos transmitidos a través de líneas electrónicas de alta velocidad o almacenados en sistemas informáticos. Hay dos objetivos principales: el secreto o privacidad, para evitar la divulgación no autorizada de los datos.

2.4. Data Architecture

La arquitectura de datos es un conjunto de reglas, políticas, estándares y modelos que gobiernan y definen el tipo de datos recopilados y como se utilizan, almacenan, administran e integran dentro de una organización y sus sistemas de bases de datos. Proporciona un enfoque formal para crear y administrar el flujo de datos y como se procesa en los sistemas y aplicaciones de TI de una organización.

La arquitectura de datos es un término amplio que se refiere a todos los procesos y metodologías que abordan los datos en reposo, los datos en movimiento, los conjuntos de datos y como estos se relacionan con los procesos y aplicaciones que dependen de los datos. Incluye las entidades de datos primarios y los tipos de datos y las fuentes que son esenciales

para una organización en sus necesidades de gestión y suministro de datos. Normalmente, la arquitectura de datos es diseñada, creada, implementada y administrada por un arquitecto de datos.

La arquitectura de datos empresariales consta de tres capas o procesos diferentes:

- Modelo conceptual / de negocios, incluye todas las entidades de datos y proporciona un modelo de datos conceptual.
- Modelo lógico / sistema: define como se vinculan las entidades de datos y proporciona un modelo de datos lógico.
- Modelo físico / tecnológico: proporciona el mecanismo de datos para un proceso y una funcionalidad específicos, o como se implementa la arquitectura de datos real en la infraestructura tecnológica subyacente. [TechoPedia, Architecture,2018]

2.5. Data Quality

La calidad de datos es una forma compleja de medir las propiedades de los datos desde diferentes perspectivas, es un examen exhaustivo de la eficiencia y la conveniencia de los datos, especialmente cuando estos se encuentran en un data warehouse.

Una calidad de datos adecuada es vital para los procesos transaccionales y operativos, así como asegurar la longevidad de inteligencia de negocios y de los informes de análisis de negocio. La calidad de datos puede verse afectada por la forma en que se introducen los datos, como son manejados y cuál es su mantenimiento.

Para un mantenimiento eficaz de la calidad de datos es necesaria una monitorización

periódica de los datos y su limpieza, en general el mantenimiento de la calidad de datos implica la actualización o estandarización de los datos y la de-duplicación[4] de registros de forma que se pueda crear una sola vista de datos.

La habilidad para transformar los datos en información y la información en conocimiento, componen la forma en que se pueda optimizar el proceso de toma de decisiones en los negocios con Business inteligence[5] .

La calidad de datos es de vital importancia ya que proporciona información precisa y oportuna para gestionar responsabilidades y servicios, ofrece información rápida para manejar la efectividad de esos servicios y ayuda a priorizar y garantizar la utilización eficaz de los recursos.

Un ejemplo claro, es el de la calidad de datos en las direcciones de nuestros clientes, donde la repercusión de unos datos de mala calidad puede causar grandes problemas con los clientes. [Data Quality, 2016] Se refiere a los procesos, técnicas, algoritmos y operaciones encaminados a mejorar la calidad de los datos existentes en empresas y organismos.

2.6. Data Warehouse

Almacén de datos es una colección de datos orientada a un tema específico, integrado, variante en el tiempo y no volátil, que soporta el proceso de toma de decisiones. Hinmon, William H. al cual se considera como el padre de Data Waterhouse.

---

[4] De duplicación / reduplicación. Acción y Efecto de reduplicar Real Academia Española (RAE)

[5] Business intelligence, O inteligencia empresarial, se refiere a la utilización de datos en una empresa para facilitar la toma de decisiones dentro de la misma. Conjunto de estrategias y herramientas enfocadas al análisis de datos de una empresa blog de workmeter

Un data Waterhouse es un repositorio unificado para todos los datos que recogen los diversos sistemas de una empresa. El repositorio puede ser físico o lógico y hace hincapié en la captura de datos de diversas fuentes sobre todo para fines analíticos y de acceso.

Normalmente, un data Waterhouse se aloja en un servidor corporativo o cada vez más en la nube[6]. Los datos de diferentes aplicaciones de procesamiento de transacciones Online (OLTP) y otras fuentes se extraen selectivamente para su uso por aplicaciones analíticas y de consultas por usuarios.

Es una arquitectura de almacenamiento de datos que permite a los ejecutivos de negocios organizar, comprender y utilizar sus datos para tomar decisiones estratégicas. Un Data Waterhouse es una arquitectura conocida ya en muchas empresas modernas. [Power Data, 2019]

Un data Warehouse es un depósito electrónico donde generalmente una empresa u organización mantiene una gran cantidad de información. Los datos de un data Waterhouse deben almacenarse de forma segura, fiable, fácil de recuperar y fácil de administrar

2.7. Modelo y método

2.7.1. Modelo

[6] Nube: Es un modelo para permitir el acceso ubicuo, conveniente y bajo demanda a una red compartida. De recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que puede aprovisionarse y liberarse rápidamente con un mínimo esfuerzo de gestión o interacción con el proveedor de servicios.

Un modelo es una abstracción de algo, cuyo objetivo es comprenderlo antes de construirlo. Dado que los modelos omiten los detalles no esenciales es más sencillo manipularlos que manipular la entidad original. La abstracción es una capacidad humana fundamental que nos permita enfrentarnos a la complejidad. Los ingenieros, artistas y artesanos han estado construyendo modelos durante miles de años para probar los diseños antes de ejecutarlos. [Rumbaugh, Blaha, Premerlani,1996]. Modelo es una representación de la realidad simple, diseñados por un observador entendido en el tema.

Un modelo constituye una representación abstracta de un cierto aspecto de la realidad y tiene una estructura que está formada por los elementos que caracterizan el aspecto de la realidad modelada, y por las relaciones entre sus elementos. [Aracil,1995]. Finalidad de la construcción de modelos.

Medio para entender sistemas complejos.

- Ayuda a desarrollar teorías.
- Ayuda a describir el sistema.
- Conduce a hipótesis sobre la conducta del sistema.
- Sirven de medio para la experimentación.

2.7.2. Método

Desde el ángulo de la didáctica general, la palabra método, encierra el concepto de una dirección hacia el logro de un propósito, un camino a recorrer, aunque es claro que ha de entenderse que no se trata de un camino cualquiera, sino el mejor, del más razonable, del que más garantice la consecución de la finalidad propuesta. El método implica un proceso de

ordenamiento, la dirección del pensamiento y de la acción para lograr algo previamente determinado. Significa entonces, que un buen método será aquel que garantice un máximo aprovechamiento o rendimiento de la enseñanza aprendizaje en menor tiempo.

Un método integra un conjunto de principios, una descripción de la praxis, actividades y normalmente el sistema de evaluación. La elección del método o métodos de enseñanza que se utilizaran, dependerá gran parte de la información o habilidad que se está enseñando, en los métodos educativos se trabaja las habilidades cognitivas, las cuales serán afectadas por el contenido de aprendizaje y el nivel de los estudiantes. [Martínez, J. 2004].

2.8. Riesgos.

El riesgo es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático, causando un determinado impacto en la organización. [Gómez Vieites, 2017]

Un riesgo es cualquier tipo de evento o circunstancia que de ocurrir amenazarían los objetivos de una organización, estos riesgos tienen una posibilidad de ocurrencia por lo que se miden como la multiplicación de impacto por probabilidad [INDECOPI,2018]. Por lo tanto, el riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente.

2.8.1. Tipos de riesgos.

Explica tres naturalezas del riesgo, estos son: los riesgos estratégicos, tácticos y operacionales.

- Los riesgos estratégicos son los que pueden estar ligados a la seguridad de la

información; sin embargo, se encuentran más orientados a los riesgos de las ganancias y reputación de la organización, ya que se derivan de decisiones estratégicas que han sido tomadas o serán tomadas en la organización.

- Los riesgos tácticos son los asociados a los sistemas que vigilan la identificación, control y monitoreo de los riesgos que afectan a la información.
- Los riesgos operacionales son los relacionados a aquellos activos que pueden afectar los objetivos de una empresa (tales como presupuestos, cronogramas y tecnologías).

2.8.2. Gestión de riesgos

Es necesario discernir que la gestión de riesgos es una pieza vital dentro de la implantación de un SGSI, razón por la cual, la familia de normas de la NB/ISO/IEC 27000:2010 especifica una norma dedicada a lo referido, tal es la norma de la NB/ISO/IEC 27005:2010. Que no especifica ningún método de análisis de riesgo concreto, sino que, contiene recomendaciones y directrices generales para la gestión de riesgos, por tanto, puede utilizarse como guía para elaborar una metodología de gestión de riesgos de la organización.

Un proceso de gestión de riesgos comprende una etapa de evaluación previa de los riesgos del sistema informático, que se debe realizar con rigor y objetividad para que cumpla su función con garantías. [Gómez, Vieites.2017]**.** Los que realizan esta evaluación deben tener un nivel adecuado de formación y experiencia de los riesgos. Además de recursos y medios.

Se tiene el siguiente ejemplo en la figura 2.2 evaluación y gestión de riesgo.

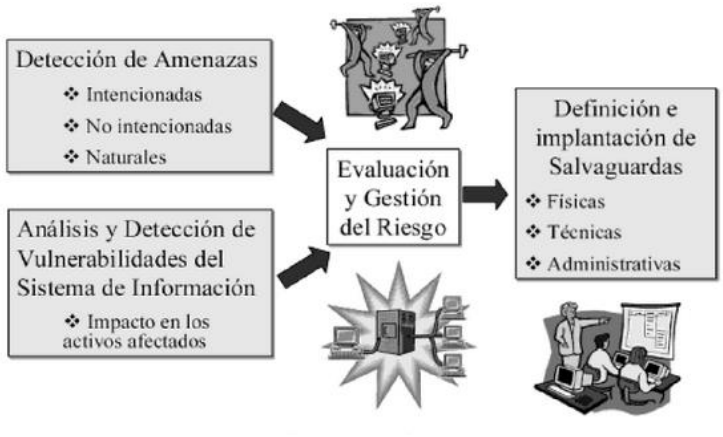


Figura 2.2 Evaluación y gestión del riesgo

Fuente: Gómez Vieites,2017. Enciclopedia de la seguridad

2.9. Control

Medios para manejar el riesgo, incluyendo políticas, procedimientos, lineamientos, practicas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal. [Aliaga, Flores, 2013].

Una clasificación generalizada de los controles puede ser:

- Preventivos: reducen las vulnerabilidades.
- Detectivos: descubren amenazas o escenarios previos a ellas permitiendo activar otros controles.
- Correctivos: contrarrestan el impacto de la ocurrencia de una amenaza.
- Disuasivos: reducen la probabilidad de ocurrencia de las amenazas. (Tupia, 2009) [Aguirre,2014].

2.10. Seguridad

La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.

Medios para manejar el riesgo, incluyendo políticas, procedimientos, lineamientos, practicas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas de gestión o de naturaleza legal. [Aliaga Flores, 2013]

La seguridad informática es la disciplina que, con base en políticas y normas internas y externas de la organización, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riesgos tanto físicos como lógicos, a los que está expuesta. [Baca, Gabriel, 2016]. En la coyuntura actual la seguridad es la constante búsqueda de una organización, en cuanto a la seguridad informática, ya que es el activo más preciado en un CPD. Y por otro lado es lo que más se busca perforar en los sistemas que maneja una organización, por parte de intrusos. Además de que existe riesgos por la pérdida de la información que ya no se puede recuperar en el peor de los casos.

La anterior definición hecha por Baca se puede complementar señalando que en caso de que una amenaza a la seguridad se haga efectiva, debe procurar recuperar la información dañada o robada.

Muchos investigadores y autores especializados en el tema de la seguridad informática por lo común se centran solo en las tres características de la información mencionadas; no

obstante, de acuerdo con el marco de gestión y de negocio global para el gobierno y la gestión de la tecnología informática (TI) de la empresa (COBIT por sus siglas en ingles), las características que debe poseer la información son: efectividad, eficiencia, confidencialidad, integridad, disponibilidad, apego a los estándares y confiabilidad.

Se establecen 8 dimensiones de la seguridad: Control de acceso, autenticación, no repudio, confidencialidad de los datos, seguridad de la comunicación, integridad de los datos, disponibilidad y privacidad (Zhao, 2006) [Velasco, Paola, 2017]

2.10.1. Seguridad física

Cuando hablamos de seguridad física nos referimos a todos aquellos mecanismos generalmente de prevención y detección destinados a proteger físicamente cualquier recurso del sistema; estos recursos son desde un simple teclado hasta un backup con toda la información que hay en el sistema, pasando por la propia CPU de la máquina.

Dependiendo del entorno y los sistemas a proteger esta seguridad será más o menos importante y restrictiva, aunque siempre deberemos tenerla en cuenta.

2.10.1.1. Protección de Hardware

El hardware es frecuentemente el elemento más caro de todo sistema informático y por tanto las medidas encaminadas a asegurar su integridad son una parte importante de la seguridad física de cualquier organización.

Problemas a los que nos enfrentamos:

- Acceso físico

- Desastres naturales
- Alteraciones del entorno

Acceso físico: si alguien que desee atacar un sistema tiene acceso físico al mismo todo el resto de medidas de seguridad se convierten en inútiles.

Incluso dependiendo el grado de vulnerabilidad del sistema es posible tomar el control total del mismo, por ejemplo, reiniciándolo con un disco de recuperación que nos permita cambiar las claves de los usuarios.

Este último tipo de ataque es un ejemplo claro de que la seguridad de todos los equipos es importante, generalmente si se controla el PC de un usuario autorizado de la red es mucho más sencillo atacar otros equipos de la misma.

Para evitar todo este tipo de problemas deberemos implantar mecanismos de prevención (control de acceso a los recursos) y de detección (si un mecanismo de prevención falla o no existe debemos al menos detectar los accesos no autorizados cuanto antes)

Para la prevención hay soluciones para todos los gustos.

- Analizadores de retina,
- Tarjetas inteligentes,
- Videocámaras,
- Vigilantes jurados

En muchos casos es suficiente con controlar el acceso a las salas y cerrar siempre con llave los despachos o salas donde hay equipos informáticos y no tener cableadas las tomas de red que estén accesibles.

Para la detección de accesos se emplean medios técnicos, como cámaras de vigilancia de circuito cerrado o alarmas, aunque en muchos entornos es suficiente con qué las personas que utilizan los sistemas se conozcan entre sí y sepan quien tiene y no tiene acceso a las distintas salas y equipos, de modo que les resulte sencillo detectar a personas desconocidas o a personas conocidas que se encuentran en sitios no adecuados.

Desastres naturales: además de los posibles problemas causados, por ataques realizados por personas, es importante tener en cuenta que también los desastres naturales pueden tener muy graves consecuencias, sobre todo si no los contemplamos en nuestra política de seguridad y su implantación.

Algunos desastres naturales a tener en cuenta.

- Terremotos y vibraciones
- Tormentas eléctricas
- Inundaciones y humedad
- Incendios y humos
- Control de acceso. En una infraestructura de este tipo siempre tenemos que tener el control en tiempo real de quien entra a donde, y para qué.
- Pruebas de mecanismos de detección y alarma. Extintores, la sala de contraincendios, los sensores de humedad, de temperatura, de detección de humo y de movimiento.
- Acceso de mercancía y personal de proveedores.
- Ausencia de seguridad perimetral o seguridad perimetral insuficiente.
- Gestión de energía. En estos centros se consumen grandes cantidades de

energía, y por tanto, se requieren medidas para asegurar el flujo de energía estética garantizada ante cualquier tipo de incidente, suministro se puede establecer como medios alternativos. Por norma general el CPD debe ser en lo posible independiente, para no depender exclusivamente de un único proveedor, y es frecuente que se hagan abastecimientos a zonas teniendo en cuenta la cantidad máxima de resiliencia eléctrica o no. Cuando todo va mal y se pierde completamente el fluido eléctrico, es normal contar con una batería de generadores diésel para garantizar el suministro en caso de contingencia eléctrica grave.

- Ausencia de compartimiento especialmente relevante en el caso de los centros de datos públicos o destinados al uso de múltiples clientes. En estos casos es lógicamente cerrada.

2.10.2. Seguridad lógica

Son las medidas internas del CPD. Características de estos sistemas:

- La mayoría de ataques tienen como objetivo la obtención de información, no la destrucción del medio físico que la contiene.

En los puntos siguientes mencionaremos los problemas de seguridad que afectan a la transmisión y almacenamiento de datos, proponiendo medidas para reducir el riesgo.

La interceptación o eavesdropping, también conocida por passive wiretapping, es un proceso mediante el cual un agente capta información que va dirigida a él; esta captación puede realizarse por muchísimos medios: sniffing en redes ethernet o inalámbricas un

dispositivo se pone en modo promiscuo y analiza todo el tráfico que pasa por la red, capturando radiaciones electromagnéticas muy caro, pero permite detectar teclas pulsadas, contenidos de pantallas, copias de seguridad, soportes no electrónicos, el sistema de arranque, la BIOS del PC Intel, la OpenBootProm de Sun SPARC. Además de:

- Actualización de los sistemas: englobamos aquí todos los problemas relacionados con la falta de actualización de los elementos del CPD: sistemas operativos, aplicaciones, firmware, hay que obtener pruebas de que los sistemas más se están actualizando, y es posible que se verifique con una herramienta de análisis de vulnerabilidad la fiabilidad.

- Configuración de seguridad: en este apartado se incluye la red de seguridad que deriva de la falta de gestión de los componentes puestos y producción como enrutadores, conmutadores y demás elementos de red.

- Operaciones de seguridad: en un CPD tiene que haber operaciones de seguridad IDS / IPS, firewalls, honeypots, gestión antifraude, SIEM, DLPs.

- Segregación de entorno: tener entornos de producción, aceptación, soporte, desarrollo y pruebas compartiendo los mismos discos en distintas particiones es normal, pero también es posible cometer errores de configuración que permitan el salto entre particiones.

- Cifrado: hay que tener en cuenta que es en general los datos en su caso y en su lugar están cifradas allí donde es susceptible de interceptarlos, por ejemplo, en las copias de seguridad, o la posibilidad de interceptar el tráfico de explotación, que podría tener datos confidenciales como usuarios y contraseñas.

- Accesos privilegiados: en un CPD es necesario tener accesos privilegiados para poder operar los servicios. Es una parte natural del uso de servicios que contemplan la gestión de usuarios, como, por ejemplo, los sistemas operativos, aunque el acceso privilegiado puede ser definido por otros aspectos, como, por ejemplo, los segmentos de red en la explotación que son capaces de acceder a servicios críticos.

- Accesos remotos: en los casos donde el desarrollo lo hacen empresas externas, donde también es posible que se ocupe del mantenimiento, es crucial entender cómo se accede y cuál es su nivel de privilegio. Aunque es normal que estos accesos se hacen con la cabeza, mediante conexiones VPN o circuitos MPLS dedicados, hay que cerciorarse de tener absolutamente claro quien accede y cómo.

- Entornos multicliente: en casos de centros de procesamientos de datos públicos o semipúblicos es posible que los servicios sean utilizados como varios clientes.

- Continuidad y recuperación: controlar la calidad del material y sistema de mantenimiento continuo. [Pichardo, J.2017]

2.11. Planes de Seguridad.

Como norma general, debería ser redactado el Plan de Seguridad de cada Centro de Procesamiento de Datos, como documento que recoja aquellos aspectos relacionados con la seguridad de los mismos y que, ante el riesgo de intrusión, terrorismo, robo, etc. desarrollará los siguientes puntos:

- Normas para establecer el control de acceso.

- Diseño del sistema de seguridad ante el riesgo de intrusión.
- Planos de ubicación de elementos de Seguridad.
- Distribución de líneas de conexión.
- Datos de la Central Receptora de Alarmas.

2.11.1. Tipos de Seguridad.

2.11.1.1. Activa

Comprende el conjunto de defensas o medidas cuyo objetivo es evitar o reducir los riesgos que amenazan al sistema. [Aguilera, P,2010].

Ejemplos: impedir el acceso a la información a usuarios no autorizados mediante introducción de nombres de usuario y contraseña; evitar la entrada de virus instalando un antivirus; impedir, mediante encriptación, la lectura no autorizada de mensajes.

2.11.1.2. Pasiva.

Está formada por las medidas que se implementan para, una vez producido el incidente de seguridad, minimizar su repercusión y facilitar la recuperación del sistema; por ejemplo, teniendo siempre al día copias de seguridad de los datos. [Aguilera, P,2010].

Es importante el back up, pero no entrar en la de-duplicacion.

2.12. Vulnerabilidades.

Una vulnerabilidad es una debilidad o fallo en un sistema de información que pone en

riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la confidencialidad, integridad o disponibilidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible. [Incibe, 2019]. La vulnerabilidad está presente cuando se empiezas a realizas monitoreo en SGSI.

2.12.1. Tipos de vulnerabilidades

- Conocidas sobre aplicaciones o sistemas instalados

Son vulnerabilidades de las que ya tienen conocimiento las empresas que desarrollaran el programa al que afecta y para los cuales ya existe una solución, que se publica en forma de parche.

Existen listas de correo relacionadas con las noticias oficiales de seguridad que informan de la detección de esas vulnerabilidades y las publicaciones de los parches a las que podemos suscribirnos.

- Conocidas sobre aplicaciones no instaladas

Estas vulnerabilidades también son conocidas por las empresas desarrolladores de la aplicación, pero puesto que nosotros no tenemos dicha aplicación instalada no tendremos que actuar.

- Aún no conocidas

Estas vulnerabilidades aún no han sido detectadas por la empresa que desarrolla el programa, por lo que, si otra persona ajena a dicha empresa detectara alguna, podría utilizarla contra todos los equipos que tienen instalado este programa.

Se tiene la siguiente tabla sobre la clasificación de vulnerabilidades Tabla. 2.1

Calificación	**Definición**
Critica	Vulnerabilidad que puede permitir la propagación de un gusano de internet sin la acción del usuario.
Importante	Vulnerabilidad que puede poner en peligro la confidencialidad, integridad o disponibilidad de los recursos de procesamiento.
Moderada	El impacto se puede reducir en gran medida a partir de factores como configuraciones predeterminadas, auditorias o la dificultad intrínseca en sacar partido a la vulnerabilidad.
Baja	Vulnerabilidad muy difícil de aprovechar o cuyo impacto es mínimo.

Tabla 2.1 Clasificación de gravedad de vulnerabilidades

Fuente. Incibe, 2019

2.13. Amenazas

Se considera una amenaza a cualquier evento accidental o intencionado que pueda ocasionar algún daño en el sistema informático, provocando pérdidas materiales, financieras o de otro tipo a la organización. [Gómez, 2010].

Las amenazas son por accidentes fortuitos o de manera provocada debido a un interés.

Se puede establecer la siguiente clasificación a la hora de estudiar las amenazas a la seguridad.

- Amenazas naturales: inundación, incendio, tormenta, fallo eléctrico, explosión.
- Amenazas de agentes externos: virus informáticos, ataques de una organización

criminal, sabotajes terroristas, disturbios y conflictos sociales, intrusos en la red, robos, estafas, etcétera.

- Amenazas de agentes internos: empleados descuidados con una formación inadecuada o descontentos, errores en la utilización de las herramientas y recursos del sistema.

También definimos una clasificación alternativa, teniendo en cuenta el grado de intencionalidad de la amenaza.

- Accidentes: averías del hardware y fallos del software, incendio, inundación…
- Errores: errores de utilización, de explotación, de ejecución de determinados procedimientos, etcétera.
- Actuaciones malintencionadas: robos, fraudes, sabotajes, intentos de intrusión, etcétera. [Gómez, 2010].

2.14. Centro de Procesamiento de datos

Un data center o también llamado centro de procesamiento de datos (CPD) es un espacio con determinadas características físicas especiales de refrigeración, protección y redundancia, cuyo objetivo es alojar todo el equipamiento tecnológico de una organización brindando seguridad y confiabilidad. Todas estas condiciones aseguran la disponibilidad de los servicios de red. [Pació, G. 2014]

Es un lugar crítico para una organización, ya que en él se alojan los activos más importantes de una organización, y además es una unidad de negocio muy importante con valor propio. En este espacio físico se almacenarán los servidores que enviaran sus correos electrónicos, alojan a los servidores web de la organización: su cara al cliente. También se

procesarán las transacciones del negocio y los balances, se guarda información sensible financiera, e incluso secretos industriales.

Los costos de construcción y mantenimiento de un data center tienen un porcentaje importante dentro del presupuesto total de infraestructura tecnológica (IT). Por ello es fundamental no fallar en el momento del diseño estructural y de sus componentes centrales. Debido a la infraestructura especial necesaria los costos de construcción y operación por metro cuadrado son mucho más altos comparándolos con los espacios de oficinas tradicionales. [Pació, G. 2014]

Todas estas condiciones hacen que un data center sea un lugar clave dentro la organización.

2.14.1. Clasificación

Los data centers se caracterizan según su dimensión y según sus prestaciones físicas hacia los elementos que almacenan. Existen tres tipos.

- Sala de servidores: es una estructura chica, pocos servidores. Muy informal.
- Centro de cómputos: dimensión mediana, puede tener Rack, condiciones de seguridad y ambientales básicas.
- Data center: gran dimensión, obligatoriamente todos los elementos que lo componen están alojados en racks de forma ordenada, bajo condiciones de seguridades reguladas, controles estrictos eléctricos y ambientales (incluso alguno o varios sistemas redundantes).

Descripción de prestaciones generales, como se ve en la Tabla 2.2.

Característica	Sala servidores	Centro de cómputos	Data Center
Piso flotante	No	No/Si	Si
Tamaño	< 20 mts2	< 40 mts2	>40 mts2
Cantidad de servers	< 20	< 50	>50
Aire acondicionado	Hogareño	Profesional	Profesional/central
Acceso	Cerradura	Tarjeta magnética	Tarjeta magnética/Biométrico
Red	Hub/switch	Switch	Fiber switch
Cableado	Utp 5/5E	Utp 5E/6	UTP 6a/fibra óptica
Sistema eléctrico de contingencia	No	UPS	UPS + Generador
Prevención de incendios	No	Extintores manuales	Detección de humo + Extintor de fuego + Rociadores.
Registro de accesos físicos	Manual	Manual	CCTV
Sensores o detectores	No	No	Si
Monitoreo centralizado	No	No	Si

Tabla 2.2 Prestaciones generales típicas

Fuente: Pacio,2014

2.15. Seguridad de la información

La seguridad de la información es la protección de la confidencialidad, integridad y disponibilidad de la información; es decir, es asegurarse que esta sea accesible solo a las personas autorizadas, sea exacta sin modificaciones no deseadas y que sea accesible a los usuarios cuando lo requieran. Así también puede involucrar otras propiedades como la autenticidad, no repudio y confiabilidad. La seguridad de la información protege a la

información (implantando un conjunto adecuado de controles -que pueden ser políticas, prácticas, procedimientos, estructuras organizativas y funciones de software y hardware, monitoreándolos, revisándolos y mejorando donde sea necesario) de un amplio rango de amenazas para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio (INDECOPI, 2007).

2.16. Infraestructura tecnológica / Plataforma.

Es el conjunto de sistemas: ordenadores, equipos de electrónica de red, equipos de almacenamiento, y demás elementos físicos, junto con la manera que se ha elegido para gestionarlos, lo que incluye procesos y herramientas de gestión de los equipos, de medición de su rendimiento, de seguridad ante incidencias y catástrofes además de los sistemas operativos básicos. [Ceupe, 2018]

El servicio que ofrece el conjunto de dispositivos y aplicaciones para una organización, es conocido como infraestructura IT. Este sistema se gestiona a través de la monitorización mediante el despliegue de los equipos suficientes, máquinas y software para el usuario.

2.16.1. Los elementos de la infraestructura IT.

Son cuatro los elementos que forman la infraestructura tecnológica IT:

- **Servidores:** existen distintos tipos de servidores en función de las necesidades de las empresas y el tamaño de estas.
- **Almacenamiento:** son diferentes soluciones de almacenamiento las que pueden aplicarse, entre otras, las hiperconvergentes cabinas de almacenaje y los dispositivos NAS como posibles copias de seguridad.

- **Networking:** esto permite distintas funcionalidades al sistema sin correr riesgos de seguridad. La agilidad y la flexibilidad hacen aumentar la visibilidad en las redes.
- **Seguridad:** este elemento proporciona seguridad informática a la organización y facilita el acceso a los datos en caso de pérdida o un ataque al sistema. [Saavedra, A. 2018].

2.17. Estándares de seguridad.

2.17.1. BICSI.

BICSI es una asociación profesional que apoya a la industria de los sistemas de tecnología de la información (ITS). Los STI cubren el espectro de las tecnologías de voz, datos, seguridad y protección electrónica y audio y video. Abarca el diseño, la integración y la instalación de vías, espacios, sistemas de distribución basados en fibra y cobre, sistemas inalámbricos e infraestructura que soportan el transporte de información y la señalización asociada entre las comunicaciones y los dispositivos de recopilación de información.

BICSI es una asociación global que impulsa la comunidad de tecnologías de la información y la comunicación.

Las normas internacionales de BICSI contienen información que se considera de carácter técnico para la industria y se publican a petición del comité organizados. El programa de Normas internacionales de BICSI somete todas sus pautas preliminares a un rigoroso proceso de resolución de comentarios surgidos de la revisión publica, que forma parte del proceso integral de desarrollo y aprobación de toda norma internacional de BICSI.

El programa de Normas Internacionales de BICSI revisa periódicamente sus pautas. Al finalizar el quinto año tras haberse publicado, la norma se revocará o modificará según las actualizaciones y comentarios presentados por todas las partes interesadas.

2.17.2. El Estándar TIA 942 En Data Center.

Concebido como una guía para los diseñadores e instaladores de centros de datos, el estándar TIA942 (2005) proporciona una serie de recomendaciones y directrices (guidelines) para la instalación de sus infraestructuras.

Aprobado en 2005 por ANSI-TIA (American National Standars Institute-Telecomunications Industry Association), clasifica a este tipo de centros en varios grupos, llamados TIER, indicando así su nivel de fiabilidad en función del nivel de disponibilidad.

Al diseñar los centros de datos conforme a la norma, se obtienen ventajas fundamentales como son:

- Nomenclatura estándar.
- Funcionamiento a prueba de fallos.
- Aumento de la protección a agentes externos.
- Fiabilidad a largo plazo, mayores capacidades de expansión y escalabilidad.

De acuerdo con el estándar TIA-942, la infraestructura de soporte de un Data Center estará compuesta por cuatro subsistemas:

- Telecomunicaciones: cableado de armarios y horizontal, accesos redundantes, cuarto de entrada, área de distribución, backbone, elementos activos y

alimentaciones redundantes, patch panels y latiguillos, documentación.

- Arquitectura: selección de ubicación, tipo de construcción, protección ignifuga y requerimientos NFPA 75(Sistemas de protección contra el fuego para información), barreras de vapor, techos y pisos, áreas de oficina, salas de UPS y baterías, sala de generador, control de acceso, CCTV, NOC (Network Operations Center – Centro operativo).
- Sistema eléctrico: número de accesos, puntos de fallo, cargas críticas, redundancia de UPS y topología de UPS, puesta a tierra, EPQ (Emergency Power Off-sistemas de corte de emergencia) baterías, monitorización, generadores, sistemas de transferencia.
- Sistema mecánico: climatización, presión positiva, tuberías y drenajes, CRACS y condensadores, control de HVAC (High Ventilating Air Conditionning), detección de incendios y sprinklers, extinción por agente limpio (NFPA 2001), detección de líquidos.

Asimismo, y siguiendo las indicaciones del estándar, un CPD deberá incluir varias áreas funcionales:

- Una o varias entradas al centro.
- Área de distribución principal.
- Una o varias áreas de distribución principal.
- Áreas de distribución horizontal.
- Área de equipo de distribución.
- Zona de distribución.

- Cableado horizontal y backbone.

A continuación, en la Tabla 2.3 se tiene principales características de los Tiers.

SUBSISTEMA ARQUITECTONICO	TIER I	TIER II	TIER III	TIER 4
Proximidad a áreas de inundación Registradas por las autoridades	NA	No permitido Dentro de áreas	No debe haber Historias de Inundación durante los últimos 100 años y de 50 años a menos de 91 m.	No debe haber historias de inundación durante los últimos 100 años a menos de 91m.
Proximidades a autopistas	NA	NA	No menos de 91 m.	No menos de 0.8 Km.
Proximidades a aeropuertos	NA	NA	No menos de 1.6 Kms. y no más 48 Kms.	No menos de 8 Kms y no más de 48 Kms.
Áreas de parqueo de visitantes y Empleados separados	NA	NA	Si, físicamente separada por una barrera o pared	18.3 mts. de separación con barreras físicas
Edificio con diferentes dueños	NA	Permitido si no hay riesgos en los ocupantes	Permitido si todos los ocupantes son compañías de TC	Permitido si todos los ocupantes son compañías de data centers o TC
Debe cumplir con requerimiento De NFPA 75	NA	Si	Si	Si

Tabla 2.3 Principales características de los tiers

Fuente: Norma ANSI/TIA 942,2005

2.17.3. El concepto de TIER.

El nivel de fiabilidad de un centro de datos viene indicado por uno de los cuatro niveles

de fiabilidad llamados TIER, en función de su redundancia. A mayor número de TIER, mayor disponibilidad, y por tanto mayores costes de construcción y mantenimiento. Como se ve en la Tabla 2.4.

TIER	% Disponibilidad	% Parada	Tiempo anual de parada
TIER I	99.67%	0.33%	28.82 horas
TIER II	99.74%	0.25%	22.68 horas
TIER III	99.982%	0.02%	1.57 horas
TIER IV	100.00%	0.01%	52.56 minutos

Tabla 2.4 Nivel de fiabilidad de un centro de datos

Fuente: ANSI TIA,2005

TIER I-Nivel 1 (Básico)

- Disponibilidad del 99.671 %.
- Sensible a las interrupciones, planificadas o no.
- Un solo paso de corriente y distribución de aire acondicionado, sin componentes redundantes.
- Sin exigencias de piso elevado.
- Generador independiente.
- Plazo de implementación: 3 meses.
- Tiempo de inactividad anual: 28.82 horas.
- Debe cerrarse completamente para realizar mantenimiento preventivo.

TIER II- Nivel II (Componentes redundantes)

- Disponibilidad de 99.741 %.
- Menor sensibilidad a las interrupciones.
- Un solo paso de corriente y distribución de aire acondicionado, con un componente redundante.
- Incluye piso elevado, UPS y generador.
- Plazo de implementación: 3 a 6 meses.
- Tiempo de inactividad anual: 22.0 horas.
- El mantenimiento de la alimentación y otras partes de la infraestructura de un cierre de procesamiento.

TIER III-Nivel III (Mantenimiento concurrente)

- Disponibilidad 99.982 %.
- Interrupciones planificadas sin interrupción de funcionamiento, pero posibilidad de problemas en las no previstas.
- Múltiples accesos de energía y refrigeración, por un solo encaminamiento activo. Incluye componentes redundantes (N+1).
- Plazo de implementación: 15 a 20 meses.
- Tiempo de inactividad anual: 1.6 horas.

TIER IV – Nivel IV (Tolerancia a errores)

- 99,995 % de disponibilidad.

- Interrupciones planificadas sin interrupción de funcionamiento de los datos críticos. Posibilidad de sostener un caso de improviso sin daños críticos.
- Múltiples pasos de corriente y rutas de enfriamiento, incluye componentes redundantes. Incluye componentes redundantes (2(N+1))-2 UPS cada uno con redundancia (N+1).
- Plazo de implementación: 15 a 20 meses.
- Tiempo de inactividad anual: 0,4 horas. [Cofitel, 2014]

2.17.4. Norma 942A.

Resumimos en este apartado las modificaciones introducidas, en el campo del cableado, tanto en fibra como en cobre, por el estándar TIA 942A, de aplicación en Data Centers.

Si bien se trata de una normativa de origen USA, el estándar ANSI/TIA-942, editado en 2005, y con revisiones cada 5 años, puede ser considerado como "un sistema genérico de cableado para los Data Centers y su ámbito de influencia" (Pagina IX de las normativas). En su reciente actualización (2013), incorpora las siguientes novedades:

- La utilización en los DC de fibras multimodo queda reservada a los tipos OM3 y OM4 (50/125) y equipos con emisores LASER 850 nm. Quedando prohibida la utilización de fibras de los tipos OM1 y OM2 anteriormente empleados.

- Para los cableados de cobre, se recomienda el empleo de Cat6 apantallados. En este campo se coincide con ISO/IEC 24764, que reconoce únicamente enlaces Clase EA (Cat 6ªA)

- Queda suprimida la limitación de 100 m. de longitud en cableados horizontales, para la fibra óptica, quedando la definición de este concepto a la responsabilidad del fabricante.
- Conectores ópticos: queda reducida la selección a los tipos LC. [Cofitel, 2014] para actualizaciones de la norma 942A ANSI/BICSI 002-2014, Mejores prácticas de diseño e implantación de centro de datos. [BICSI,2018]

2.18. Norma NB/ISO/IEC 27001:2013.

Norma estándar para la seguridad de la información publicada en octubre de 2005 y modificada a finales del 2013. Describe los aspectos necesarios para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información en las organizaciones independientes de su tipo, tamaño o naturaleza. Esta norma también incluye los requisitos para la valoración y el tratamiento de riesgos de seguridad de la información, adoptadas a las necesidades de la organización.

Se conoce comúnmente como el Ciclo de Deming (Planear, Hacer, Verificar, Actuar) o PDCA. Como vemos en la figura 2.3

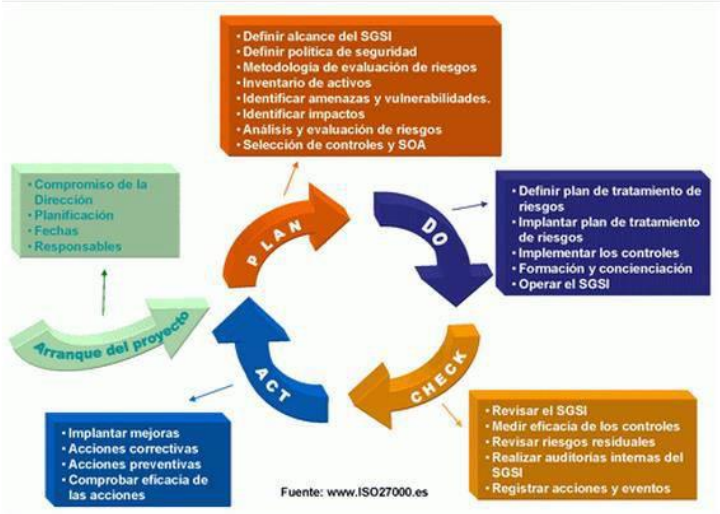


Figura 2.3. Ciclo Deming

Fuente: Agustín & Javier,2016

El nombre del ciclo PDCA (o ciclo PHVA) viene de las siglas Planificar, Hacer, Verificar y Actuar, También es conocido como ciclo de mejora continua o circulo de Deming, por ser Edward Deming su autor. Esta metodología describe los cuatro casos esenciales que se deben llevar a cabo de forma sistemática para lograr la mejora continua. Entendiendo como tal el mejoramiento continuado de la calidad disminución de fallos, aumento de la eficacia y eficiencia, solución de problemas, previsión y eliminación de riesgos potenciales… [Agustín & Javier,2016].

Los dominios de la norma NB/ISO/IEC 27001:2013 corresponde a los diferentes capítulos que establecen los requerimientos que las organizaciones deben cumplir para el establecimiento de un Sistema de Gestión de Seguridad de la Información, las cuales se resumen a continuación en la figura 2.4.

0.	Introducción
1.	Objeto y campo de aplicación
2.	Referencias normativas
3.	Términos y definiciones
4.	Contexto de la organización
5.	Liderazgo
6.	Planificación
7.	Soporte
8.	Operación
9.	Evaluación de desempeño
10.	Mejora

Figura 2.4. Dominios de la norma

Fuente: NB/ISO/IEC 27001:2013

2.19. Norma /ISO/IEC 27002:2014.

Esta 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 la información (SGSI) en base a ISO/IEC 27001 para las organizaciones que implementan controles de seguridad de información de aceptación común. Esta norma también es para el uso en el desarrollo de directrices de gestión de seguridad de la información y la industria de la organización, teniendo en cuenta su entorno de riesgo seguridad de la información.

Organizaciones de todos los tipos y tamaños incluyendo sector público y privado, comercial y sin fines de lucro, recoger procesar, almacenar y transmitir información en muchas formas, incluyendo conversaciones y presentaciones por ejemplo electrónicos, físicos y verbales.

Los activos están sujetos a las amenazas deliberadas o accidentales, mientras que los relacionados con los procesos, los sistemas, las redes y las personas tienen vulnerabilidades inherentes. Los cambios en los procesos de negocio y sistemas u otros cambios externos (por ejemplo, nuevas leyes y reglamentos) pueden crear nuevos riesgos de seguridad de la información. Por lo tanto, dada la multiplicidad de formas en que las amenazas podrían aprovecharse de las vulnerabilidades para dañar a la organización, los riesgos de seguridad de la información están siempre presentes. Seguridad de la información eficaz reduce estos riesgos mediante la protección de la organización contra las amenazas y vulnerabilidades, y luego reduce los impactos de sus activos.

Seguridad de la información se logra mediante la implementación de un conjunto adecuado de controles, incluidas las políticas, procesos, procedimientos, estructuras organizativas y de software y funciones de hardware. Estos controles se deben establecer, implementar, supervisar, revisar y mejorar, cuando sea necesario, para asegurar que se cumplan los objetivos específicos de seguridad y de negocios de la organización. Un SGSI como el que se especifica en la norma ISO/IEC 27001 tiene una visión holística y coordinada de los riesgos de seguridad de la información de la organización con el fin de poner en práctica un conjunto completo de controles de seguridad de la información en el marco general de un sistema de gestión coherente.

Muchos sistemas de información no han sido diseñados para ser seguro en el sentido de la norma ISO/IEC 27000.

La norma ISO 27002 fue publicada originalmente como un cambio de nombre de la norma 17799 ISO existente, un código de prácticas para la seguridad de la información.

Básicamente describe cientos de potenciales controles y mecanismos de control, que pueden ser implementadas, en teoría, con sujeción a las directrices proporcionadas en la norma ISO 27001.” [Agustín & Javier,2016].

2.20. Norma ISO/IEC 27003:2011

Este estándar es nuestra guía para la implementación de un SGSI dentro la organización. Este documento explica dicha implementación enfocándose en la iniciación, planeamiento y la definición del proyecto: describe los procesos desde la obtención de la aprobación de la alta gerencia para implementar el SGSI hasta la conclusión final del plan de proyecto.

A diferencia de ISO 27001, este documento nos da recomendaciones y buenas prácticas, más no indica requerimientos ni obligaciones: es para el uso en conjunto con la norma ISO 27001 y no para modificar o reducir los requerimientos especificados en dicha norma.

El proceso del planteamiento de la implementación de un SGSI contiene cinco fases y cada fase es representada por una cláusula. Todas estas cláusulas tienen una estructura similar: cada clausula tiene uno o varios objetivos y una o varias actividades necesarias para lograr dichos objetivos. Las cinco fases son:

- Obtención de la aprobación de la alta gerencia para dar comienzo al SGSI.
- Definición del alcance de las políticas del SGSI.
- Conducir el análisis de la organización.
- Conducir un análisis de riesgos y un plan de tratamiento de riesgos.
- Diseñar el SGSI.

2.21. ISO/IEC/27005:2010

Este estándar nos brinda directrices para la gestión de riesgos de la seguridad de información, dando soporte particularmente a los requerimientos de un SGSI, de acuerdo con la norma ISO/IEC 27001. Sin embargo, esta norma no es de por si una metodología para la gestión de riesgos, aunque lo puede llegar a ser según el alcance que el SGSI tenga o el contexto de la gestión de riesgos donde se aplique dicha norma.

La estructura de la norma se descompone en 12 clausulas, las cuales son:

- Clausula 1: Alcance.
- Clausula 2: Referencias y términos
- Clausula 3: Términos y definiciones.
- Clausula 4: Estructura de la norma.
- Clausula 5: Background.
- Clausula 6: Resumen del proceso de la gestión de los riesgos de la seguridad de información.
- Clausula 7: Establecimiento del contexto.
- Clausula 8: Risk Assessment.
- Clausula 9: Risk Treatment.
- Clausula 10: Risk Acceptance.
- Clausula 11: Risk Comunication.
- Clausula 12: Risk Monitoring.

2.22. ICREA.

2.22.1. ICREA-Std-131-2017

ICREA-Std-131-2017 es un conjunto de recomendaciones y mejores prácticas consensadas entre varios países y un grupo de expertos en CPD que define la forma de construir un data center de acuerdo con los niveles de confiabilidad y seguridad deseados siendo los siguientes:

Nivel	Descripción	Disponibilidad
I	Quality assurance data center (QADC)	95%
II	World Class Quality Assurance Data Center (WCQA)	99%
III	Safety World Class Quality Assurance Data Center (S-WCQA)	99.9%
IV	High Securuty World Class Quality Assurance Data Center (HS-WCQA)	99.99%
V	High Security High Available World Class Quality Assurance Data Center (HSHA-WCQA)	99.999%
VI	Redundant High Available World Class Quality Assurance Data Center (RHA-WCQA)	99.9999%

Incluye: Aspectos generales

Instalaciones eléctricas

Climatización

Comunicaciones

Enviroment (Piso elevado, acabados, obra civil)

Seguridad (CCTV, control de acceso, detección y supresión de incendios)

Anexos para certificación de CPS's [ICREA,2016].

2.23. COSO

COSO define el control interno como un proceso, ejecutado por la junta de directores, la administración principal y otro personal de la entidad, diseñado para proveer seguridad razonable en relación con el logro de los objetivos de la organización. Tales objetivos son: eficacia y eficiencia de las operaciones; confiabilidad de la información financiera; cumplimiento de normas y obligaciones; y salvaguarda de activos. [Romero, 2012].

Bajo esta definición se debe indicar que es de suma importancia que la organización cuente con un historial de control interno porque podría ser de gran ayuda para proteger su seguridad y así no se vea afectada la continuidad de su organización. Como se ve en la figura 2.5 los aspectos claves de un control interno.

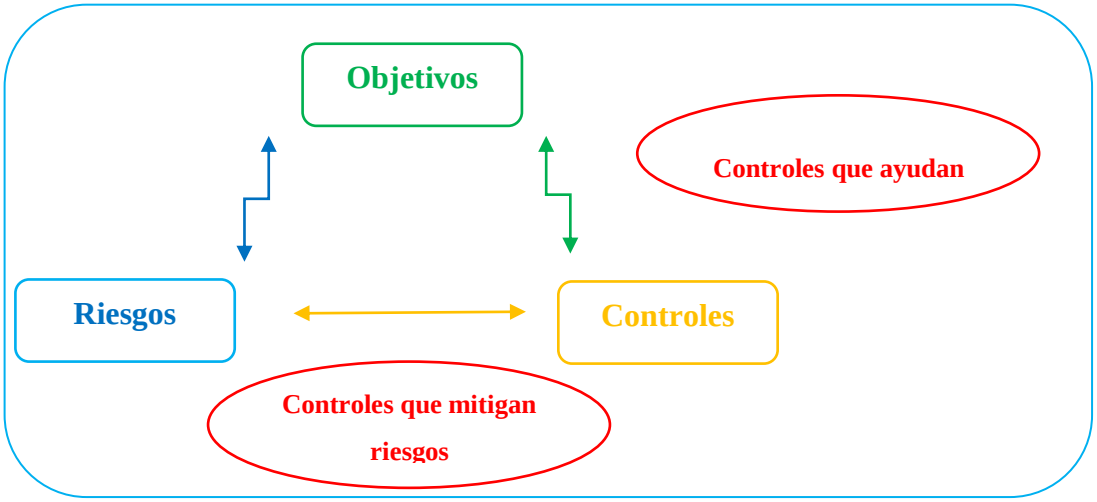


Figura 2.5. Aspectos claves de control interno

Fuente: Informe COSO,2013 Elaboración: Jorge Badillo Ayala

2.24. Definición según COBIT

Lo define como: Las políticas, procedimientos, prácticas y estructura organizacional, diseñados para brindar seguridad a los objetivos institucionales, logrando así que dichos objetivos sean alcanzados y erradicando o sanando eventos no deseados que se presenten (ISACA, 2012)

ISACA. (2012). *COBIT: Un marco de Negocio para el Gobierno y la Gestión de.* Estados Unidos: ISACA.

CAPÍTULO III

Fase de Desarrollo

En el presente capítulo se detallará el diseño del Modelo de Sistema Gestión de la Seguridad de la Información (SGSI) que servirá de base para la creación de un estándar al interior de una organización, necesaria para pensar en la implementación de este tipo de sistemas.

Para lograr la implementación de un SGSI, es necesario llevar a cabo unos pasos del ciclo PHVA (Planear, Hacer, Verificar y Actuar) de acuerdo a NB/ISO/IEC 27001:2013 para definir paso a paso la creación del sistema.

3.1. Planear

La planificación rastrea y busca las actividades de mejora para establecer los objetivos a lograr. Para buscar posibles mejoras se pueden conformar grupos de trabajo, recepcionar ideas a través de reuniones, las opiniones de los trabajadores, buscar tecnologías emergentes de las que se están usando ahora, entre otras.

Como primera acción es necesario la evaluación de los diagramas físicos y lógicos de la infraestructura existente en el data center. De esta manera podremos analizar que se tiene, que existe y concluir de ahí a donde será nuestros objetivos.

El estudio de información es el primer paso para la obtención de los conocimientos vigentes en distintas fuentes de información, y este va desde la recopilación y lectura de textos hasta la interpretación para obtener informes o resultados.

En esta etapa se afirmará los objetivos y procesos necesarios para llegar a demostrar los controles de seguridad de información esperados por la organización, en este caso de estudio, la defensa de los activos de información para las áreas ejecutivas. Para ello, realizaremos las siguientes acciones que enumeraremos a continuación:

Punto de partida: valoración de la situación de seguridad actual: como primera medición de los indicadores previstas antes del desarrollo del proyecto de investigación a la organización, citada esta información nos servirá como punto de partida para reconocer el valor de los indicadores antes de iniciarse las acciones planificadas, es decir establecer un punto de partida del proyecto.

Dentro del desarrollo del trabajo, este punto de partida que construiremos nos posibilitara establecer venideras comparaciones y permitiéndonos investigar por los cambios ocurridos conforme el programa o plan se vaya desarrollando.

El resultado del punto de partida se manifiesta en un informe que delinea la situación actual de la organización, en cuanto al estado de seguridad de los activos de información, el informe referido se basa en el estándar NB/ISO/IEC 27001:2013.

Análisis de brechas: este diagnóstico nos proporcionara conocer la condición actual de la organización de cara al cumplimiento de la NB/ISO/IEC 27001:2013, taxativamente en los 114 controles definidos en la NB/ISO/IEC 27002:2014 que el modelo o estándar ofrece, esto es, facilitándonos describir la realidad actual concerniente a la administración de seguridad de información al interior del modelo de negocio de la organización. Que tiene constituido un campo de acción mesurado y previa coordinación con el encargado superior de la organización, el plan de investigación se apoyará en 5 puntos, las cuales son:

- Cultura organizacional.
- Recursos Humanos.
- Control de accesos.
- Seguridad física y ambiental.
- Continuidad de negocio.

Las finalidades principales de este diagnóstico, son examinar la información emitida en el control, jerarquizando o priorizando las brechas respecto al programa fundamental del negocio para identificar las principales brechas respecto al plan esencial del ente para reconocer las principales brechas a tratar y proveer un resumen operativo determinando las más importantes dificultades de seguridad que padecen la entidad.

Tamaño	Apartado	Detalle	A	NA	AP	Inspección	Cita en la NB/ISO/IEC 27001:2013

Párrafos abajo, se propone el esquema del documento que será aplicado en el SGSI. Por otra parte, resulta muy esencial admitir que criterios o parámetros anotar en cada uno de los campos de la matriz de este documento:

- Tamaño: El tamaño básico de la seguridad de la información
- Apartado: Código del control que se está utilizando para llegar al objetivo de verificación consiguiente,
- Inspección: nombre de la inspección que se están utilizando para llegar al propósito de regulación correspondiente.
- A: Acata la defensa en la organización.
- NA: No acata la defensa en la organización.
- AP: Acata parcialmente la defensa en la organización.

- Inspección: concepto del monitoreo especifico basada en la norma.
- Cita de la NB/ISO/IEC 27001:2013: fundamento de la aplicación del monitoreo.

Con los cuales se tiene una vector de análisis de brechas, con lo cual establecemos estrategias y mecanismos de acción para llegar a resultados de procedimientos y objetivos de monitoreo y desarrollar SGSI.

3.2. Monitorear

En esta etapa del ciclo se realizan los cambios para implementar la mejora del data center.

Esta etapa del modelo PDCA, es la etapa donde la institución deberá implementar y poner en funcionamiento el SGSI, poniendo en práctica las políticas y los controles que de acuerdo al análisis de riesgo se han seleccionado para su cumplimiento. Para ello deberá implementar y poner en funcionamiento el SGSI, poniendo en práctica las políticas y los controles que de acuerdo al análisis de riesgo se han seleccionado para su cumplimiento. Para ello deberá disponer de procedimiento en los que se identifique claramente quien debe que hacer cada tarea previa capacitación para ello.

Para ello debe cumplirse con los siguientes objetivos:

- Aplicación de estándares y procedimientos de seguridad: en esta actividad se tendrá que elaborar y aplicar los estándares de seguridad de la información definidos dentro del alcance del SGSI, y una línea base para la organización, así como los procedimientos correspondientes y complementarios a estos estándares.

- Implementación de controles: una vez realizado el alcance, políticas, resultado de la evaluación de riesgos (Alto nivel y detallado), declaración de aplicabilidad y plan de tratamiento de riesgo, la siguiente acción es la implementación de cada control, correspondiente a un objetivo de control, debiendo de analizarse como mini-proyecto en el sentido de su estrategia de implementación. Dependiendo de la dimensión del control, tendrá documentación especifica de su fase conceptual y de diseño y por otro lado un nivel más detallado respecto a su implementación concreta con las actividades y aspectos técnicos, instrumentación, planes de capacitación, asesorías, etc. Por todo lo anterior, es conveniente formular un plan de implementación de controles, a los efectos de estimar recursos y tiempo que deberá ser apropiado por la dirección ejecutiva, es por ello habiendo mencionado en el inicio de un caso de estudio posible, que dicha investigación se basaría en la propuesta de un SGSI, queda como responsabilidad de la institución realizar la implementación SGSI.

Pero como recomendación para la implementación del SGSI, mencionamos que los controles que contienen niveles no tolerables por la institución, deben tener prioridad de implementación para su mitigación, los activos que tiene un riesgo muy elevado son los siguientes.

- Las políticas de seguridad: afectan a los activos de tipo personal.
- Aspectos organizativos de la seguridad de la información: afecta al activo de centro documentario (documento).
- Seguridad ligada a los recursos humanos: afecta a los activos comprendidos con valor cualitativo.
- Seguridad física y ambiental: afecta a los activos

- Seguridad en las operaciones: afecta al activo data center (servidor).

3.3. Hacer

El resultado de los riesgos y vulnerabilidades en cuanto a seguridad deben plasmarse en las políticas de seguridad para no solo proteger el sistema y la infraestructura una sola vez, sino defenderla continuamente

Una vez implantada las mejores propuestas, se deja un periodo de prueba para verificar su correcto funcionamiento. Si la mejora no cumple las expectativas iniciales habrá que modificarla para ajustarla a los objetivos esperados, como mejora continua.

3.4. Actuar

Para que todas las actividades y análisis presentados sean validados es importante que tengan un respaldo de calidad y esto se logra basándose en normas establecidas como lo es el estándar NB/ISO/IEC 27001:2013 el cual debemos estudiar para moldear nuestras políticas y presentar un completo e integro documento para implementar en la organización.

Una vez concluido el chequeo se deben estudiar los resultados. Si los resultados son satisfactorios se implantará la mejora de forma definitiva, y si no lo son habrá que decidir si realizar cambios para ajustar los resultados o si desecharla en un paso siguiente.

3.5. Modelo de seguridad de la información

3.5.1. Representación de las etapas de ejecución

En líneas siguientes se esclarece las etapas de procedimiento del modelo de ejecución, mediante una descripción detallada de cada una de las cinco (5) etapas que lo incluyen.

- Etapas de funcionamiento del modelo de ejecución: dichas etapas poseen objetivos, metas y herramientas que permiten que la seguridad de la información sea un sistema de gestión sostenible dentro de las organizaciones.

En la figura 3.1 se indican las etapas del modelo propuesto de SGSI planteada, se puede observar de forma más clara las etapas de la solución:

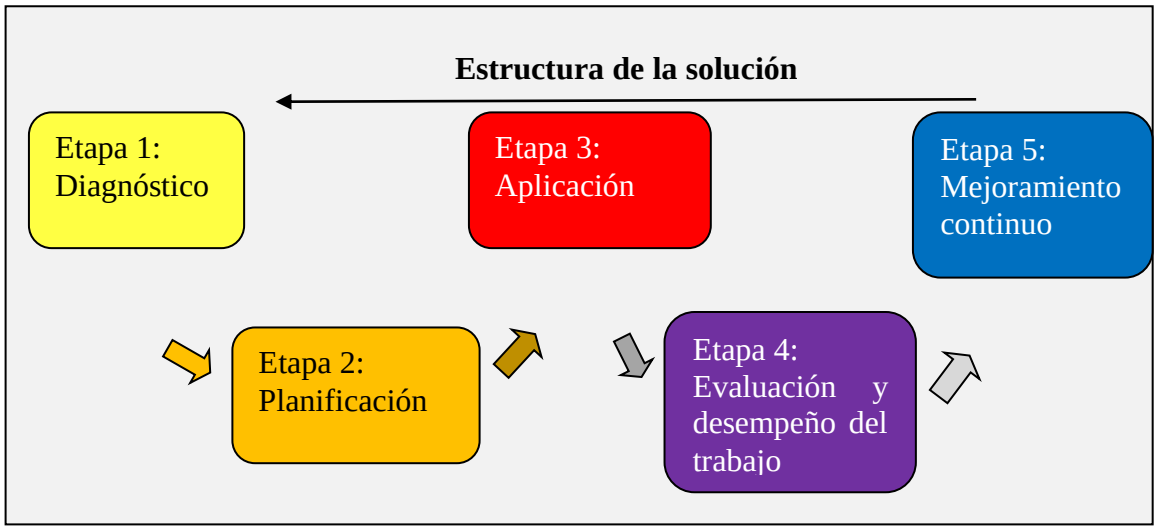


Figura 3.1 Etapas del sistema gestión de seguridad de la información

Fuente: Elaboración propia

3.5.2. Etapa 01 – de diagnóstico

A través de esta etapa 01 es imprescindible que las organizaciones identifiquen el estado actual, en el marco de los requerimientos del modelo de SGSI de la información. Asegurando la privacidad sobre todo las etapas que tiene el modelo SGSI. A continuación, se desglosa la etapa 01 que es el de diagnóstico, el cual vemos desarrollada en la figura 3.2.

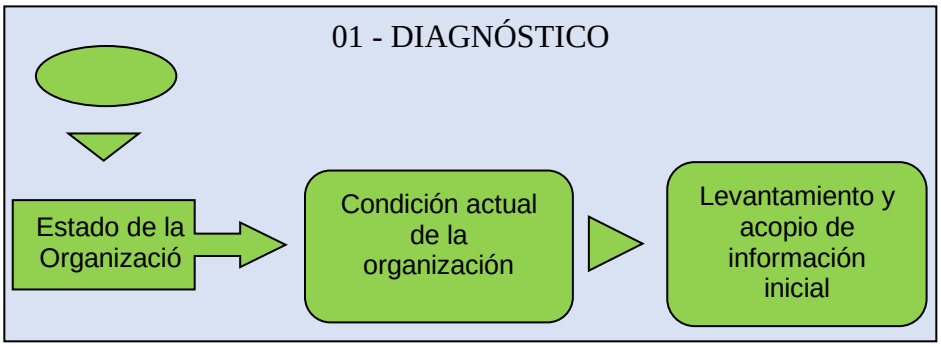


Figura 3.2 Etapa de Diagnóstico

Fuente: Elaboración propia

En la tabla 3.1 describimos los siguientes objetivos, resultados además de herramientas

Objetivos	Resultados	Herramientas
Determinar la situación actual de la organización	Gestión de la herramienta	Material de Diagnóstico
Identificar los puntos vulnerables que sirvan como elemento para la fase 02 de planificación	Documento con el resultado de los hallazgos encontrados en las pruebas de vulnerabilidad	Material de Diagnóstico

Tabla 3.1 – Objetivos, resultados y material de la etapa de diagnóstico

Fuente: NB/ISO/IEC 27001:2013

A través de esta etapa se pretende lograr los siguientes objetivos:

a) Establecer la etapa inicial de la gestión de la información dentro de la organización.

b) Reconocer el avance de la ejecución del periodo de operación dentro de la organización.

c) Reconocer el nivel de acatamiento con la reglamentación vigente relacionada con protección de datos personales.

d) Reconocimiento del uso de buenas prácticas en seguridad informática.

Para lo cual se encarga manejar los siguientes pasos:

- Reunión inicial
- Solicitud y Acopio de información.
- Programación de entrevistas
- Identificar las secciones

} REGISTRO DE INFORMACIÓN

- Pruebas administrativas
- Pruebas técnicas
- Análisis ciclo PHVA

} PRUEBAS

- Identificación de brechas
- Recomendaciones para subsanar los riesgos
- Elaboración de informes

} INFORMES

Para ejecutar la fase mencionada los encargados de aplicar el modelo deben realizar la recopilación de la información con la ayuda de los tres puntos mencionados líneas arriba.

Incluida la: revisión de manuales de función, políticas de la organización, bitácoras,

organigrama, inventario de activos.

Identificación de amenazas o evaluación del riesgo tanto en el personal, infraestructura y los procesos.

- Clasificar los activos de la organización.
- Elaborar una lista de amenazas emergentes.

Obteniendo documentación, listas y riesgos en el data center, a la vez de observar detalladamente todos los activos físicos, su entorno y el perímetro del data center.

- Realización de informes y las recomendaciones: una vez concluida la investigación preliminar y ya con el resultado de la descripción inicial y se efectúa al desarrollo de la etapa 02 que es la planificación.

3.5.3. Etapa 02 - de planificación

Seguidamente se tiene la etapa 02 – de Planificación en donde se debe delinear la táctica con el objetivo de coordinar el trabajo anticipado por la organización, partiendo de los resultados recolectadas en la etapa 01 de diagnóstico, para proceder a realizar el plan de seguridad de la información y aproximar a un grado de realización conveniente para proteger la información reservada compatible dar una respuesta a los desafíos de disponibilidad a la información.

El campo de aplicación del SGSI otorga a la organización definir los alcances sobre las cuales se pondrá en práctica la seguridad en la organización. Este centro de atención es por procesos y debe ampliarse al marco de la organización.

Teniendo en cuenta las siguientes sugerencias que vemos en la figura 3.3 se desarrolla la etapa de planificación[7]

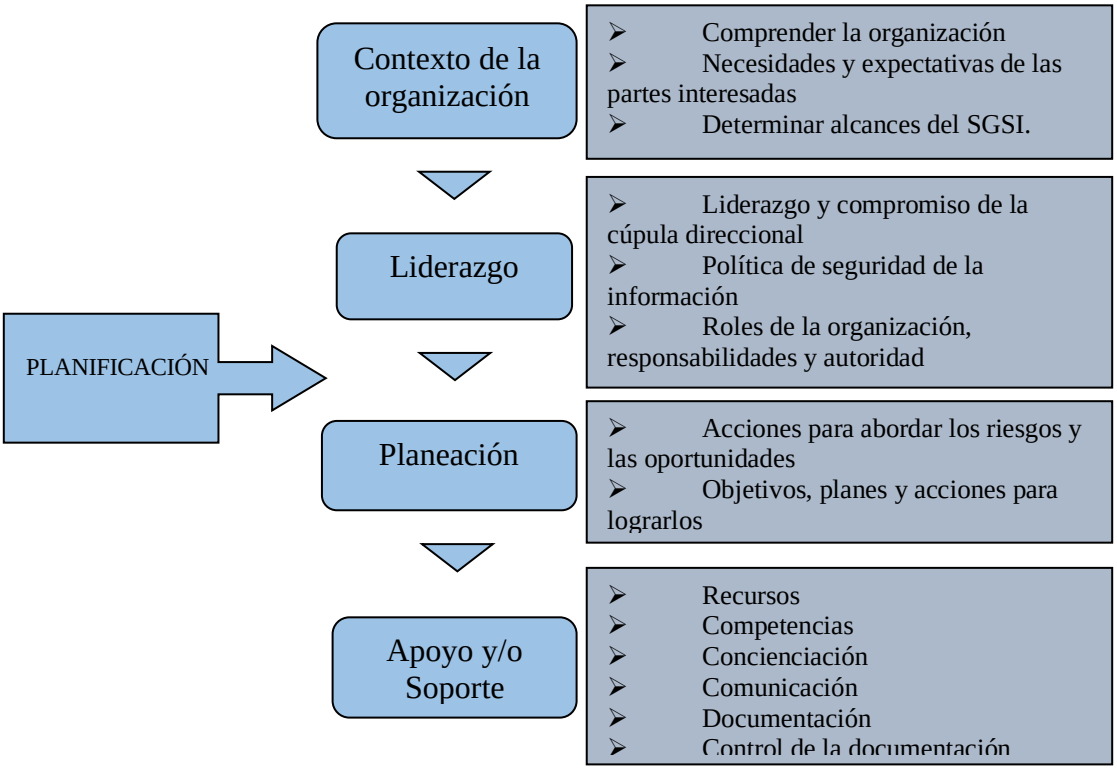


Figura 3.3 Etapa de Planificación[7]

Fuente: Elaboración propia

A continuación, detallamos los objetivos, resultados y herramientas de la etapa planificación en la Tabla 3.2. Seguidamente, se explica de manera general la fase 02 de planificación del modelo de SGSI.

[7] El contenido de la figura 3.3 fue tomada de la norma ISO IEC 27001 Capítulos 4, 5, 6, 7, que permite orientar cómo se desarrolla la planificación del SGSI.

Objetivos	Resultados	Herramientas
Políticas de la seguridad de la información	La alta cúpula directiva emite un documento con la política de seguridad de la información, debidamente facultado y socializada en la propia organización y a las partes externas relacionadas. Guía o Manual con las políticas de seguridad de la información, debidamente homologadas por la alta cúpula de la dirección y socializadas al interior de la organización.	Política General SGSI
Medidas o procedimientos de seguridad de la información	Medidas o procedimientos, de forma adecuada documentados, socializados y homologados por la junta directiva que incorpore los sistemas de ejecución institucional	Políticas
Roles y responsabilidades de la seguridad de la información	Las responsabilidades en su conjunto deben designarse quien será responsable de la seguridad de la información al interior de la organización.	Políticas
Inventario de activos de información	Responsabilidad sobre los activos Clasificación de la información	Gestión de activos
Integración de SGSI con el sistema de gestión documental	Integración del SGSI, con el sistema de gestión documental	Políticas

	de la institución	
Identificación, valoración y tratamiento de riesgo	Documento con la metodología de gestión de riesgos. Documento con el análisis y evaluación de riesgos. Documento con el plan de tratamiento de riesgos. Documento con la declaración de aplicabilidad. Documentos revisados y aprobados por la alta cúpula directiva.	Políticas
Plan de comunicaciones	Documento con el plan de comunicación, sensibilización y capacitación para la organización.	Políticas

Tabla 3.2 Objetivos, resultados e instrumentos de la etapa 02 - Planificación.

Fuente: NB/ISO/IEC 27001:2013

- Política de seguridad de la información: a continuación, se tiene la siguiente guía para la elaboración de la política general.

La Política del SGSI que representa la posición de la dirección de la organización con respecto a la protección de los activos siguientes:

- Los funcionarios
- Contratistas
- terceros
- La información
- La información
- los procesos
- Las tecnologías de información Hardware y software

La organización para tener control estratégico, establece lineamientos compatibles y objetivos como ser:

- Cumplir con los estándares de seguridad de la información

- Dar fuerza a la socialización de la cultura de seguridad de la información en el personal y clientes si fuese necesario.
- Disminuir el riesgo de los procesos
- Establecer las políticas
- Implementar el SGSI
- Proteger los activos de información

Estas políticas tienen un alcance y aplicabilidad a toda la organización, personal, clientes y terceros.

En la organización debe existir un nivel de cumplimiento del 100% de la política emanada por la alta cúpula de la directiva.

Como base se establece una decena de políticas de seguridad del SGSI de la organización

1. La organización a través de la dirección ha decidido definir, implementar, operar y mejorar de forma continua un SGSI.
2. Las responsabilidades serán definidas, compartidas, publicadas y aceptadas por cada uno del personal.
3. La organización protegerá la información generada, procesada o resguardada por los procesos al interior de la organización y así mismo los activos.
4. La organización protegerá la información creada, procesada, transmitida o resguardada por sus procesos, con el único motivo de disminuir riesgos.
5. La organización protegerá su información de las amenazas por parte del personal.

6. La organización protegerá las instalaciones de Tic.
7. La organización controlara la operación de sus procesos garantizando la seguridad de los recursos tecnológicos.
8. La organización implementara controles de acceso a la información, sistemas.
9. La organización tendrá la disponibilidad de sus procesos y la continuidad de manera lo más segura posible.
10. La organización controlara el cumplimiento de las políticas descritas anteriormente.

- **Gestión de Activos**: se indica al personal los límites y procedimientos, las políticas con referencia a la gestión de activos debe ver como mínimo:
  - Identificación de activos.
  - Clasificación de activos.
  - Etiquetado de la información.
  - Devolución de los activos
  - Dispositivos móviles

Control de acceso

- Control de acceso con usuario y contraseña
- Gestión de contraseñas
- Perímetro de seguridad
- No repudio: la política de no repudio con el fin de que los usuarios eviten haber realizado alguna acción.
- Privacidad y confidencialidad: esta política debe contener una descripción de la privacidad y confidencialidad del tratamiento y protección de datos

personales.

- Integridad: se refiere al manejo integro e integral de la información tanto interna como externa, la cual es aceptada por los funcionarios y terceros de la organización.

En consecuencia, toda información verbal, física o electrónica, debe ser procesada y entregada o transmitida integralmente, coherentemente, exclusivamente a las personas correspondientes, sin ninguna modificación o alteración, o en su defecto si fuere autorizada por los responsables de dicha información.

- Disponibilidad del servicio e información: la organización deberá contener con un plan de continuidad del proceso. Ante evento de un incidente.
- Gestión de incidentes: la organización deberá documentar una gestión general de gestión de eventos, incidentes y vulnerabilidades. La cual debe ser cumplida por todos los usuarios que tienen acceso autorizado a cualquier sistema de información.
- Capacitación: deben existir continuas capacitaciones, con el objeto de disminuir las vulnerabilidades y amenazas relacionadas con el personal. Con los siguientes parámetros:
- Contener políticas adicionales relacionadas directamente con el debido comportamiento de los usuarios como las que sigue a continuación: política de escritorio limpio, política de uso aceptable y ética
- Definir los roles y responsabilidades de quienes diseñarán los programas, quienes lo comunicarán.
- La cúpula deberá comprometerse a destinar los recursos suficientes.

- A quien va destinado el entrenamiento, a quienes serán sensibilizados.

La política de seguridad de la información está contenida en un documento de alto nivel para apoyar la implementación del modelo SGSI. La Política debe contener una declaración general por parte de la administración, donde se especifique sus objetivos, alcance, nivel de cumplimiento. La política debe ser aprobada y divulgada al interior de la organización.

3.5.4. Etapa 003 - de aplicación

Esta etapa le facilitara a la organización, llevar acabo la implantación de la aplicación efectuada en la etapa anterior del SGSI.

Desglosando esta etapa se tiene la figura 3.4

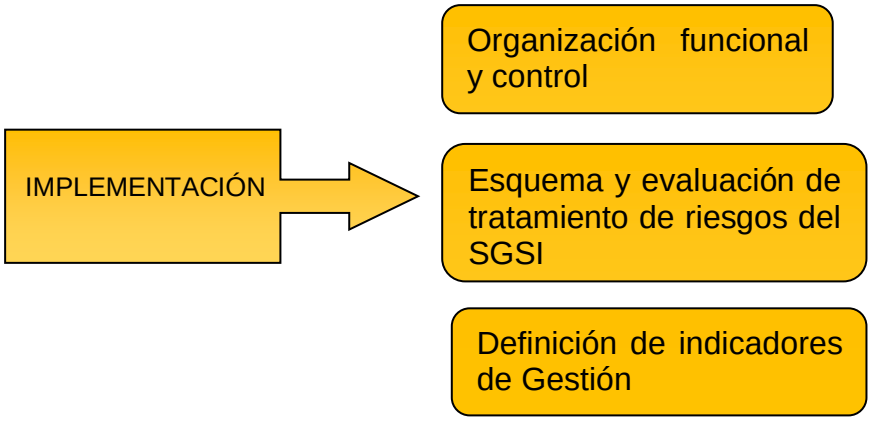


Figura 3.4 Etapa de Implementación[8]

Fuente: Elaboración propia

[8] El contenido de la figura 3.4 fue tomado de la NB/ISO/27001:2013 capitulo 8 que permite orientar como se desarrolla la implementación del SGSI.

A continuación, en la Tabla 3.3 describimos los objetivos, resultados como las herramientas de la etapa de planificación.

Objetivos	Resultados	Herramientas
Implantación del plan de tratamiento de riesgos	Informe de la ejecución del plan de tratamiento de riesgos	Documento con la declaración de aplicabilidad. Documento con el plan de tratamiento de riesgos
Indicadores de gestión	Documento con la descripción de los indicadores de gestión de seguridad de la información SI	Indicadores de gestión

Tabla 3.3 Objetivos, resultados e instrumentos de la Etapa de planificación

Fuente: NB/ISO/IEC 27001:2013

Con los resultados de las etapas anteriores, deberá ejecutarse las siguientes actividades.

- Planificación y control de las acciones operacionales: la organización debe seguir una planificación, luego implementar para finamente controlar los trámites necesarios para cumplir con los requisitos de seguridad de la información que permitan aplicar las participaciones determinadas en el plan de tratamiento de riesgos.

La organización debe tener información documentada en el grado necesario para tener la fiabilidad en que los trámites se han llevado a cabo según lo programado, por otra parte, deberá llevarse una supervisión de modificaciones que le permitan llevar participaciones o

acciones para paliar efectos contrarios cuando sea esencial.

- Poner en práctica el plan de tratamiento de riesgos: se debe poner en práctica el plan de tratamiento de riesgos de seguridad de la información, en el cual se reconoce la supervisión a aplicar para llevar cada uno de las amenazas a un nivel aceptable para la organización, en donde el cimiento para ejecutar esta actividad es la guía de controles de seguridad del SGSI.

Es claro tener presente que la aplicación del control sobre los riesgos detectados debe estar homologado por el dueño de cada trámite.

- Indicadores de Gestión: la organización deberá establecer señales que le permitan cuantificar la efectividad, la eficiencia y la eficacia en la gestión y las acciones implementadas en seguridad de la información.

Los indicadores buscan medir:

- Efectividad en los controles.
- Eficiencia del SGSI al interior de la organización.
- Proveer estados de seguridad que sirvan de guía en las revisiones y la mejora continua.
- Comunicar valores de seguridad al interior de la entidad.
- Servir como insumos al plan de control operacional.
- Indicadores de gestión: se crea con el fin de la medición de efectividad, eficiencia y eficacia, indicadores que servirán como ingrediente para la mejora continua. Cuyos objetivos son:

- Evaluar la efectividad de la implementación de los controles.
- Evaluar el modelo de SGSI al interior de la organización, en su eficiencia.

Brinda información relacionada para poder llevar a cabo la realización de esta entidad.

3.5.5. Etapa 04 - Evaluación de desempeño del trabajo

La gestión de continuación y control del SGSI se realiza con fundamento a las conclusiones que arrojan los referentes de la seguridad de la información planteados para comprobación de la efectividad, la eficiencia y la eficacia de las participaciones ejecutadas. Como veremos en la figura 3.5

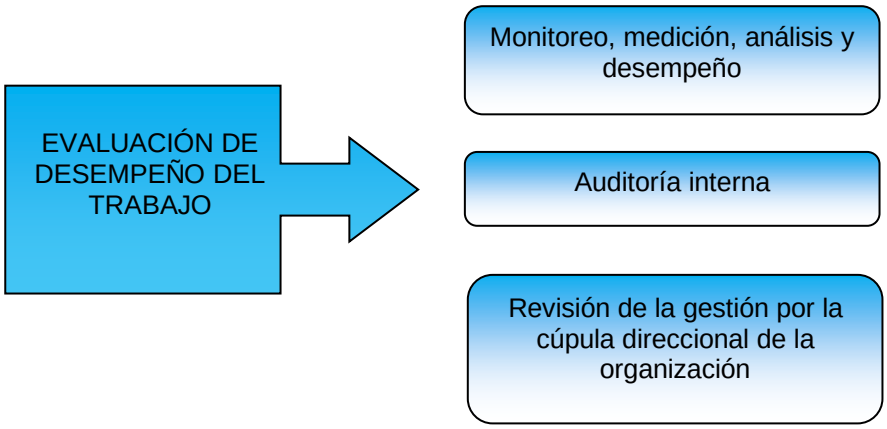


Figura 3.5 Evaluación de desempeño del trabajo[9]

Fuente: Elaboración Propia

A continuación, describimos la Tabla 3.4 de evaluación de desempeño del trabajo.

[9] El contenido de la figura 3.5 fue tomada de la norma NB/ISO/IEC 27001 Capítulo 09, que permite orientar cómo se desarrolla la evaluación del SGSI.

OBJETIVOS	RESULTADOS	Herramientas
Formulario de verificación y monitoreo a la implementación del SGSI	Informe con el plan de seguimiento y revisión del SGSI verificado y aprobado por la cúpula de la dirección.	Evaluación del desempeño del trabajo
Plan de ejecución de auditorias	Informe con el plan de implementación de auditorías y verificaciones autónomas al SGSI, revisado y autorizado por la cúpula de la dirección.	Políticas

Tabla 3.4 Objetivos, Resultados e instrumentos de la etapa de evaluación de desempeño.

Fuente: NB/ISO/IEC 27001:2013

Programa de verificación y monitoreo a la implementación del SGSI

En esta operación la organización necesita elaborar un programa que incluya las siguientes tareas:

- Revisión de los controles establecidos.
- Revisión de la evaluación de los niveles de riesgo.
- Seguimiento al alcance y a la implementación del SGSI.
- Medición de los indicadores de gestión del SGSI.

Este programa tendrá que autorizar el afianzamiento de indicadores de forma regular y su diagnóstico de cara a los objetivos esperados: los cuales tienen que ser evaluados facultando ser analizados los orígenes de la variante y su colisión en la ejecución de las metas y objetivos del SGSI.

- Evaluación del desempeño: ofrece información vinculada con el fin de realizar esta actividad.

3.5.6. Etapa 005 - de mejoramiento continuo

En esta etapa la organización tiene que afianzar los resultados logrados de la etapa de evaluación de desempeño, para delinear el programa de mejora continua de seguridad de la información, realizando los movimientos debidos para aminorar los puntos débiles detectadas.

Detallamos en la figura 3.6 la mejora continua

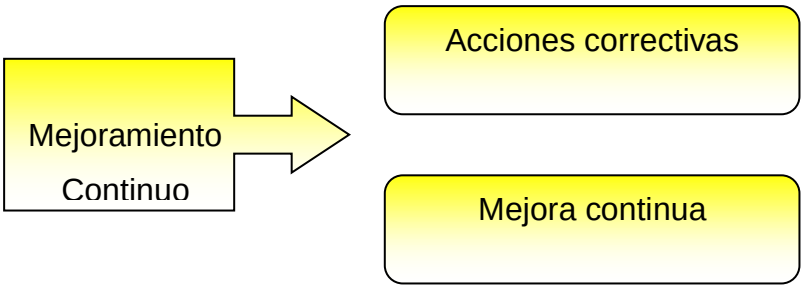


Figura 3.6 Etapa de Mejoramiento Continuo[10]

Fuente: Elaboración propia

En esta etapa es fundamental que la organización lleve a cabo el programa de mejora continua con cimiento en las conclusiones de la etapa de evaluación del desempeño.

A continuación, detallamos en la Tabla 3.5 la etapa Mejora continua.

[10] El contenido de la figura 3.6 fue tomada de la NB/ISO/IEC 27001:2013 Capitulo 10, que permite orientar cómo se desarrolla la fase de mejoramiento continuo del SGSI

Mejora continua		
Objetivos	Resultados	Herramientas
Programa de mejora continua	Informe con el programa de mejoramiento. Informe con el programa de comunicación de resultados.	Resultados de la ejecución del programa de revisión y seguimiento, a la implementación del SGSI

Tabla 3.5 Objetivos, resultados y herramientas de la etapa de mejora continua.

Fuente: NB/ISO/IEC 27001:2013

Este programa incluye:

- Productos o resultados de la ejecución del plan de seguimiento, evaluación y análisis para el SGSI.
- Productos o resultados del plan de ejecución de auditorías y revisiones independientes al SGSI.

Empleando los datos anteriores, la organización puede lograr las regulaciones a los entregables, controles y procedimientos dentro del SGSI. Estos datos tendrán como producto un programa de mejoramiento y un programa de notificaciones de mejora continua, verificados y aceptados por la alta dirección de la organización. La verificación por la alta dirección hace referencia a las decisiones, cambios, prioridades etc. tomadas en sus comités y que impacten el SGSI

- Mejora continua: le permitirá a la organización en base a los resultados de la

etapa de gestión, corregir los errores, así como mejorar los pasos ejecutados en las anteriores etapas.

- No conformidades: en el hecho de existir no conformidades, la organización deberá realizar los pasos necesarios para controlar y corregir debidamente y evitar que se vuelva a mostrar.
- Tomar las acciones necesarias en la implementación
- Verificar la efectividad de lo realizado en cuanto a las acciones correctivas tomadas.
- Tomar acciones necesarias en el sistema al realizar los cambios.
- La organización documentará estas nuevas correcciones de la forma: se tomará nota de las no conformidades y las soluciones nuevas realizadas.
- Mejora continua: es evidente que el SGSI es un ciclo por lo que deberá estar continuamente revisada por la organización. Se comunicará de las mejoras al personal correspondiente.

CAPITULO IV

Conclusiones y recomendaciones

4.1. Conclusiones

Es de vital importancia para la ejecución de un proyecto, establecer un plan de trabajo y dar cumplimiento a las actividades propuestas acorde al cronograma planteado.

La declaración de aplicabilidad permite a una organización establecer un nivel de cumplimiento respecto de a las normas NB/ISO/IEC 27001:2013, a partir de esto establecer controles que le permiten mejorar su SGSI, proteger los datos de la organización.

Definir un cuadro de riesgos y/o vulnerabilidades permitirá a la organización disminuir los riesgos relacionados al no cumplimiento y brindar una mayor protección de la información, con base en los procedimientos y controles que establezca para este fin.

Es importante implementar en cualquier organización normas y políticas, ya que es importante acoplar los procesos, recursos e información con las estrategias y objetivos de la organización con el fin de maximizar beneficios, capitalizar oportunidades y ventajas competitivas.

Las organizaciones deben comprender que la seguridad ya no es un lujo, sino que es una necesidad y prioridad en estos tiempos, para proteger el bien activo y más valioso de ella, los datos. La seguridad informática para las organizaciones y personas, se ha convertido en una necesidad de todas las organizaciones hoy en día, ya que una amenaza recibida afecta en la imagen, como primera instancia, por lo que se reconoce como fundamental contar con un sistema de protección para la información.

La organización debe realizar auditorías internas como una de las actividades fundamentales dentro del proceso de retroalimentación o feed back y control de todo sistema para obtener información sobre el funcionamiento del SGSI.

La organización en coordinación con el área de gestión de RRHH debe realizar constantes charlas para exponer los riesgos de la seguridad informática a los empleados, describiendo los daños que causan los ataques y la forma en la que ingresan al sistema y con ello lograr concientizar a las personas para lograr disminuir los riesgos y vulnerabilidades detectándolos y previniéndolos.

A través de un SGSI, la organización integra e institucionaliza buena planificación y organización, adquisición e implantación, entrega de servicios, soporte y monitorización del rendimiento de TI relacionadas para soportar los objetivos de la organización.

4.2. Recomendaciones

Es necesario promover por parte de la organización la importancia del valor de seguridad de la información al interior de la organización. Realizar un esfuerzo y compromiso continuo por parte de la organización para inculcar en todos los funcionarios la apropiación y el cumplimiento de las políticas de seguridad de información permitiendo mantener la organización con mejoras. Gestionar adecuadamente y con más frecuencia las actividades y controles de seguridad de información, posibilitara implantar varios sistemas de gestión para mejorar y beneficiar la organización bajo los parámetros establecidos por los estándares nacionales e internacionales.

Referencias bibliográficas

Aguirre Mollehuanca, D. A. Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú S.A(Tesis de grado). Pontificia Universidad Católica del Perú, Lima Perú.

Aliaga Flores, L (2013). Diseño de un sistema de gestión de seguridad de información para un instituto educativo- Tesis para optar por el título de Ingeniero informático, que presenta el bachiller. Lima: Pontificia Universidad Católica del Perú. Facultad de ciencias e ingeniería

Aracil Javier.1995 Dinámica de sistemas, Madrid.

Ludwing von, Bertalanffy,1986. teoría general de sistemas. New York: George Brasilier

Chiavenato Diaz S.,2006. Introducción a la teoría general de la administración. México: McGraw-Hill interamericana.

Ferrel, O. C., H. (2004). Introducción a los negocios en un mundo Cambiante. Cuarta Edición. México: McGraw-Hill Interamericana Editores.

James Rumbaugh,Michael Blaha, William Premerlani, Frederick Eddy y William Lorensen Modelado y diseño orientado a objetos 1996 Prentice Hill

López, 2013. Análisis de las posibilidades de uso de Big Data en las organizaciones (Master in

Business and Information Technology), Universidad de Cantabria, Cantabria – España.

Martínez, J. Estrategias metodológicas y técnicas para la investigación social. México D.F.: Universidad Mesoamericana

Piattini, Mario G, Del Peso Emilio, Auditoria Informática Alfaomega RaMa 2da edición

Purificación Aguilera, Seguridad Informática, 1ra ed. Editex, Tipos de Seguridad, 2010, pp. 9.

Metodología de la investigación Hernández Sampieri Roberto, Fernández Collado Carlos, Baptista Lucio Pilar, 6ª Edición, Mc Graw Hill.

Pablo de I. (1989) El reto informático, (La gestión de la información en la empresa) Ediciones Pirámide, Madrid.

(Sommerville, 2005) Sommerville Ian, (2005). Ingeniería de software. Séptima versión. Madrid. T-3408

Viktor Schönberger. (2013). Big data: La revolución de los datos masivos Traducción: Antonio J. Iriarte. España. Editorial: Turner.

Referencias Web

Aguilera, P. Seguridad Informática, 1ra ed. Editex, Tipos de Seguridad. Obtenido de: https://books.google.es/books?hl=es&lr=&id=Mgvm3AYIT64C&oi=fnd&pg=PA1&dq=seguridad+f%C3%ADsica+y+l%C3%B3gica&ots=PqorVAEIX2&sig=QJ7pSJuDM

IezfFlxy-Vm9i7sgrw#v=onepage&q=seguridad%20f%C3%ADsica%20y%20l%C3%B3gica&f=false

Agustin, L. N., & Javier, L. S. ISO27000. Es el portal de 27001 en español. Obtenido de: http://www.iso27000.es/sgsi.html

Agustin, L. N., & Javier, L. S. ISO27002. Es el portal de 27002 en español. Obtenido de:http://www.iso27000.es/iso27002.html

Baca,Gabriel Introducción a la seguridad informática Obtenido de: https://books.google.es/books?hl=es&lr=&id=IhUhDgAAQBAJ&oi=fnd&pg=PP1&dq=seguridad+inform%C3%A1tica+en+las+empresas&ots=0WPC8zvjKt&sig=2jS-zeLOskKD3z89u7jBy8lGLOY#v=onepage&q=seguridad%20inform%C3%A1tica%20en%20las%20empresas&f=false

BICSI,2018. Obtenido de: https://www.bicsi.org/standards/bicsi-standards/available-standards-store/single-purchase/ansi-bicsi-002-2014

Ceupe, 2018. Obtenido de: https://www.ceupe.com/blog/infraestructura-tecnologica.html 24-abril-2019 hrs.16:00

Ciclo Deming. Obtenido de: https://www.pdcahome.com/5202/ciclo-pdca/

Cofitel, 2014. Obtenido de: https://www.c3comunicaciones.es/data-center-el-estandar-tia-942/

Cofitel, 2014. Para actualizaciones Obtenido de:

https://www.c3comunicaciones.es/productos/soluciones-para-data-center/

Conceptodefinición.de. Obtenido de: https://conceptodefinicion.de/informacion/

[Pichardo, J,2017] Obtenido de: https://www.academia.edu/8970272/Controles_Fisicos_SI

GOMEZ, VIEITES Alvaro,2017 ED RA-MA Enciclopedia de la seguridad informática

obtenido de:

https:/books.google.es/books?hl=es&lr=&id=Bq8-DwAAQBAJ&oi=fnd&pg=PT2&dq=seguridad+inform%C3%A1tica&ots=dwpa1e2idE&sig=AZ_T-VHwXZsObg2pq_LeCGicsV0#v=onepage&q=seguridad%20inform%C3%A1tica&f=false

ICREA. International Computer Room Experts Association ICREA Obtenido de:

http://www.icrea-international.org/nuevoPortal/publicaciones.asp#block1

[Incibe,2019]. Obtenido el 2019 de: may https://www.incibe.es/protege-tu-

empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

Ponemon Institute (2016). Flipping the Economics of Attacks. Obtenido el 2019 de:

https://www.polyscope.ch/site/assets/files/42688/06_16_53.pdf

Power Data, 2019. Obtenido de https://www.powerdata.es/data-warehouse

[Data Architectur] obtenido de: https://www.techopedia.com/definition/6730/data-architecture

Norma ISO27000. Obtenido de: www.27000.org/iso-27002.htm-

Norma ISO27001. Obtenido de: http://iso27000.es/iso27000.html

PACIO,2014. Data center hoy. Obtenido de:

https://books.google.com.bo/books?hl=es&lr=&id=43xNDAAAQBAJ&oi=fnd&pg=PT17&dq=data+center+libros&ots=yGHV0QoPhJ&sig=aS-mymRnIl9sdNE8ZB1aNDYygC0#v=onepage&q=data%20center%20libros&f=false

PowerData,2016. Obtenido de: https://blog.powerdata.es/el-valor-de-la-gestion-de-

datos/seguridad-de-los-datos

- [Schönberg Víctor]. obtenido de:

https://blog.powerdata.es/el-valor-de-la-gestion-de-datos/topic/data-quality

Sergio Tornati, 2015. Obtenido de:

https://medium.com/data-management-en-espa%C3%B1ol/que-es-data-management-e3e625ac974a

VELASCO, JIMENEZ, CHAFLA,2016 Análisis de los mecanismos de encriptación para la

seguridad de la información en redes de comunicaciones. Obtenido de: http://revistasdigitales.upec.edu.ec/index.php/sathiri/article/view/38/92

Techopedia,2018 obtenido de: https://www.techopedia.com/definition/6730/data-architecture

De Pablos, Lopez, Medina, 2006 Obtenido de :

https://books.google.es/books?hl=es&lr=&id=U0MXWtqjxtsC&oi=fnd&pg=PA9&dq=inform%C3%A1tica+basica&ots=D8goEP2v8z&sig=HQOMzQLSev7t0Lew_eQzYJHtFSs#v=onepage&q=inform%C3%A1tica%20basica&f=false

Magerit obtenido de:

https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XOaun4hKi00

Romero, J.2019 Control interno según COSO. Obtenido de

https://www.gestiopolis.com/control-interno-segun-coso/

Saavedra, A. 2018. Obtenido de:

https://www.clavei.es/blog/que-es-la-infraestructura-it/

Wolff, C. G., Ago 2002. La tecnología datawarehousing. Ingenieria Informatica: La revista electrónica del DIICC. Obtenido de: http://www.inf.udec.cl/revista/ediciones/edicion3/cwolf.PDF

[ICREA] Obtenido de:

http://www.icrea-international.org/nuevoPortal/publicaciones.asp#block1

[YARLEQUE 2018] Obtenido de:

https://repositorio.une.edu.pe/bitstream/handle/UNE/3109/MONOGRAF%c3%8dA%20-%20YARLEQUE%20FERRER.pdf?sequence=1&isAllowed=y

ANEXO

SISTEMA DE SEGURIDAD DE INFORMACION INSTITUCIONAL

Encuesta de Seguridad de información

Indique la relación que tiene con la organización

Directivo ☐ Administrativo ☐ Consultor/Docente ☐

Función que cumple en la Organización: ……

Responda cada una de las secciones teniendo en cuenta la información conocida por Usted marcando con una X sobre la casilla. Tenga en cuenta que las preguntas son de respuesta única.

SECCION: POLÍTICAS DE SEGURIDAD

¿En la organización existe un documento que contenga las políticas de la seguridad de la información?

1. No existe ☐
2. Si existe, pero no está aprobado, no está publicado y por tanto no es conocido por todo el personal ☐
3. Si existe, está aprobado por la dirección de la organización, es de obligatorio cumplimiento, pero no está publicado y por tanto no es conocido por todo el personal. ☐
4. Si existe, está aprobado por la dirección de la organización, es de obligatorio cumplimiento, está publicado y es conocida por el personal. ☐
5. No tiene conocimiento. ☐

SECCION: ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION

¿Los siguientes aspectos de la gestión de la seguridad de la información están contemplados en la organización?

1. Existe una estructura interna apoyada desde la dirección que gestiona a la seguridad. ☐
2. En dicha estructura están involucradas las diferentes jerarquías de la organización (usuarios, administradores, diseñadores de aplicaciones, gestores, etc.…) ☐
3. Están definidas las responsabilidades y pautas en cuanto a la protección de los activos. ☐
4. Están contemplados y establecidos procesos de autorización para los nuevos recursos de tratamiento de la información. ☐

5. Están contemplados y establecidos planes de revisión de cambios ☐
6. Ninguna de las anteriores ☐

¿Se establecen acuerdos de no divulgación y confidencialidad relacionados con el acceso e intercambio de información en la institución?

1. No ☐
2. Sí, solo para el personal interno ☐
3. Sí, solo para los contratistas ☐
4. Sí, tanto para personal interno como para contratistas ☐

SECCION: GESTION DE ACTIVOS

¿La organización gestiona los activos (hardware, software, documentación, etc.)?

1. No ☐
2. La organización dispone de un inventario parcial de activos ☐
3. La organización dispone de un inventario completo y actualizado de los activos ☐
4. Además de lo anterior tiene delimitadas las responsabilidades respecto a su gestión. ☐
5. Además de lo anterior están delimitadas las responsabilidades respecto a su gestión y existen directrices claras, escritas y publicas sobre el uso correcto y seguro de los mismos. ☐

¿Están clasificados los activos (según su grado de sensibilidad y criticidad) de la institución?

1. No ☐
2. Sí, pero de forma parcial ☐
3. Sí, los activos están clasificados ☐
4. Sí, además de lo anterior están etiquetados y existen normas claras para manejarlos. ☐

SECCION: SEGURIDAD FISICA Y AMBIENTAL

Respecto a la seguridad física y ambiental - ¿Las infraestructuras TIC criticas o con información sensible están ubicadas en tornos protegidos y con controles de acceso?

1. Sí, se encuentran en locales aislados ☐
2. Sí, los locales están especialmente preparados contra daños externos (electricidad, fuego, agua, sabotajes, etc.…) ☐
3. Sí, existe control de acceso para el personal autorizado ☐
4. Sí, existen directrices claras para visitar ☐
5. Ninguna de las anteriores ☐
6. Todas las anteriores a excepción de la 5 ☐

¿El equipamiento por el que circula información sensible se encuentra protegido contra robo, perdida, daños, compromiso de la información o interrupción de servicio?

1. Sí, el equipamiento se encuentra en locales protegidos ☐
2. Sí, el equipamiento está preparado para trabajar en caso de otras anomalías externas (cortes de agua, inundación, etc. ...) ☐
3. Sí, las instalaciones de cableado eléctrico y de datos son independientes, están protegidas y existe más de una ruta física. ☐
4. Ninguna de las anteriores ☐
5. Todas las anteriores ☐

SECCION: GESTIÓN DE COMUNICACIONES Y OPERACIONES

¿Existen procedimientos documentados relativos a los procesos de operación de los equipos y del tratamiento de la información?

1. No existe ☐
2. Existen algunos procedimientos, para algunos equipos y sistemas de información ☐
3. Sí, está todo con procedimientos ☐
4. Además de lo anterior, se dispone de un sistema de revisión y de estos procedimientos, ☐

con un responsable para autorizar estas revisiones, que incluye la evaluación que estos cambios pueden provocar en los sistemas. Los procedimientos están al alcance de todos los usuarios que los precisen.

¿Existe un procedimiento de gestión de cambios en los sistemas de información?

1. Se identifican y registran los cambios significativos ☐
2. Se realiza una planificación, una evaluación de impactos potenciales de seguridad y pruebas de los camios ☐
3. Existe un procedimiento de emergencia y respaldo ☐
4. Existe un procedimiento de comunicación de los cambios a las personas involucradas ☐
5. Ninguna de las anteriores ☐
6. Todas las anteriores ☐

¿Existe un procedimiento para la aceptación de nuevos sistemas, actualizaciones de aplicaciones, nuevas versiones de sistema operativo, cambio de hardware, etc. …?

1. No, simplemente se realizan algunas pruebas ☐
2. Sí, existe un procedimiento ☐
3. Sí, existe un procedimiento que tiene en cuenta planes de contingencia, efectos colaterales en otros sistemas y recuperación ante errores ☐
4. Además de lo anterior, los nuevos desarrollos y sistemas tienen en cuenta las pruebas de rendimiento, la formación de todos los involucrados y la documentación ☐

¿Contra el código malicioso, se toman medidas en la organización?

1. Todos los equipos de los usuarios cuentan antivirus y antimalware ☐
2. Además de lo anterior el correo electrónico cuenta con antivirus y antispam ☐
3. Además de lo anterior se ha establecido una gestión centralizada de los equipos de la organización para actualizaciones del sistema operativo y antivirus ☐
4. Además de los anteriores, se cuenta para la navegación web sistemas de protección ☐
5. Además, se cuenta con una política y mecanismos que determinan qué código móvil (javascripts, Activex, etc.) puede ser ejecutado ☐
6. Ninguna de las anteriores ☐

Respecto a las copias de seguridad:

1. No se realizan copias de seguridad ☐
2. Se realizan copias de seguridad de software y datos ☐
3. Además de lo anterior, existen procedimientos detallando el objeto de la copia de seguridad, periocidad y los procesos documentados de recuperación ☐
4. Además de lo anterior, las copias de seguridad y procedimientos se almacenan en locales distintos de donde están ubicados los sistemas de información ☐
5. Además de lo anterior, los procesos de restauración de copias de seguridad son probados regularmente para verificar su correcta aplicación y efectividad ☐

Respecto a los servicios de red de la institución

1. Se monitorizan todos los elementos de red ☐
2. Existen procedimientos para la conexión de equipos a la red ☐
3. Hay establecidas medidas para garantizar la confidencialidad e integridad de los datos cuando son transportados por redes inalámbricas y redes públicas ☐
4. Todos los servicios de red tienen un documento con las condiciones de uso y los niveles de servicio ☐
5. Existen procedimientos para restringir el acceso a servicios de red o aplicaciones cuando sea necesario ☐
6. Ninguna de las anteriores ☐
7. Todas las anteriores ☐

Sobre la gestión de medios extraíbles (CDs, DVDs, memorias flash, discos duros portátiles, etc.) y copias empresas:

1. Existe un procedimiento documentados que incluye instrucciones de almacenamiento, transporte y destrucción de los medios extraíbles utilizados ☐
2. Se almacenan en lugar seguro y protegido del fuego e inundaciones fuera del centro de proceso de datos ☐
3. Se lleva un inventario completo ☐

☐

4. Cuando llega el fin de su vida útil se destruyen físicamente

5. Ninguna de las anteriores ☐

6. Todas las anteriores ☐

¿Existe una política de protección de la información cuando se produce un intercambio electrónico de la misma?

1. No hay ninguna política de control ☐

2. Sí, para los accesos lógicos ☐

3. Sí, para los accesos lógicos y físicos ☐

4. Sí, y además está documentada ☐

5. Sí, y además de lo anterior se revisa y se hace un seguimiento de cumplimiento ☐

SECCIÓN: CONTROL DE ACCESO

¿Son los usuarios conscientes de la responsabilidad que tienen para que sean eficaces los controles de acceso, en particular con las contraseñas, equipos informáticos y el entorno de trabajo?

1. No, los usuarios no tienen responsabilidad sobre uso de las contraseñas, sus equipos informáticos o escritorios ☐

2. No, pero se aplican las medidas de bloqueo de los equipos informáticos desatendidos garantizando la calidad de las contraseñas ☐

3. Sí, además de lo anterior, a los usuarios se les informa expresamente sobre la forma de gestionar correctamente sus contraseñas, los equipos informáticos, sesiones desatendidas y el entorno de trabajo ☐

¿Existen procedimientos y medios para restringir adecuadamente el acceso a las aplicaciones y a la información contenida en ellas?

1. No ☐

2. Sólo medidas de autentificación, pero no se aplican perfiles de acceso ☐

3. Sí, los usuarios tienen restricciones según su perfil de acceso ☐

4. Sí, los usuarios tienen restricciones, alineadas con la política de control de acceso. Además, se controla que la información confidencial solo puede ser enviada a terminales autorizados ☐

5. Sí, y además de lo anterior, se aíslan tanto lógica como físicamente los sistemas que manejan información confidencial, quedando documentada explícitamente la sensibilidad de dicha información y aplicación ☐

Respecto a los dispositivos y comunicaciones móviles (celular, portátil, tablets, etc. …):

1. No existen políticas y procedimientos que regulen su uso ☐

2. Aunque no existen políticas, se aplican medidas técnicas que garantizan la privacidad de las comunicaciones, el control de acceso, la seguridad del equipo remoto (cortafuegos, antivirus), de sus datos (cifrado y backup), etc. ☐

3. Existe una política expresa donde se reflejan los requisitos de seguridad arriba indicados y se dan directrices de uso (seguridad física y otras precauciones) ☐

SECCION: ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION

¿Se identifican y documentan los requisitos de seguridad de los sistemas de información antes de su desarrollo y/o implantación?

1. No o no se hace sistemáticamente ☐

2. Sí, teniendo en cuenta la criticidad de los activos gestionados ☐

3. Además de lo anterior, se hace un seguimiento formal de cumplimiento de los requisitos ☐

¿Siendo la criptografía el método para volver ilegible la información, existe una política de uso de controles criptográficos en la entidad?

1. No ☐

2. Si ☐

3. Si y existe además un sistema de gestión de claves (creación, modificación, perdida, destrucción, etc.) que garantiza una correcta aplicación de los controles criptográficos ☐

SECCION: GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACION

Respecto a la gestión de incidentes de seguridad de la información:

1. Existen mecanismos conocidos por toda la institución, para la notificación de eventos de seguridad y puntos débiles ☐
2. Los responsables de la gestión de incidentes conocen y aplican, cuando es necesario, los protocolos para la recolección de evidencias con validez legal ☐
3. Ninguna de las anteriores ☐

SECCION: GESTION DE LA CONTINUIDAD DEL NEGOCIO

¿Se incluye la seguridad en los planes de continuidad de la actividad de la organización?

1. No ☐
2. Sí, se tienen en cuenta diversos aspectos de la seguridad como los activos implicados, el impacto de los incidentes de seguridad, etc. ☐
3. Sí, además hay planes de continuidad de la actividad para el caso en que ocurra un incidente ☐
4. Sí, además los planes se revisan y actualizan de forma periódica ☐

SECCION: CUMPLIMIENTO DE LOS REQUISITOS LEGALES

¿Se realizan auditorías a los sistemas de información sobre el cumplimiento de las políticas de seguridad?

1. No ☐
2. Si y de forma periódica ☐
3. Sí, lo hace una empresa externa especializada de forma periódica de acuerdo a unos procedimientos establecidos y se deja todo documentado ☐

Con cuál de las siguientes preguntas se identifica más:

¿Cuándo se levanta del puesto de trabajo, generalmente usted bloquea la sesión en su computador?

1. Siempre ☐
2. Algunas veces ☐
3. Frecuentemente ☐
4. Nunca ☐

¿Si a su bandeja de entrada de correo electrónico llegan correos con archivos adjuntos desconocidos usted descarga los archivos?

1. Siempre ☐
2. Algunas veces ☐
3. Frecuentemente ☐
4. Nunca

¿Si en su computador ve una alerta de virus como reaccionaria?

1. Ignora el mensaje ☐
2. Llama a un funcionario del Centro de informática y comunicaciones ☐
3. Consulta a un compañero de su área ☐
4. Ejecuta el antivirus ☐

¿Si percibe que hay fuga de información de la organización a través de compañeros que actitud asumiría?

1. Informa a su jefe ☐
2. Omite esta situación y continua su labor ☐
3. Informa a la oficina de Control Disciplinario ☐
4. Informa a la oficina de Control Interno ☐
5. No sabe que hacer ☐

¿Quién considera usted que es el responsable de mantener la seguridad de la información en la organización?

1. Del jefe de cada área ☐
2. Del área de tecnología ☐
3. De todos los funcionarios y contratistas ☐
4. Del responsable del proceso ☐

¿Qué es un activo de información?

1. Todos los datos recopilados por las Directivas de la Organización ☐
2. Cualquier cosa que tiene valor para la institución (Información, software, hardware, personas, intangibles) ☐
3. No sabe ☐

¿Un sistema de Gestión para la Seguridad de la Información (SGSI) está diseñado para?

1. Preservar la información ubicada en cada servidor ☐
2. Garantizar la disponibilidad de los activos de información ☐
3. Implementar controles de seguridad que protejan los activos de información que brinden confianza ☐
4. No sabe ☐