UNIVERSIDAD MAYOR DE SAN ANDRÉS

FACULTAD DE HUMANIDADES Y CIENCIAS DE LA EDUCACIÓN

CARRERA DE BIBLIOTECOLOGÍA Y CIENCIAS DE LA INFORMACIÓN

SEGURIDAD DE LA INFORMACIÓN EN LA PROTECCIÓN DE LOS DATOS PERSONALES EN LA FIRMA DIGITAL DE LA AGENCIA PARA EL DESARROLLO DE LA SOCIEDAD DE LA INFORMACIÓN EN BOLIVIA (ADSIB) 2017.

TESIS DE GRADO PARA OPTAR EL TÍTULO DE

LICENCIATURA

ESTUDIANTES:

JIMÉNEZ MANCILLA JOSÉ ANTONIO

ORELLANA HEREDIA DEYCI

TUTOR:

LIC. MARÍA ANA LORENA MARTÍNEZ QUINTEROS

LA PAZ – BOLIVIA

2018

Resumen

La presente investigación analiza la seguridad de la información y la protección de los datos personales en la firma digital implementados por la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB). Se aplicó la metodología cuantitativa, descriptiva y deductiva. Se analizó el comportamiento de la sociedad de la información en Bolivia los datos fueron obtenidos de la encuesta nacional de opinión sobre tecnologías de información y comunicación (TIC) y se realizó la entrevista al Comité de Calidad, Seguridad de la Información y de Emergencia de la ADSIB. Los resultados obtenidos de esta investigación manifiestan que no se cuenta con implementación de políticas y regulación integral en temas de seguridad y protección de datos personales dirigidos a toda la sociedad de la información de Bolivia. Se demuestra la importancia y de este tema en la sociedad, organizaciones y profesionales que gestionan o administran la información. Se presentan las normas, leyes nacionales e internacionales en relación al tema de investigación. Asimismo, la discusión de los diversos enfoques, relacionados a la sociedad de la información en Bolivia, sobre la seguridad de la información y protección de datos personales.

Finalmente, debemos tomar en cuenta que la sociedad de la información y el impacto de la revolución tecnológica en la misma, debe ser un campo donde la seguridad de la información y protección de datos personales sea una garantía para el buen control y desarrollo de esta sociedad. Asimismo, permita contemplar mejoras adaptables en seguridad de la información y protección de datos personales hacia la sociedad de la información boliviana, proporcionando estadísticas para excelentes políticas, controles y diseños en temas de seguridad de la información y protección de datos personales.

Palabras claves: <seguridad de la información><datos personales><firma digital><sociedad de la información><protección de los datos personales>

Agradecimiento

A Dios por todo lo otorgado en nuestras vidas y por ser el guía en nuestros caminos.

A nuestros padres por su amor, comprensión y paciencia quienes nos brindaron apoyo incondicional, ejemplo y educación

A nuestros formadores, maestros, docentes, que nos enseñaron que el estudio significa sacrificio para lograr cambios en el futuro.

En especial a la Lic. María Ana Lorena Martínez Quinteros, por compartir sus conocimientos, consejos y tiempo brindado.

También así, a la Agencia Para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB), y la Agencia de Gobierno Electrónico y Tecnologías de la Información y Comunicación (AGETIC)

Dedicatoria

A Dios por habernos mostrado su camino, por darnos la salud y bendición para alcanzar nuestras metas guiándonos en el trayecto de nuestras vidas.

En memoria de mi padre Josué Jiménez Fernández y eterno agradecimiento a mi madre Eusebia Mancilla y hermanos.

José Antonio Jiménez Mancilla

A mi hijo quien ha sido mi mayor motivación para nunca rendirme en los estudios y llegar a ser un ejemplo para él.

Deyci Orellana Heredia

ÍNDICE

LISTA DE FIGURAS

LISTA DE CUADROS

LISTA DE GRÁFICOS

LISTA DE ANEXOS

GLOSARIO DE TÉRMINOS

Activo.- En general, activo es todo aquello que tiene valor para la entidad o institución pública.

Activo de Información.- Conocimientos, información o datos que tienen valor para la organización.

Acuerdo de Confidencialidad.- Documento en el cual el servidor público y/o terceros se comprometen a respetar la confidencialidad de la información y a usarla solo para el fin que se estipule.

Amenaza.- Causa potencial de un incidente no deseado, que puede dar lugar a daños en un sistema o en una organización.

Comité de Seguridad de la Información (CSI).- Equipo de trabajo conformado para gestionar, promover e impulsar iniciativas en seguridad de la información.

Confidencialidad.- Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Custodio del Activo de Información.- El servidor público encargado de administrar y hacer efectivo los controles de seguridad, que el responsable o propietario del activo de información haya definido.

Criptografía.- Escritura secreta. Arte de escribir con signos convenidos para impedir que su significado sea descifrado por quien no sea la clave.

Criptografía simétrica.- este tipo de criptografía se usa para cifrar y descifrar mensajes, se basa en el uso de una única clave conocida de antemano por ambas partes. La seguridad de este tipo de criptografía radica principalmente en mantener en secreto la clave y no se preocupa necesariamente por el algoritmo de cifrado, es decir, que no es de mucha ayuda conocer el algoritmo que se utilizó.

Criptografía asimétrica.- La que utiliza un par de claves (clave pública y clave privada) para el envío del mensaje, una para cifrar y otra para descifrar el mensaje; lo que se cifra en emisión con una clave, se descifra en recepción con la clave inversa.

Dato.- Representación formal de la información preparada con el propósito de someterla al tratamiento automático, especialmente de la que se ofrece en la formulación de un problema y es diferente a sus resultados, o de la que es objeto del tratamiento a diferencia de las señales de mando que lo controlan.

Declaración de Aplicabilidad.- Documento en el cual se enumeran los controles a implementar o implementados ya previamente.

Digital.- Se refiere a la representación de datos de forma discreta (discontinua) a diferencia de analógico, que denota la representación en forma continua (Conde & Arteaga, 2011, p. 93)

Disponibilidad.- Propiedad de acceso y uso de información a entidades autorizadas cuando estas lo requieran.

Evento de Seguridad de la Información.- Ocurrencia identificada de un estado de un sistema, servicio o red que indica que una posible violación de la política de seguridad de la información o la falla de controles o una situación previamente desconocida, que pueda ser relevante para la seguridad.

Firma.- Nombre o apellido de una persona, que se pone, con rubrica o sin ella, al pie de un escrito para darle validez y autenticidad. Designa el nombre de una casa de comercio y razón social (Conde & Arteaga, 2011, p. 131).

Firma.- Rasgo o conjunto de rasgos, realizados siempre de la misma manera, que identifican a una persona y sustituyen a su nombre y apellidos para aprobar o dar autenticidad a un documento.

firma digital.- es una modalidad de firma electrónica que utiliza una técnica de criptografía asimétrica y que tiene la finalidad de asegurar la integridad del mensaje de datos a través de un código de verificación, así como la vinculación entre el titular de la firma digital y el mensaje de datos remitido.

Firma electrónica.- es simplemente un concepto genérico y neutral que se refiere a todas las tecnologías con las cuales una persona puede “firmar” un mensaje de datos

Impacto.- Cambio adverso en la operación normal de un proceso de la institución pública.

Incidente de Seguridad de la Información.- Evento o una serie de eventos de seguridad de la información no deseada o inesperada, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad.- Propiedad que salvaguarda la exactitud y completitud de la información.

Plan Institucional de Seguridad de la Información (PISI).- Documento que establece las actividades relativas a la organización y gestión de la seguridad de la información en la entidad o institución pública.

Política de Seguridad de la Información (PSI).- Acciones o directrices que establecen la postura institucional en relación a la seguridad de la información, incluidas dentro del Plan Institucional de Seguridad de la Información (PISI).

Propietario o Responsable del Activo de Información.- Servidor público de nivel jerárquico quien tiene la responsabilidad y las atribuciones de establecer los requisitos de seguridad y la clasificación de la información relacionada al activo, según el alcance definido del proceso al cual pertenece la misma.

Propietarios de procesos.- Servidor público de nivel jerárquico que tiene la responsabilidad y atribución de establecer las actividades, roles y responsabilidades de los procesos.

Responsable de Seguridad de la Información (RSI).- Servidor público responsable de gestionar, planificar, desarrollar e implementar el Plan Institucional de Seguridad de la Información (PISI).

Responsable de Seguridad de la Información.- Servidor público que tiene asignadas las funciones de desarrollar e implementar el Plan Institucional de Seguridad de la Información, que entre las responsabilidades está la de gestionar incidentes.

Riesgo.- Combinación de la probabilidad de un evento adverso y su consecuencia.

Seguridad de la Información.- La seguridad de la información es la preservación de la confidencialidad, integridad y disponibilidad de la información; además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no repudio y confiabilidad.

Seguridad Informática.- Es el conjunto de normas, procedimientos y herramientas, las cuales se enfocan en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante.

Servidor Público.- Persona individual, que independientemente de su jerarquía y calidad, presta servicios en relación de dependencia a una entidad, u otras personas que presten servicios en relación de dependencia, cualquiera sea la fuente de su remuneración.

Seudonimización.- el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable. (El Parlamento Europeo y el Consejo de la Unión Europea, 2016, p. 29)

Software.- Conjunto de programas y sistemas operativos que forman el material intelectual necesario para el uso y funcionamiento de la computadora. Componentes lógicos (programas) de un ordenador. Se llama también lógica. Conjunto estructurado de instrucciones que permiten al computador ejecutar los trabajos que se le piden. Estas instrucciones se expresan en lenguaje que el computador entiende directamente, con el nombre del lenguaje de máquina y que está fundado en la numeración binaria, o en un lenguaje evolucionado, que se llama lenguaje de programación, que el computador traduce el lenguaje de máquina. (Conde & Arteaga, 2011, p. 252).

Usuario de la información.- Persona autorizada que accede y utiliza la información en medios físicos o digitales para propósitos propios de su labor.

Vulnerabilidad.- Debilidad de un activo o control, que puede ser explotada por una amenaza.

ÍNDICE DE SIGLAS

AASANA.- Administración de Aeropuertos y Servicios Auxiliares a la Navegación Aérea.

ABC.- Administradora Boliviana de Carreteras.

ADSIB.- Agencia para el Desarrollo de la Sociedad de la Información en Bolivia.

AE.- Autoridad de Fiscalización y Control Social de Electricidad.

AEPD.- Agencia Española de Protección de Datos.

AGETIC.- Agencia de Gobierno Electrónico y Tecnologías de la Información y Comunicación.

AIT.- Autoridad de Impugnación Tributaria.

ANB.- Aduana Nacional de Bolivia.

ANH.- Agencia Nacional de Hidrocarburos.

ASFI.- Autoridad de Supervisión del Sistema Financiero.

ATT.- Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes.

BCB.- Banco Central de Bolivia.

BDP-SAM.- Banco de Desarrollo Productivo.

BJA.- Programa Bono Juana Azurduy.

BUSA.- Banco Unión S.A.

CGE.- Contraloría General del Estado.

CGII.- Centro de Gestión de Incidentes Informáticos.

CIA.- Consejo Internacional de Archivos.

COPLUTIC.- Comité Plurinacional de Tecnologías de Información y Comunicación.

CP.- Políticas de Certificación

CPE.- Constitución Política del Estado.

CPS.- Declaración de Prácticas de Certificación

CSI.- Comité de Seguridad de la Información.

CTIC.- Consejo para las Tecnologías de la Información y Comunicación.

CTIC-EPB.- Consejo para las Tecnologías de la Información y Comunicación del Estado Plurinacional de Bolivia.

DIGEMIN.- Dirección General de Migración.

DIREMAR.- Dirección Estratégica de Reivindicación Marítima.

DNI.- Documento Nacional de Identidad

EGPP.- Escuela de Gestión Pública Plurinacional.

EMAPA.- Empresa de Apoyo a la Producción de Alimentos.

EMI.- Escuela Militar de Ingeniería.

FBI.- Departamento Federal de Investigaciones.

FFAA.- Fuerzas Armadas

FONDESIF.- Fondo de Desarrollo del Sistema Financiero y de Apoyo al Sector Productivo.

GADP.- Gobierno Autónomo Departamental de Potosí.

IBMETRO.- Instituto Boliviano de Metrología.

IBNORCA.- Instituto Boliviano de Normalización y Calidad.

IEC.- International Electrotechnical Commission - Comisión Electrotécnica Internacional

IFLA.- Federación Internacional de Asociaciones de Bibliotecarios y Bibliotecas

INE.- Instituto Nacional de Estadística.

ISO.- Organización Internacional para la Normalización.

LOPD.- Protección de Datos de Carácter Personal.

MAGERIT.- Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

MEFP.- Ministerio de Economía y Finanzas Públicas.

MIN-GOB.- Ministerio de Gobierno.

MIN-SAL.- Ministerio de Salud.

MND - MIN-DEF.- Ministerio de Defensa.

MOPSV.- Ministerio de Obras Públicas Servicios y Vivienda.

NB.- Norma Boliviana

OCDE.- Organización para la Cooperación y el Desarrollo Económico.

OPCE.- Observatorio Plurinacional de la Calidad Educativa.

OPE.- Órgano Plurinacional Electoral.

PGE.- Procuraduría General del Estado.

PISI.- Plan Institucional de Seguridad de la Información.

PSI.- Política de Seguridad de la Información.

RAR.- Resolución Administrativa Regulatoria

RSI.- Responsable de Seguridad de la Información.

RUAT.- Registro Único para la Administración Tributaria Municipal.

SEDEM.- Servicio de Desarrollo de las Empresas Públicas Productivas.

SEGIP.- Servicio General de Identificación Personal.

SENARECOM.- Servicio Nacional de Registro y Control de la Comercialización de Minerales y Metales.

SENASAG.- Servicio Nacional de Sanidad Agropecuaria e Inocuidad Alimentaria.

SENASIR.- Servicio Nacional del Sistema de Reparto.

SERGEOMIN.- Servicio Geológico Minero.

SGSI.- Sistema de Gestión de Seguridad de la Información.

SIDA.- Síndrome de Inmunodeficiencia Adquirida.

SIM.- Subscriber Identity Module - Módulo de Identificación de Abonado

SIN.- Servicio de Impuestos Nacionales.

SNIS y VE.- Sistema Nacional de Información en Salud y Vigilancia Epidemiológica.

SYMATEC.- Corporación multinacional estadounidense que desarrolla y comercializa software para computadoras.

TA.- Tribunal Agroambiental.

TI.- Tecnologías de la Información.

TIC.- Tecnologías de la Comunicación y Comunicación.

UDAPE.- Unidad de Análisis de Políticas Sociales y Económicas.

UE.- Unión Europea

UMSA.- Universidad Mayor de San Andrés.

UNAM.- Universidad Nacional Autónoma de México

UNE.- Una Norma Española

YPFB.- Yacimientos Petrolíferos Fiscales Bolivianos.

Resumen

La presente investigación analiza la seguridad de la información y la protección de los datos personales en la firma digital implementados por la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB). Para esto, se aplicó la metodología de investigación cuantitativa, descriptiva y deductiva. Y se realizó un análisis del comportamiento de la sociedad de la información en Bolivia en factores asociados a la filtración de la información, servicios, ataques cibernéticos, daño a la imagen, actividad económica y desarrollo de trámites, análisis obtenido mediante el uso de la encuesta nacional de opinión sobre tecnologías de información y comunicación (TIC), proporcionado por la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC), cuya ejecución se realizó en diciembre de 2016 y la publicación de los resultados fueron presentados en diciembre de 2017. En efecto, la encuesta cuenta con una licencia de uso y con declaración de datos abiertos (ver anexo 1).

La entrevista fue dirigida hacia el Comité de Calidad, Seguridad de la Información y de Emergencia ADSIB (ver anexo 3), que tiene como objetivo garantizar, coordinar, evaluar, y aprobar iniciativas de calidad de los servicios y seguridad de la información y la activación y desarrollo del Plan de Continuidad para la prestación del servicio de la Entidad Certificadora Pública. En otras palabras, lograr con ello una comunicación interpersonal necesaria, con el fin de obtener respuestas verbales a las interrogantes que planteamos sobre el problema investigado. En síntesis, la entrevista permitió obtener una información más completa.

Los resultados obtenidos de esta investigación manifiestan que no se cuenta con implementación de políticas y regulación integral en temas de seguridad y protección de datos personales dirigidos a toda la sociedad de la información de Bolivia. No obstante, la ADSIB solo cuenta con estas características orientadas solo en los servicios que brinda como Entidad

Certificadora Publica. En consecuencia, el componente más importante para mantener la confidencialidad, integridad y disponibilidad y primicias de protección de datos personales es la sociedad de la información, por su relación e involucramiento en los distintos organismos de Estado.

También así, se muestra la importancia y justificación de este tema hoy en día, orientados a la sociedad, organizaciones y profesionales que gestionan o administran la información. Se presentan las normas, leyes nacionales e internacionales en relación al tema de investigación. Asimismo, discusión de los diversos enfoques relacionados a la sociedad de la información en Bolivia, concernientes a la seguridad de la información y protección de datos personales.

Finalmente, debemos tomar en cuenta que la sociedad de la información y el impacto de la revolución tecnológica en la misma, debe ser un campo donde la seguridad de la información y protección de datos personales sea una garantía para el buen control y desarrollo de esta sociedad. Asimismo, permita contemplar mejoras adaptables en seguridad de la información y protección de datos personales hacia la sociedad de la información boliviana, proporcionando estadísticas para excelentes políticas, controles y diseños en temas de seguridad de la información y protección de datos personales.

CAPÍTULO I - INTRODUCCIÓN

La seguridad de la información es el resultado de la protección de la confidencialidad, integridad y disponibilidad de la información. De ahí que, es altamente sustancial lograr entender cada una de las partes que la conforman. Es necesario aseverar que la información en las organizaciones no haya sido alterada, de tal manera, que se puedan garantizar el acceso y automatización de la información por las entidades autorizadas. Por lo tanto, la misma también involucra otras características como ser; la relación con la autenticidad de la información, confiabilidad, responsabilidad y no repudio.

Si bien es cierto, que todas las empresas, entidades, organismos, desempeñan sus actividades almacenando y generando nueva información infatigablemente, pues bien, la información es considerada como conjunto de datos, los cuales son procesados para generar conocimiento, con un valor que sirve para la toma de decisiones o desarrollo de acciones. De ahí que, la información llega a ser apreciada como un activo, que es de gran valor y de vital importancia para la organización. De modo que, la información generada, se encuentra plasmada en documentos físicos como digitales entre los más importantes, los cuales se hallan en resguardo y procesamiento en los archivos. En efecto, la información vital y de gran valor para una organización se encuentra en los archivos, los cuales deben considerar gestionar políticas y normas para la protección de la misma.

Resulta claro, que constantemente y día a día las organizaciones tratan con miles y miles de datos personales para poder gestionar los servicios que realizan, de ahí que, la operación de la información que las organizaciones desarrollan con los datos personales, tanto de la ciudadanía y personal que cuenta, en su proceso, son: recogidas, almacenadas, utilizadas, modificadas, grabadas, canceladas, y suprimidas, etc. Es decir, que la información personal es considerada

como cualquier información concerniente a una persona, estas pueden ser: nombre y apellido, fecha de nacimiento, dirección de domicilio, correo electrónico, número de cuenta, ingresos percibidos, e historial médico entre otros. Las administraciones de las organizaciones de empresas públicas como privadas, recogen esta información y la utilizan para desarrollar su actividad. Es decir, con esta información, una organización puede deducir los intereses y nivel adquisitivo de una persona, así como gustos o aficiones, por lo cual, su protección es significativa para una organización. Es más, las organizaciones que obtengan datos personales, tienen la obligación de proteger los datos obtenidos de los individuos, ya que los mismos son propiedad de la persona a la que se refiere, razón por la cual han de ser tratados para ser resguardados.

El uso de las nuevas tecnologías de la información y comunicación, son el aprovechamiento del acceso hacia la información presentada en diferentes códigos (texto, imagen. Sonido, video, etc.), de ahí que, la información combinada con tecnologías, trabaja más de forma interactiva, lo que le permite, almacenarla, recuperarla, procesarla, facilitando la comunicación de la información. En consecuencia, las necesidades de tecnología en la sociedad, para una mejor planificación, organización, desarrollo de una infraestructura tecnológica, son necesarias para lograr los fines previstos. En efecto, la combinación de estos recursos, permite el procesamiento, almacenamiento y transmisión de la información, donde internet forma parte de ese desarrollo, además incorpora el uso de las computadoras y tecnologías al alcance de todos, como un teléfono móvil o computadora ultra portátil, que constantemente cuentan con mayor capacidad de operar en redes inalámbricas y de mejor acceso y rendimiento.

Se ha verificado, que una característica del aprovechamiento de las tecnologías de la información y comunicación, es la capacidad de almacenar la información, que en su detallada composición cuentan con datos específicos y relacionados, y la estandarización de estos, son

vislumbrados como datos abiertos. Es decir, los datos abiertos son datos accesibles que se encuentran normalizados, los mismos son la referencia de la actividad que los organismos generan. En consecuencia, la mayoría de estos datos son masivos, y caracterizan perfectamente el comportamiento de una sociedad, organización o empresa. Por ende, estos datos son reutilizables y pueden ser manipulados por países, universidades, centros de investigación, científicos e investigadores para estudiar un fenómeno, de manera que, el fin de la accesibilidad y explotación de estos datos, es para que los distintos actores puedan utilizarlos.

Importa, y por muchas razones que una población que comprende, crece y se desarrolla alrededor de la información, se caracteriza y vislumbra como una sociedad de la información, de ahí que, la misma perfecciona las oportunidades que brindan las tecnologías de la información y comunicación en el desarrollo individual, profesional y población que la forma, a fin, de realizar esfuerzos por convertir la información en conocimiento.

Siendo las cosas así, resulta claro, que una interacción y relación de la ciudadanía con el gobierno, apoyada por el aprovechamiento de herramientas informáticas y tecnologías de la información y comunicación es comprendida como gobierno electrónico. Pues bien, comprende la necesidad de los gobiernos para poder agilizar, optimizar, flexibilizar y transparentar trámites o procesos, mejorando las herramientas de gestión y el aprovechamiento de la velocidad de las tecnologías de la información y comunicación, de ahí que, para ello comprende la creación de plataformas de trabajo como ser, interoperabilidad, datos libres, seguridad, software libre entre otros. En efecto, es la transformación del gobierno, para un mejor rendimiento de gestión gubernamental.

Dentro de esta perspectiva, las entidades que comprenden la importancia de la integridad, autenticidad y el no repudio de los datos en la información, vislumbran las ventajas de la

reducción de tiempo en los trámites, de forma que, entienden el dominio de la brecha digital con el uso de los documentos digitales, es por ello, que el sector público y la población en general, orientadas en el manejo de las nuevas tecnologías de la información y comunicación, aplican la firma digital en sus operaciones y organización. En efecto, la firma digital es aquella que, mediante un certificado digital, garantiza la autoría del firmante, asimismo, está compuesta por dos claves criptográficas que cifran el mensaje, protegiendo la confidencialidad del documento. En resumen, facilita el intercambio de información entre instancias, entidades, empresas y personas, con el impulso de las tecnologías de la información y comunicación.

Bajo esta perspectiva, el actual estudio se llevó a cabo en la sociedad de la información de Bolivia, y de igual manera, en la agencia encargada para su desarrollo a nivel nacional. En efecto, la particularidad de esta población es que se desarrolla y crece alrededor de la información y que se ve afectada por el progreso tecnológico de manera profunda en las actividades que realizan, como en el trabajo o acción diaria, por consiguiente, comprende que el relacionarse y comunicarse se basa fundamentalmente en el uso de las nuevas tecnologías de la información y comunicación.

Para el presente trabajo se utilizó la Base de Datos Abiertos de la encuesta de opinión nacional de tecnologías de la información y comunicación, proporcionado por la Agencia de Gobierno Electrónico y Tecnologías de la Información y Comunicación (AGETIC), donde los resultados publicados en la gestión 2017, logran identificar a esta sociedad. Tanto así que, por sus características de datos abiertos, estos son: detallados, disponibles, oportunos y de acceso libre y sin restricciones, contando con una licencia para su uso.

Uno de los componentes más importantes, de la investigación lo conforma la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB), una entidad descentralizada

bajo la tuición de la Vicepresidencia del Estado Plurinacional de Bolivia, cuyo objetivo es implementar políticas, estrategias y acciones orientadas a reducir la brecha digital en el país. En definitiva, una de sus particularidades es constituirse en entidad certificadora pública, proporcionando el servicio de certificación digital y firma digital para el sector público y población en general. De modo que, la misma cuenta con un comité de calidad, seguridad de la información y de emergencia, con la finalidad de garantizar, coordinar, evaluar aprobar iniciativas en tema de seguridad de la información. Razón por la cual, cada uno de estos componentes, en su alcance e importancia son factores muy esenciales y necesarios para la comprensión de la seguridad de la información y protección de datos personales, en un entorno donde se desarrolla la sociedad de la información, la automatización de la información gracias a las nuevas tecnologías de la información y comunicación, que están orientadas a una transformación digital y gobierno electrónico.

Dentro de esta perspectiva, la presente investigación queda constituida en los siguientes capítulos determinados de la siguiente manera:

Capítulo 1. Se presentan los aspectos principales de la investigación como ser: Antecedentes, planteamiento del problema, hipótesis de investigación, objetivo general y especifico, justificación, etc. Como también el marco referencial.

Capítulo 2. Se encuentra desarrollado el marco teórico, con el desglose de la investigación científica en el estudio de la Seguridad de la Información y Protección de Datos Personales, y avances desarrollados por el país, esta construcción teórica está acompañada de igual manera con el desarrollo del Marco Legal y Marco Normativo, en refuerzo hacia la investigación.

Capítulo 3. Se presenta la metodología empleada para la investigación, como herramientas del análisis estadístico, el tipo de estudio y el uso de datos.

Capítulo 4. Se encuentran los resultados, en los cuales se presentan los gráficos interpretados y descritos en apoyo a la investigación. Del mismo modo, la entrevista al Comité de Calidad, Seguridad de la Información y Emergencia de la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB)

Capítulo 5. Se encuentran las conclusiones de la investigación, así como también la bibliografía.

Capítulo 6. Se presentan el marco propositivo y anexos.

1.1 Antecedentes

1.1.1 Antecedentes históricos de la seguridad de la información

Cabe señalar, que el concepto de seguridad de la información es tan antiguo al igual que la historia del hombre, es decir, comprende la época en que la información era transmitida oralmente, esta no era comunicada a cualquiera, más aún en temas susceptibles como: intereses particulares, posesión territorial o militar, en ese caso, se percibió que la información no debía ser poseída por cualquiera, y mucho menos ser compartida a terceros (Maggiore, 2014). De ahí que, en su atributo el individuo hizo uso de la escritura buscando proteger la información, vinculante en relación a su vida económica, social, cultural, jurídica, etc. En efecto, la seguridad de la información era un tema muy transcendental desde la antigüedad, partiendo desde el grado de importancia que comprendía la información

De estas evidencias, distintas culturas manejan la seguridad a su manera, tal es el caso de la Biblioteca de Alejandría[1], que fue destruida en tres oportunidades, y su recuperación total no pudo realizarse jamás. En definitiva, la Biblioteca de Alejandría era la más grande del mundo fundada a comienzos del siglo III a. C. por Ptolomeo I Sóter[2]. En resumen, llegó a albergar hasta

[1] Biblioteca de Alejandría: La biblioteca de Alejandría. Tras la muerte de Alejandro Magno, sus conquistas fueron divididas entre sus generales. En este contexto surge la ciudad de Alejandría, situada en el margen izquierdo del delta del río Nilo. Esta ciudad estuvo a cargo de la dinastía de los Ptolomeos; Ptolomeo I Soter y Ptolomeo II Filadelfo . Hay tres personajes involucrados en estos eventos: Julio César, Teófilo de Alejandría y el Califa Omar de Damasco. Teófilo fue quien quemó varios templos paganos en Alejandría defendiendo el cristianismo, y la biblioteca tenía muchos pergaminos que probablemente fueron quemados.

[2] Ptolomeo I Sóter: Ptolomeo I Sóter, fue un general griego macedonio al servicio de Alejandro Magno y uno de los tres diádocos que se disputaron el control de su extenso imperio. Ptolomeo se convirtió en gobernante de Egipto entre 323 y 282 a.C.

900.000 manuscritos[3] plasmados en distintos soportes conocidos en la antigüedad, como: pergaminos, papiros, tablillas de arcilla entre otros, tanto así que, se llegó a perder mucha información que jamás se recuperó, gracias a los conflictos armados. Es por ello, que nace la necesidad de resguardar la información que comprende el respaldo de hechos importantes, ya sea en el soporte[4] en el que se encuentre y donde haya sido almacenada.

Evidentemente, las medidas de seguridad implementadas por los reinos para proteger la información de sus documentos, era importante pues estos eran de vital importancia para la comunicación y defensa militar, de modo que, la transmisión de la información estaba adaptada al soporte de la época, como por ejemplo se hacía uso del sello que contenían los anillos de los reyes[5] para autenticar y conservar la confidencialidad del documento o pergamino, estos no debían presentar ninguna observación de abuso para confirmar su credibilidad, en otras palabras, el no repudio del documento (Maggiore, 2014). En efecto, esto demostró las tareas de seguridad aplicadas en esos tiempos, y el cuidado y tiempo dedicado a ellas, incluyendo de este modo a la seguridad en la información, que infatigablemente fue una tarea importante en el desarrollo de la historia.

Queremos con ello significar, que la historia siempre percibió la importancia de la seguridad de la información, esto se pudo apreciar tras comprender a las grandes civilizaciones y a las más

---

[3] Manuscritos: Un manuscrito se trata de un documento que contiene información escrita a mano sobre un soporte flexible y manejable, con materias como la tinta de una pluma, de un bolígrafo o simplemente el grafito de un lápiz.

[4] Soporte de información: son los materiales físicos que almacenan datos, y que posteriormente permiten recuperar la información contenida en ellos mediante el uso de un dispositivo de entrada-salida adecuado. son los dispositivos que permiten trasladar la información desde el ordenador a los soportes de información y viceversa.

[5] Sello del anillo de los reyes: El término sello (en algunos países también llamado timbre) se aplica, por un lado, para nombrar el instrumento con imágenes grabadas que, a través de la impresión de tinta sobre el papel, se utiliza para autorizar documentos.

importantes potencias[6] que existieron en el mundo. De ahí que, en la edad media[7], los registros del Imperio Europeo[8] eran plasmados en soportes como los pergaminos entre otros y recibían una seguridad como uno de los más importantes tesoros que estos poseían, estos archivos[9] agrupados, eran llevados en mulas de carga detrás de los reyes y señores feudales. “los reyes llevaban el archivo del reino consigo a todas partes a fin de que los mismos guardias, destinados para la seguridad de sus personas pusieran también a cubierto un tesoro tan precioso” (como se citó en Oporto Ordoñez , 2011, p. 27-28).

Así se ha verificado, que las organizaciones, implementaban maneras de proteger la información, necesarios para su funcionalidad, de modo que, diferenciamos a las primeras organizaciones, cuando ellas requerían hacer uso de la información que se encontraba disponible solo en soporte papel, las autoridades e intervinientes, que eran los responsables de los mismos, implementaron así, para su cuidado el uso de armarios con llaves, puertas con doble seguro, maquinaria para su custodia, etc.

Fue también relevante, el siglo XX reconocido por el desarrollo de las industrias o revolución industrial[10], donde los grandes promulgadores de las organizaciones y direcciones de empresas comprendieron la necesidad de la seguridad como una función empresarial. Así, la teoría clásica

---

[6] Potencias: mundial es el calificativo atribuido a un Estado que tiene la capacidad de influir o proyectar poder, tanto política como económicamente, a escala mundial.

[7] Edad media: Período histórico, posterior a la Edad Antigua y anterior a la Edad Moderna, que comprende desde el fin del Imperio romano, hacia el siglo V, hasta el siglo XV.

[8] Imperio Europeo: El imperialismo europeo. El imperialismo se puede definir como el sistema en el que la política, la economía y la cultura de una parte del mundo se organizan en función del dominio de unos países sobre otros..

[9] Archivos: conjunto ordenado de documentos o lugar donde estos se almacenan. El archivo informático (o fichero informático), conjunto de bits almacenados en un dispositivo.

[10] Revolución industrial: Se conoce como Revolución Industrial a aquel período histórico que se extendió desde la segunda mitad del siglo XVIII, hasta principios del XIX y en el cual, preeminentemente en Europa, se produjo una incontrolable e innumerable cantidad de transformaciones tecnológicas, culturales y socioeconómicas, que desde la etapa neolítica no se sucedían.

de la administración[11] vio la importancia de la seguridad como una función empresarial, tanto así, con el mismo valor de otras actividades como la: financiera, administrativa, comercial y de producción (Herrera, 2012). Cuando las particularidades de esta relación, entrelazan la cercanía de la seguridad con la administración, y esa comprensión articuló el sentido de la seguridad con la gestión.

Las organizaciones, intuían la necesidad de efectuar la seguridad, ante cualquier amenaza que se presentara hacia sus activos que eran de gran importancia, de ahí que, a inicios del siglo XX una organización buscaba proporcionar seguridad, la misma salvaguardaba las propiedades contra el robo, inundación, huelgas, felonías y personas. Pues así, de forma amplia también contra los disturbios sociales [12]y medidas que lleguen a poner en peligro el progreso y negocio. Fue por este motivo que las medidas de seguridad dentro de este periodo de tiempo, tomó más importancia a la protección de activos[13] físicos e instalaciones, (Gómez Vieites, 2007). Por consiguiente, estas organizaciones desplegaron la necesidad de proteger los activos más trascendentales para su empresa ante cualquier contexto o escenario que amenazara a estos bienes.

Es importante subrayar, el valor de la información, y su necesidad de protección, que está claramente arraigada a la historia del hombre, en su sociedad, organización y en la virtud de comunicar o transferir la información. En ese caso, para su mejor disposición, la información paso por distintos soportes que fueron evolucionando con el tiempo, examinando los nuevos

[11] Teoría clásica de la administración: La teoría clásica de la administración se distingue por el énfasis en la estructura y en las funciones que debe tener una organización para lograr la eficiencia. Su exponente fue Henry Fayol en 1,916. La exposición de Fayol parte de un enfoque sintético, global y universal de la empresa, inicia con la concepción anatómica y estructural de la organización.

[12] Disturbios sociales: conflicto armado, por lo general en la vía pública, donde se ve alterado el orden público por medio de la violencia. Por lo común, ocurre durante una manifestación.

[13] Activos: son los bienes, derechos y otros recursos controlados económicamente por la empresa, resultantes de sucesos pasados de los que se espera obtener beneficios o rendimientos económicos en el futuro.

procesos para su soltura hasta nuestros tiempos. En la actualidad el uso de soportes de información físicos[14] como digitales[15], requiere nuevas medidas para proteger la información.

Comprendiendo trascendentales cambios adquiridos por la edad moderna[16], con una comunicación permitida de manera casi inmediata, y una conectividad a nivel mundial se abrieron las puertas a diversas formas de desarrollo en todos los campos, gracias a las tecnologías de la información y comunicación[17]. De forma que, la globalización de la economía, alcanzó nuevas dimensiones, comprendiendo la necesidad de depender de un desarrollo tecnológico, para seguir evolucionando y creciendo. En consecuencia, esto produjo el aumento de la vulnerabilidad en una amplia gama de amenazas a la seguridad de la información.

1.1.2 Antecedentes históricos de la protección de los datos.

Es importante subrayar, la protección de datos personales, que comprende cualquier información concerniente a una persona, y su razón data desde las grandes conglomeraciones en las importantes ciudades, como es el caso de la antigua ciudad de Roma[18], donde la sociedad adquiría esclavos[19]y estos podían comprar la libertad del hombre, pero no sus pensamientos. De manera que, esta sociedad entendió la existencia de un hombre exterior y un hombre interior. De

[14] Información física: es el soporte de almacenamiento de datos o medio de almacenamiento de datos es el material físico donde se almacenan los datos que pueden ser procesados por una computadora, un dispositivo electrónico, o un sistema informático, aunque este término también abarca el concepto de documento no necesariamente informatizable.

[15] Digital: El concepto, de todas formas, está estrechamente vinculado en la actualidad a la tecnología y la informática para hacer referencia a la representación de información de modo binario.

[16] Edad moderna: Período histórico, posterior a la Edad Media y anterior a la Edad Contemporánea, que comprende desde el siglo XV hasta fines del siglo XVIII.

[17] Tecnología de la información y comunicación: Las Tecnologías de la Información y la Comunicación, también conocidas como TIC, son el conjunto de tecnologías desarrolladas para gestionar información y enviarla de un lugar a otro. Abarcan un abanico de soluciones muy amplio. ... Fácil acceso a todo tipo de información.

[18] Roma: Conocido como uno de los imperios más importantes y poderosos de la Antigüedad, el Imperio Romano puede describirse como una fenomenal estructura de poder político, económico y cultural que abarcaría uno de los territorios más extensos de la historia y que duraría más de cuatro siglos como tal hasta su caída en el año 476 d.C.

[19] Esclavo: Que carece de libertad y derechos propios por estar sometido de manera absoluta a la voluntad y el dominio de otra persona que es su dueña y que puede comprarlo o venderlo como si fuera una mercancía.

modo que, la sociedad Romana obtenía esclavos, pero no conseguía tener la mente de los mismos. Es decir, que podemos considerar como uno de los orígenes de la protección de datos personales y de la privacidad.

En la edad media, Santo Tomas[20] y San Agustín[21] consideran que la intimidad es un bien sagrado, que el hombre en su conexión con Dios mediante la oración, era un tiempo de intimidad sagrada. Por lo tanto, "Estas palabras inspiradas expresan bien que el hablar divino nos transforma y diviniza porque nos introduce en la intimidad de Dios" (Blanco de la Lama, 1981, p. 57). En definitiva, la intimidad y privacidad comprende algo bien valorado, donde algunas definiciones lo entienden como un bien, y parte la necesidad de proteger ese bien.

No obstante, en la Edad Moderna, Locke[22] comprende la razón y la libertad negativa en la que el individuo habita en una esfera íntima, en la cual dentro de ese espacio ya concebía la existencia de la protección de los datos, por lo que manifiesta que:

> *Los ciudadanos de la antigüedad dependían entonces de las leyes de su comunidad, la cual no diferenciaba entre la esfera pública y la esfera privada. En el espacio público el ciudadano no solo tomaba decisiones sobre asuntos comunes sino también sobre asuntos privados y, de la misma forma en que este intervenía en la esfera íntima de sus conciudadanos.* (Fonnegra Osorio , 2014, p. 37)

[20] Santo Tomas: Filósofo y teólogo dominico italiano. Nacido en Roccasecca (Nápoles). Es uno de los más eminentes doctores de la Iglesia (1227-1274)

[21] San Agustín: Filósofo y uno de los más ilustres padres de la Iglesia. Nació en la provincia de Numidia, África (352-430). ... Según sus teorías, la filosofía es el amor a Dios, y la fe ayuda a la razón y ésta sirve de apoyo a aquélla.

[22] Johb Lokie: (Wrington, Somerset, 1632 - Oaks, Essex, 1704) Pensador británico, uno de los máximos representantes del empirismo inglés, que destacó especialmente por sus estudios de filosofía política.

Lo cual indica que, la razón de no poder diferenciar la información pública, y la información privada influía de gran manera en la población, esto vulneraba el espacio privado de las personas, cuando se normalizaba alguna ley en su entorno.

1.1.3 Seguridad de la información en Bolivia.

El perfeccionamiento de la seguridad en cuanto a la confidencialidad, integridad y disponibilidad de la información en Bolivia, progresó gracias a la intervención de las nuevas tecnologías de la información y comunicación. De ahí que, el Estado Plurinacional de Bolivia, estableció la Agencia de Gobierno Electrónico y Tecnologías de la Información y comunicación (AGETIC), con políticas y lineamientos establecidos, para el perfeccionamiento y desarrollo de avances en temas de procesos y tecnología. En consecuencia, esta agencia cuenta con la colaboración del Consejo para las Tecnologías de la Información y Comunicación del Estado Plurinacional de Bolivia (CTIC-EPB), cuyas tareas determinadas, comprenden la formulación de propuestas de política y normativa relacionadas al Gobierno Electrónico.

Por lo tanto, en fecha 5 de mayo de 2016 se llevó a cabo la primera reunión para la conformación de grupos temáticos de trabajo en: interoperabilidad[23], software libre, seguridad[24], infraestructura[25], desarrollo de software[26] y datos abiertos[27]. De forma que, los mismos fueron

[23] Interoperabilidad: La interoperabilidad es la capacidad que tiene un producto o un sistema, cuyas interfaces son totalmente conocidas, para funcionar con otros productos o sistemas existentes o futuros y eso sin restricción de acceso o de implementación.

[24] Seguridad: el término seguridad posee múltiples usos. A grandes rasgos, puede afirmarse que este concepto que proviene del latín securitas hace foco en la característica de seguro, es decir, realza la propiedad de algo donde no se registran peligros, daños ni riesgos. Una cosa segura es algo firme, cierto e indubitable. La seguridad, por lo tanto, puede considerarse como una certeza.

[25] Infraestructura: Conjunto de medios técnicos, servicios e instalaciones necesarios para el desarrollo de una actividad o para que un lugar pueda ser utilizado.

[26] Desarrollo de Software: Desarrollar un software significa construirlo simplemente mediante su descripción. Desarrollo de software. ... En un nivel más general, la relación existente entre un software y su entorno es clara ya que el software es introducido en el mundo de modo de provocar ciertos efectos en el mismo.

conformados por los servidores públicos de las entidades del nivel central del Estado: Órgano Ejecutivo, Legislativo, Judicial y Electoral, incluyendo sus instituciones descentralizadas, autárquicas, empresas públicas y autoridades de regulación sectorial; Ministerio Público y Procuraduría General del Estado. Por consiguiente, se invitaron a participar, en calidad de miembros adjuntos, a representantes de entidades territoriales autónomas, universidades públicas e indígenas y sociedad civil, a fin de trabajar y elaborar propuestas a ser presentadas al Consejo para su posible implementación a nivel estatal, motivo por el cual, el grupo de seguridad formuló los lineamientos para las entidades o instituciones públicas del Estado Plurinacional de Bolivia, para la elaboración de planes institucionales de seguridad de la información, de ahí que, el mismo estaba conformado por los representantes de las siguientes entidades:

- Administradora Boliviana de Carreteras (ABC).
- Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC).
- Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB).
- Autoridad de Fiscalización y Control Social de Electricidad (AE).
- Autoridad de Impugnación Tributaria (AIT).
- Autoridad de Supervisión del Sistema Financiero (ASFI).
- Aduana Nacional de Bolivia (ANB).
- Banco Central de Bolivia (BCB).

---

[27] Datos Abiertos: es una filosofía y práctica que persigue que determinados tipos de datos estén disponibles de forma libre para todo el mundo, sin restricciones de derechos de autor, de patentes o de otros mecanismos de control.1 Tiene una ética similar a otros movimientos y comunidades abiertos, como el software libre, el código abierto (open source, en inglés) y el acceso libre (open access, en inglés).

• Banco de Desarrollo Productivo (BDP-SAM).

• Banco Unión S.A (BUSA).

• Programa Bono Juana Azurduy (BJA).

• Dirección Estratégica de Reivindicación Marítima (DIREMAR).

• Empresa de Apoyo a la Producción de Alimentos (EMAPA).

• Instituto Nacional de Estadística (INE).

• Empresa Estatal de Transporte por cable “Mi Teleférico”.

• Escuela de Gestión Pública Plurinacional (EGPP).

• Gobierno Autónomo Departamental de Potosí.

• Ministerio de Defensa (MIN-DEF).

• Ministerio de Economía y Finanzas Públicas (MEFP).

• Ministerio de Salud (MIN-SAL).

• Empresa Pública QUIPUS.

• Registro Único para la Administración Tributaria Municipal (RUAT).

• Senado Nacional (Cámara de Senadores de la Asamblea Legislativa Plurinacional).

• Servicio de Impuestos Nacionales (SIN).

• Servicio General de Identificación Personal (SEGIP).

• Servicio Geológico Minero (SERGEOMIN).

• Servicio Nacional del Sistema de Reparto (SENASIR).

• Sistema Nacional de Información en Salud y Vigilancia Epidemiológica (SNISyVE).

• Universidad Mayor de San Andrés (UMSA).

• Yacimientos Petrolíferos Fiscales Bolivianos (YPFB).

• Sociedad Civil.

También, participaron otras entidades u órganos del Estado a través de explicaciones y acotaciones al documento, las entidades participaron fueron:

• Administración de Aeropuertos y Servicios Auxiliares a la Navegación Aérea (AASANA).

• Agencia Nacional de Hidrocarburos (ANH).

• Contraloría General del Estado (CGE).

• Dirección General de Migración (DIGEMIG).

• Escuela Militar de Ingeniería (EMI).

• Fondo de Desarrollo del Sistema Financiero y de Apoyo al Sector Productivo (FONDESIF).

• Instituto Boliviano de Metrología (IBMETRO).

• Ministerio de Obras Públicas Servicios y Vivienda (MOPSV).

• Ministerio de Gobierno (MIN-GOB).

• Observatorio Plurinacional de la Calidad Educativa (OPCE).

• Órgano Plurinacional Electoral (OPE).

• Procuraduría General del Estado (PGE).

• Servicio de Desarrollo de las Empresas Públicas Productivas (SEDEM).

• Servicio Nacional de Registro y Control de la Comercialización de Minerales y Metales (SENARECOM).

• Servicio Nacional de Sanidad Agropecuaria e Inocuidad Alimentaria (SENASAG).

• Tribunal Agroambiental.

• Unidad de Análisis de Políticas Sociales y Económicas (UDAPE).

Cabe destacar, al Centro de Gestión de Incidentes Informáticos (CGII), bajo la tutela de la agencia ya que es la que vislumbra el desarrollo de lineamientos para la protección de la información, activos de información, promoviendo la seguridad e incidentes de seguridad. De ahí que, evalúa la seguridad de los sistemas informáticos de las entidades del sector público, así como el monitoreo de sitios Web gubernamentales[28].

Por su parte, el esfuerzo desarrollado por el Centro de Gestión de Incidentes Informáticos (CGII), establecieron el documento de lineamientos para las entidades del sector público, donde "El presente documento tiene como objetivo establecer los lineamientos para que las entidades del sector público del Estado Plurinacional de Bolivia puedan elaborar e implementar sus Planes Institucionales de Seguridad de la Información, en concordancia con la normativa vigente" (Consejo para las tecnologías de información y comunicación CTIC, 2017, p. 21). En efecto, la participación de las distintas organizaciones en colaboración, con los intuidos en tema y sus

[28] Webs gubernamentales: Tienen como objetivo mejorar la provisión de información y ofrecer a los ciudadanos el acceso a los servicios públicos. También están incluidas las informaciones sobre eventos, espectáculos, transporte público, bolsa de trabajo, políticas de empleo, licitaciones, mapas, etc. Como ejemplos de servicios interactivos se pueden mencionar: solicitudes de documentos públicos, solicitudes de documentos legales y certificados, expedición de permisos y licencias, otorgamiento de turnos, pagos Online de impuestos, tasas y servicios.

representantes, que trabajaron para el desarrollo de los lineamientos en tema de seguridad a nivel nacional.

1.2 Planteamiento del problema

La seguridad de la información, parte cuando no se contempla el cuidado de la información, la confidencialidad, la modificación de la información, su trasgresión o alteración de integridad de la misma, y dificultando el acceso de la información, impidiendo su disponibilidad, o restándole el valor a la información, por quienes la administran, ya sea personas, organismos de Estado o empresas públicas o privadas, entre otros.

Cabe considerar, por otra parte, el acontecimiento que atenuó la confidencialidad de la información, donde tal hecho fue descrito como el caso Quiborax[29], en el cual no se consideró la sensibilidad de la información de carácter confidencial, manipulada en documentos digitalizados[30], almacenados en un ordenador portátil, provocando un daño económico de más cuarenta y tres millones de dólares al Estado Plurinacional de Bolivia.

> *Para la defensa de los intereses del Estado frente al proceso iniciado por Quiborax ante el Ciadi[31], la Procuraduría gastó 1.384.801 dólares. Ese monto, sumado a los 406.741 dólares por los honorarios y gastos del centro de arbitraje, además de los 42,6 millones que se fijó como compensación, da cuenta de un monto total de 44,3 millones de dólares.* (Los Tiempos, 2018)

---

[29] Quiborax: es una empresa chilena que se fundó en 1986 y comenzó su producción recién en 1988. Se encargan de producir ácido bórico y productos agroquímicos. Exporta a través de los puertos de Arica a todo el mundo.

La empresa, representada por el estudio Bofill Mir & Álvarez Jana, comenzó a operar en Bolivia hace más de 16 años con exploración del mineral no metálico de ulexita en el Salar de Uyuni, en Potosí, a través de una sociedad con Non-Metallin Minerales SA.

[30] Documento digitalizado: La digitalización de documentos es un proceso tecnológico que permite, mediante la aplicación de técnicas fotoeléctricas o de escáner, convertir la información contenida de un documento en papel a una imagen digital.

[31] Ciadi: Centro de Arreglo de Diferencias Relativas a Inversiones https://icsid.worldbank.org/sp

Por otra parte, la acometida a la integridad de la información, producida en el Banco Unión[32], donde uno de los funcionarios alteró los datos y la información concerniente a los depósitos de dinero, hacia los cajeros distribuidos en distintas áreas, permitiendo un monto económico en bolivianos, dañando a la entidad bancaria y vulnerando su capacidad de gestionar la información en sus operaciones.

Observamos también, el acceso a la información, el cual se efectúa a través de correos electrónicos o corporativos, de forma tal que, la gestión administrativa, se desarrolla por este medio, conectando y transfiriendo la información, en todas sus operaciones. En consecuencia, la misma realiza la transferencia de información ya sea en el formato en el que se encuentre, sea este en soporte físico o digital. En definitiva, la información de las organizaciones y de los archivos, son enviados por estos medios, información que en muchos casos no cuenta con controles en seguridad de la información. En consecuencia, la mala administración de esta vulnera información muy importante, tanto para los ciudadanos e incluso para entidades bancarias. Así, lo identifican expertos internacionales. El desfalco económico al Banco Unión, y relacionado con la inadecuada seguridad de la información como "Efecto Pari", ocasiona el temor de que ese riesgo pueda consumarse en cualquier organización.

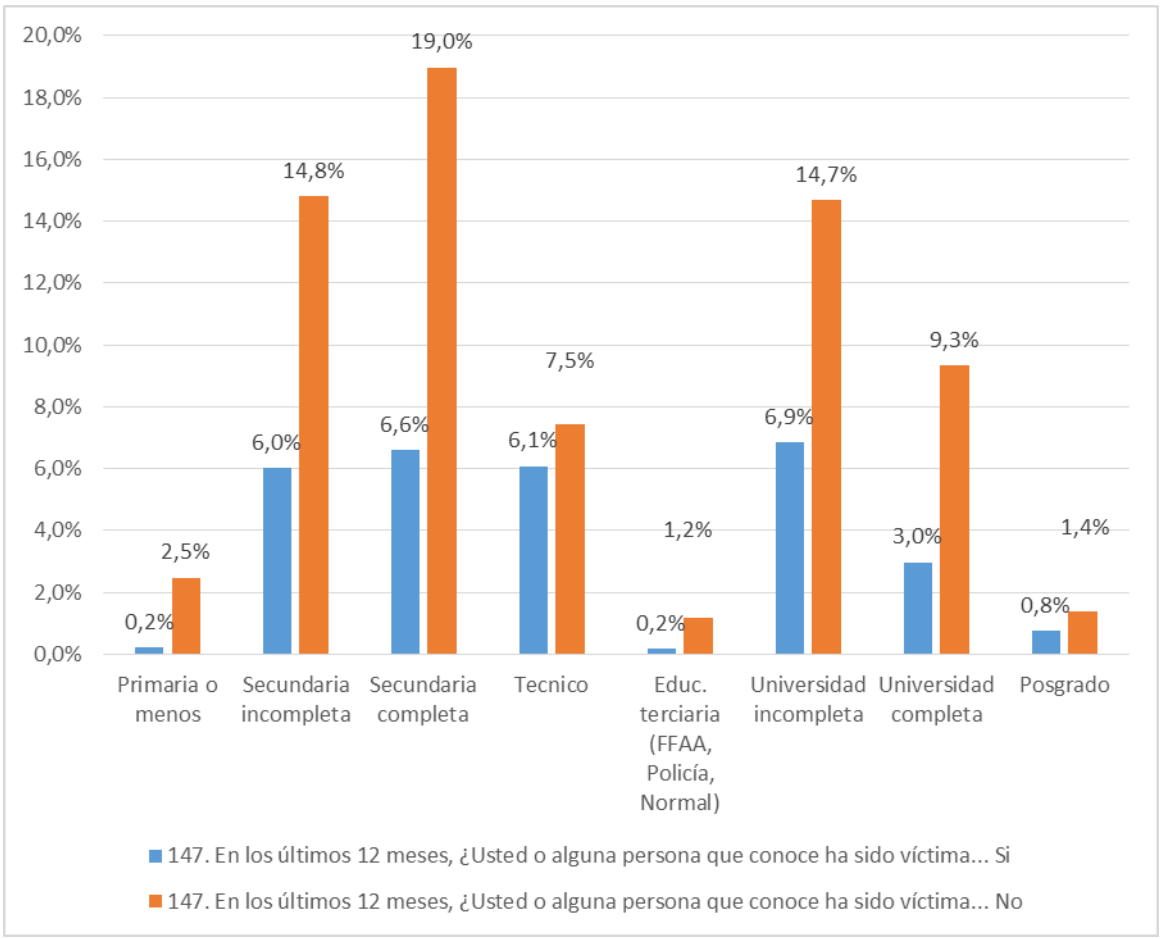
Para el peruano César Chávez, representante de Perú en la Red Latinoamericana de Informática Forense (RedLif), la banca boliviana tiene falencias en todos los niveles. "La mayoría de los bancos de Bolivia no garantizan la seguridad de las transacciones, incluso hay algunos que tienen páginas

[32] Banco Unión: El banco en la actualidad cuenta con dos filiales (Valores Unión y SAFI Unión), y se compone de una extensa red de oficinas y cajeros automáticos en todo el país, tiene un total de 850 funcionarios y un plantel ejecutivo de reconocida capacidad. http://www.bancounion.com.bo/

web endebles" y que permiten "delitos como el phishing (suplantación informática de la identidad), es una banca que no evalúa los errores", sostuvo. (Castel, 2017)

De estas evidencias, es necesario evaluar el riesgo que pueda afrontar la población, empresas u organizaciones. De forma que, descubrir el factor más débil ante un robo de información o sustracción de datos, que puedan dañar de gran manera a estos individuos u Organismos de Estado. Por consiguiente, se detalla el registro de las personas con acceso a Internet en Bolivia que sufrieron robos de identidad en esta plataforma a nivel mundial, o uso indebido de cuenta en la que desarrolla sus actividades.

Gráfico 1 Datos de personas que fueron víctimas de hackeo



Fuente: Elaboración propia en base a las encuestas Tic.

Cabe considerar por otra parte, a los datos personales, que la información referente a un individuo, en las organizaciones, también se identifica a los funcionarios o personal con el que cuenta, de ahí que, los datos personales son recogidos y dispuestos por el Estado u organización. Por si era poco "la mayor parte de nuestra sociedad carece de una cultura de protección de datos y ello se manifiesta de modo contundente en los procesos de captación de datos personales" (Martínez Martínez, 2007, p. 57). Es decir, que los datos personales de todo individuo, se ven vulnerados por la debilidad de una sociedad que carece una cultura de protección de datos, y esto afecta de manera directa a un Estado, sus organismos o empresas.

Así se ha verificado, que muchos Estados tratan de conseguir datos personales e información de los mismos en la actualidad. Gran parte de los gobiernos de los Estados realizan solicitudes formales a redes sociales[33] que almacenan esos datos de carácter personal, es decir, que en un promedio de diez países que solicitaron mayor cantidad de información lo hicieron a una de las más grandes e importantes redes sociales como Facebook[34]. En efecto, estas solicitudes fueron:

> *Estados Unidos, 26.014 solicitudes; India, 7.289 datos personales; Reino Unido, 6.366 solicitudes; Francia, 4.478 solicitudes; Alemania, 4.422 solicitudes; Italia, 1.876 solicitudes; Brasil, 1.819 solicitudes; Pakistán, 1.002 solicitudes; Argentina, 995 solicitudes; y España, 833 solicitudes. En América Latina, los países que más veces solicitaron información son: Brasil, Argentina, México, Chile y Colombia. En este tiempo, Bolivia efectuó una solicitud de información, la misma fue denegada. (Agencia de Gobierno Electrónico y Tecnologías de la Información y Comunicación [AGETIC], 2018, p. 311)*

[33] Redes sociales: Página web en la que los internautas intercambian información personal y contenidos multimedia de modo que crean una comunidad de amigos virtual e interactiva.

[34] Facebook: es una red social creada por Mark Zuckerberg mientras estudiaba en la universidad de Harvard. Su objetivo era diseñar un espacio en el que los alumnos de dicha universidad pudieran intercambiar una comunicación fluida y compartir contenido de forma sencilla a través de Internet.

La población boliviana en la gestión 2017, cuenta con un 96% que hace el uso de las redes sociales, y donde las predominantes son: Facebook, con un 94% de la población que figura tener una cuenta en esa red social, y un 91% menciona estar registrada en WhatsApp[35], red social de mensajería que también es perteneciente a la compañía de Facebook, estos datos figuran en los resultados finales de la encuesta de opinión nacional sobre tecnologías de información y comunicación, proporcionados por la Agencia de Gobierno electrónico y Tecnologías de Información y comunicación.

Asimismo, la red social de Facebook se enfrentó a las autoridades de Estados Unido y del Reino Unido, por la perdida y filtración de más de 87 millones datos personales de sus usuarios.

> *El escándalo de la filtración de datos de Facebook alcanza Europa. Los datos personales de 2,7 millones de usuarios europeos podrían haber sido transmitidos a Cambridge Analytica, la empresa británica que manipuló de forma irregular información de 87 millones de internautas para fines electorales en Estados Unidos, según ha indicado este viernes la Comisión Europea.* (Internacional, 2018)

Luego de una serie de reflexiones podemos señalar que Bolivia, no contempla una característica en gran avance para la protección de los datos personales, en consecuencia, se encuentra vulnerable a amenazas e intereses por otros Estados, empresas u organizaciones.

En la perspectiva que aquí se adopta, las organizaciones almacenan y gestionan información, la cual es vital para la toma de decisiones, ya sea en los servicios o actividades que tiene la organización. De ahí que, todas estas diligencias se encuentran documentadas, donde el mayor

[35] WhatsApp: es el nombre de una aplicación que permite enviar y recibir mensajes instantáneos a través de un teléfono móvil (celular). ... Además, se utiliza la palabra “app” para referirse a una “application” (es decir, a una aplicación).

fragmento de esta información está plasmado en documentos físicos como digitales, que cumplen una función probatoria, de respaldo, representación, y de factor muy vital e importante para la entidad. En consecuencia, la filtración de esta información daña en gran manera a la organización o Estado, vulnerando la información confidencial, clasificada o estratégica. De forma que, estas grandes filtraciones pueden ser comprendidas con la infiltración hacia la organización para el robo de información sin importar en el soporte en el que se encuentre, un acto de esta manera afecta directamente en los intereses de la organización, ya sea esto de carácter económico, en temas de confiabilidad, y asuntos legales actuales.

De estas evidencias, cabe considerar el ejemplo de filtración de información sufrido por el Estado Boliviano, que hace mención a una injerencia política de parte de Estados Unidos, denominándolo, el caso wikileaks[36] por lo siguiente:

> *Ya sea diplomacia moderna o capacidad expedicionaria civil, los cables de Wikileaks mostraron hasta donde llega la pericia de los funcionarios norteamericanos para conocer hasta los más íntimos detalles de la política interna de un país. Dichos cables dieron lugar a una serie de análisis periodísticos en la región sobre, entre otras cosas: la veracidad de su contenido, lo que revelan, los objetivos de la embajada y sus mecanismos para obtener información. (Torres Gorena, Suarez Mamani, Telleria Escobar, & Merida Aguilar, 2016, p. 153)*

En consecuencia, muchos Estados, entidades o individuos intentan aprovechar la vulnerabilidad en la información que tienen muchas organizaciones, más aún cuando estas no comprenden la importancia de la misma. En efecto, es necesario implementar una mayor

[36] Wikileaks: es una organización mediática internacional sin ánimo de lucro, que publica a través de su sitio web informes anónimos y documentos filtrados con contenido sensible en materia de interés público, preservando el anonimato de sus fuentes.

conciencia de seguridad y categoría de la información en las organizaciones, y directamente más en los funcionarios o trabajadores que se encargan de gestionarla.

Siendo las cosas así, resulta claro, comprender el aprovechamiento de las tecnologías de la información y comunicación para la aplicación de servicios en las organizaciones, siendo un punto donde el cual se concentra la participación de una sociedad y un Estado u organización. Es decir, el fortalecimiento institucional, se desarrolla gracias a la combinación de la tecnología y la gestión, que apoya en las operaciones y servicios. A saber, que muchos de estos aplican para su expansión el uso de servicios digitales[37], lo cual proporciona muchos beneficios como perjuicios, cuando no se la administra de manera correcta. En efecto, es evidente la necesidad de proporcionar medidas de seguridad en los servicios, ante la sensibilidad que puedan sufrir.

En este sentido se comprende, las posibles amenazas y vulnerabilidades que están expuestas la información que tiene valor para la organización, o activo de información, es dado comúnmente por la inexistencia de eficiencia en la identificación y control hacia estos activos de información. Cabe señalar, que los activos de información son aquella información de gran valor para una organización, estas pueden estar conglomeradas en distintos soportes, como documentos digitales o impresos. De ahí que, toda organización cuenta con el almacenamiento y gestión de su información en sus archivos, ya sea estos que contemplen la característica de un archivo de gestión[38], archivo central[39], archivo intermedio[40] u archivo histórico[41]. Por consiguiente, la

[37] Servicios digitales: Cuando se habla que un objeto o un servicio es digital, se está haciendo referencia a que el mismo se establece a partir del envío discontinuo o discreto de datos.

[38] Archivo de gestión: gestión documental y el archivo de documentos todo ello pensado en las necesidades de los procesos de las empresas. Definición de Gestión Documental: La Gestión Documental es la captura, almacenamiento y recuperación de documentos.

[39] Archivo central: En el que se agrupan documentos transferidos por los distintos archivos de gestión de la entidad respectiva, cuya consulta no es tan frecuente pero que siguen teniendo vigencia y son objeto de consulta por las propias oficinas y particulares en general.

información vital de una organización queda plasmada en documentación impresa, que se encuentra en los archivos de las organizaciones.

Estos activos puedes ser identificados desde un solo documento impreso, hasta un fondo documental, en efecto, es necesario comprender la necesidad de priorizar la seguridad en los archivos, ya que estos almacenan gran parte de los activos de información de una organización.

De este modo, los datos organizados que están relacionados entre sí, cumplen la meta de ser recolectados y utilizados por el sistema de información[42] de una organización, los cuales permiten un rápido acceso. De ahí que, cada uno de estos elementos que componen a la base de datos[43], guarda en sí parte de información sobre cada elemento como, por ejemplo: datos informáticos[44], datos registrados, inventarios[45], etc.

En todo caso, la imagen de la entidad es un factor muy importante donde la información y datos juegan un papel crucial, por ser responsables del prestigio que presenta la organización en el manejo de la información, autentificación[46], difusión, accesibilidad de la información. De modo que, esto es percibido de la siguiente manera: “La seguridad de la información es un

---

[40] Archivo intermedio: archivo cuya función es la gestión de los documentos transferidos desde los archivos centrales hasta su eliminación o transferencia a un archivo histórico para su conservación definitiva

[41] Archivo histórico: El archivo histórico es aquel al cual se transfiere la documentación del archivo central o del archivo de gestión que, por decisión del correspondiente comité de archivo, debe conservarse permanentemente, dado el valor que adquiere para la investigación, la ciencia y la cultura. También puede conservar documentos históricos recibidos por donación, depósito voluntario, adquisición o por expropiación.

[42] Sistema de información: es un conjunto de datos que interactúan entre sí con un fin común. En informática, los sistemas de información ayudan a administrar, recolectar, recuperar, procesar, almacenar y distribuir información relevante para los procesos fundamentales y las particularidades de cada organización.

[43] Base de datos: Una base de datos es un “almacén” que nos permite guardar grandes cantidades de información de forma organizada para que luego podamos encontrar y utilizar fácilmente.

[44] Datos informáticos: Un dato es una representación simbólica (numérica, alfabética, algorítmica, espacial, etc.) de un atributo o variable cuantitativa o cualitativa. Los datos describen hechos empíricos, sucesos y entidades.

[45] Inventarios: Lista ordenada de bienes y demás cosas valorables que pertenecen a una persona, empresa o institución.

[46] Autenticación: Procedimiento informático que permite asegurar que un usuario de un sitio web u otro servicio similar es auténtico o quien dice ser.

aspecto crítico para evitar la mala imagen que produce una empresa incapaz de contener fugas de datos[47] estratégicos" (Redacción de Capital Humano, 2012, p. 57). Por lo tanto, las organizaciones deben tomar medidas cada vez mejores ante las vulnerabilidades de la seguridad de la información y protección de datos personales, en una siglo cada vez mejor conectado gracias al Internet.

En todo caso, los daños económicos, ante un mercado que eleva más intereses por la información, no solo por personas individuales, sino hasta estados que se interesan en el aprovechamiento de la misma, las cuales son muy alarmantes. La existencia de la comercialización de los datos en sus diferentes tipologías y características, afecta no solo en la vulnerabilidad e integridad de las organizaciones, sino directamente a los datos de las personas. Por lo tanto, el propio individuo o grupo de personas son quienes tienen la potestad de elegir en que organización confiar sus datos (Candid, 2016). En definitiva, constantemente se comprenden los beneficios del uso indebido que se hace de los datos personales, así lo ejemplifica el siguiente cuadro:

MERCADO CLANDESTINO DE LOS DATOS PERSONALES	
Pasaportes reales escaneados que pueden ser utilizados con fines de robos de identidad	$1 a $2 Dólares

[47] Fuga de datos: la fuga de información o fuga de datos es la liberación deliberada o involuntaria de información confidencial o sensible, a un medio o a personas que no deberían conocerla.

Cuentas de juegos en internet que pueden llevar a obtener artículos virtuales valiosos	$12 a $3,500 Dólares
Malware[48] personalizado para robar Bitcoins[49], remplazando carteras en la memoria	No definido
1,000 seguidores en las redes sociales	$2 a $12 Dólares
Cuentas en la Nube[50] robadas para hospedar un servidor de comando y control (C&C)	$7 a $8 Dólares
Enviar Spam[51] a 1 millón de direcciones de correo electrónico verificadas	$70 a $150 Dólares
Registrar y activar la tarjeta SIM [52]de un teléfono móvil ruso	$100 Dólares

Cuadro 1 Mercado cland estino de los datos personales

[48] Malware: Un código malicioso "malware" es cualquier tipo de programa desarrollado para causar daños o introducirse de forma no autorizada en algún sistema informático.

[49] Bitcoins: moneda criptográfica.

[50] Nube: base de datos disponible en la red o internet.

[51] Spam: Los mensajes de correo electrónico con publicidad no solicitada por el destinatario constituyen lo que se ha dado en llamar "correo basura", "junk-mail" o "spam".

[52] Tarjeta SIM: acrónimo en inglés de subscriber identity module, en español módulo de identificación de abonado) es una tarjeta inteligente desmontable usada en teléfonos móviles y módems HSPA o LTE que se conectan al dispositivo por medio de una ranura lectora o lector SIM.

Fuente: en base a (Candid, 2016)

Si bien es cierto, que el interés económico no solo afecta a los datos personales de las personas, sino también a los datos más valiosos de una entidad, que son un factor estratégico en las organizaciones. El valor económico del daño sería considerado fuertemente por el país donde la organización se encuentre, imponiendo fuertes multas o sanciones. Tal es el caso de la Agencia Española de Protección de Datos (AEPD[53]), La cual da a conocer las sanciones e infracciones, "Las infracciones se califican como leves, o muy graves, estableciendo multas que van desde los 900 a los 600.000 euros" (Miguel Pérez, 2015, p. 213). En efecto, esto requiere y obliga a las organizaciones a estar preparadas para afrontar estas amenazas.

[53] AEPD: Agencia española de protección de datos. https://www.aepd.es/

1.2.1 Identificación del problema

Cuadro 2 Elaboración del problema

HECHO	CONSECUENCIAS
Inadecuada seguridad de la información.	**1.- Mala protección de los datos personales.**
	2.- Filtración de Información.
	3.- Daño a la sensibilidad de los servicios de información.
	4.- Bases de datos sensibles a ataques cibernéticos.
	5.- Daño a la imagen de la organización.
	6.- Daños económicos.
	7.- Problemas legales.

Fuente: elaboración propia

1.2.3 Formulación del problema

¿Cuál es la seguridad de la información en la protección de los datos personales de la firma digital de la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB) En la gestión 2017?

Por lo que se plantea la formulación del problema, bajo las siguientes interrogantes:

¿Cuáles son las medidas de protección de los datos personales?

¿Cuáles son las causas de la filtración documental y/o filtración de la información en una organización?

¿Cuáles son las medidas de sensibilidad en los servicios de información?

¿Cuáles son las medidas de seguridad de base de datos que son sensibles a ataques cibernéticos?

¿Cuál es la importancia de la imagen de la organización?

¿Cuál es el financiamiento para la seguridad de la información?

1.3 Objetivos

El enfoque de la investigación da a conocer los siguientes objetivos:

1.3.1 Objetivo general

Identificar la seguridad de la información para la protección de los datos personales en la firma digital de la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB), que permitan mejoras adaptables en seguridad de la información y protección de datos personales hacia la sociedad de la información boliviana, proporcionando estadísticas que permitan establecer políticas, controles y diseños en temas de seguridad de la información y protección de datos personales.

1.3.2 Objetivos específicos

- Describir las medidas de protección de los datos personales en la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia.
- Determinar las causas que originan filtración de la información en la sociedad de la información en Bolivia.
- Analizar los servicios de información sensibles para la sociedad de la información en Bolivia.
- Diagnosticar políticas de protección de los activos de información.

- Identificar la sensibilidad de ataques cibernéticos hacia la sociedad de la información en Bolivia.
- Examinar riesgos que dañen la imagen de las entidades del Estado ante la sociedad de la información en Bolivia.
- Analizar la actividad económica de la sociedad de la información en Bolivia.
- Mencionar los posibles problemas legales.
- Describir la diligencia de la sociedad de la información en Bolivia respecto a los trámites.

1.4 Hipótesis

A partir de los datos adquiridos se obtendrá una base para dar curso a la investigación que presenta la siguiente conjetura:

*"*La inadecuada seguridad de la información, repercute en la mala protección de los datos personales de la Sociedad de la Información en Bolivia*"*

1.5 Variables

El estudio determina que, para la identificación de una óptima seguridad de la información en la protección de los datos personales, se considerarán las siguientes variables:

1.5.1 variable independiente

Seguridad de la Información.

1.5.2 Variable dependiente

Protección de los Datos Personales

1.5.3 Variable interviniente

Firma Digital

1.5.4 Variable espacial

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

1.5.5 Variable temporal

Gestión 2017

1.5.6 Objeto de estudio

Sociedad de la Información en Bolivia

1.5.6 Tipo de estudio

Descriptivo

1.6 Operacionalización de variables

Cuadro 3 Operacionalización de variables

VARIABLE	CONCEPTO	DIMENSION	INDICADOR	Pregunta / actividad	ESCALA / FORMULA	FUENTES	INSTRUMENTO
Seguridad de la información	Es un proceso mediante el cual se obtiene, despliega o utiliza los recursos de información necesarios para la Seguridad de la información, garantizando la protección de la integridad, disponibilidad y confidencialidad de la información	Confidencialidad	Nivel de acceso	Nivel de confidencialidad	Publico	Personal	Entrevista
					Restringido		
				¿La entidad ha implementado lineamientos, normas y/o estándares para proteger al información personal y privada de los ciudadanos que utilicen sus servicios?	Si		
					No		
		Integridad	Integridad de la información	¿Considera que la información conserva su integridad?	Totalmente en desacuerdo	Personal	Entrevista
					En desacuerdo		
					Indiferente		
					De acuerdo		
					Totalmente de acuerdo		
				¿La información conserva su integridad?	Si		
					No		
				¿La entidad ha implementado lineamientos contra modificaciones o pérdida accidental de información?	Si		
					No		
				¿La entidad ha implementado lineamientos, normas y/o estándares para recuperar información en caso de modificaciones o pérdida accidental de información?	Si		
					No		
			Integridad de los sistemas	¿Considera que los sistemas protegen la integridad de la información?	Totalmente en desacuerdo	Personal	Entrevista
					En desacuerdo		
					Indiferente		
					De acuerdo		

					Totalmente de acuerdo		
		Disponibilidad	Acceso a la Información	¿La información está siempre a disposición?	Totalmente en desacuerdo En desacuerdo Indiferente	Personal	Entrevista
Protección de Datos Personales	Es un proceso mediante el cual se garantiza la protección de la utilización, tratamiento y uso de los datos personales	Organización	Activos de información	Electrónico Físico Magnético Informático	Si	Responsables	Entrevista
			Archivos	Archivo de gestión Archivo central Archivo intermedio Archivo histórico	No		
			Bases de datos	Nube			
		Administración-Usuarios	Uso y disposición de datos	Calidad de los datos Derecho de información en la recogida de datos Consentimiento del afectado datos especialmente protegidos Datos relativos a la salud Seguridad de los datos Deber secreto Comunicación de datos Acceso a los datos por cuenta de terceros		Personal	Entrevista
		Económico	Financiamiento en protección de los datos	Presupuesto anual Ningún presupuesto	Aplica No aplica	Responsables	Entrevista

Fuente: Elaboración Propia

Cuadro 4 Información recolectada para el estudio

INFORMACIÓN RECOLECTADA PARA EL ESTUDIO		
TIPO DE INFORMACIÓN	**ENTIDAD**	**DETALLE**
Encuesta nacional de opinión sobre TIC	AGETIC	El objetivo de la encuesta nacional de opinión sobre tic fue obtener información representativa a nivel nacional, urbano/ rural y departamental, sobre el acceso y usos de tecnologías de información y comunicación (tic), servicios de gobierno electrónico y equipamiento de la población internauta de 14 o más años de edad.
Grupo de trabajo de seguridad	CTIC	El grupo de trabajo de seguridad del consejo para las tecnologías de información y comunicación del estado plurinacional de Bolivia – CTIC-EPB elaborará estándares de seguridad y protocolos de prevención y contingencia de incidentes informáticos que permitan proteger y resguardar los sistemas y la información del estado, y brindar apoyo a la ciudadanía.
		Lineamientos para la elaboración e implementación de los planes institucionales de seguridad de la información de las entidades del sector público
		Controles de seguridad de la información
		Guía para la metodología de análisis de riesgos
		Guía para la gestión de incidentes de seguridad de la información
Clasificación de la información	ASFI	ASFI, es una institución de derecho público y de duración indefinida, con personalidad jurídica, patrimonio propio y autonomía de gestión administrativa, financiera, legal y técnica, con jurisdicción, competencia y estructura de alcance nacional, bajo tuición del Ministerio de Economía y Finanzas Públicas, y sujeta a control social.
Clasificación de la información en instituciones públicas	AE	Autoridad de Fiscalización y Control Social de Electricidad
		Políticas de tecnologías de información (TI) – AE
		Reglamento n° 3 de responsables de clasificación, acceso y almacenamiento de información
Seguridad de la información	BCB	Banco Central de Bolivia
		Análisis de riesgo, clasificación de la información, basado en el criterio de riesgo
Políticas	ADSIB	Agencia para el Desarrollo de la Sociedad de la Información en Bolivia
		Políticas de certificación (CP)
		Declaración de prácticas de certificación (CPS)
		Políticas de seguridad y procedimientos internos

Fuente: Elaboración propia

1.7 Justificación

La presente investigación tiene como objetivo determinar la seguridad de la información para la protección de los datos personales en la firma digital de la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB), para: plantear mejoras adaptables a la sociedad de la información boliviana, proporcionando parámetros para excelentes políticas, controles y diseños en temas de seguridad. Por lo tanto, es indispensable identificar el comportamiento de la población boliviana internauta mayor de catorce años para adelante, que genere una mayor comprensión del uso de tecnologías de la información y comunicación a nivel nacional.

De esta manera, los resultados obtenidos brindarán conocimiento sobre el estado actual de la sociedad de la información en Bolivia. De ahí que, la agencia responsable para su desarrollo realizará mejores procesos para optar políticas de seguridad para esta sociedad, así como para la firma digital. De modo que, una sociedad que comprenda la importancia de la seguridad de la información y protección de los datos personales, permitirá un mejor control de su información y la información que administra, siendo esto de gran beneficio y garantía para el país, ante vulnerabilidades, ataques y robo de información, filtración, provenientes de otros Estados interesados, empresas de espionaje, grupos de hacker y personas perniciosas.

La información que obtienen las entidades u órganos del Estado, es útil, por ello deben analizar, y vislumbrar la importancia de sus servicios en torno a la sociedad que crece y se desarrolla alrededor de la información, así como las diligencias en seguridad de la información y protección de datos personales, puesto que, gran parte de estas entidades son vulnerables a robo de información, filtración de la misma y mala gestión e identificación de los activos de información con los que cuenta. Por tanto, se conjetura que la fragilidad de esta es por la falta de

perspicacia hacia la sociedad de la información, donde en la misma también forman parte los funcionarios o personal, clientes y usuarios que operan y utilizan sus servicios.

1.7.1 Importancia del estudio

El presente trabajo demuestra la relevancia científica, relevancia humana y relevancia contemporánea, desarrollada en los siguientes párrafos:

Relevancia científica

La información de un Estado o población, es esencial para el desarrollo social, cultural y económico de una sociedad ya que su estudio contribuye a la mejora de la calidad de vida de la misma, por eso, la información debe ser analizada y comprendida para evitar diferentes vulnerabilidades que la amenazan. El presente trabajo se concentra en el análisis de la sociedad que genera y gestiona la información, así como su exposición con el uso de las nuevas tecnologías de la información y comunicación, desde distintos enfoques y perspectivas de seguridad, que abarcan: las organizaciones internacionales y las políticas de diferentes Estados, al momento de tratar la información de sus organismos y la información de su población.

Así mismo, tiene como objetivo dar a conocer los enfoques internacionales y nacionales para la seguridad de la información, normativa internacional y principios para la protección de datos personales, con la incorporación de datos para la adecuación en las políticas internas y de adecuación en el desarrollo de servicios, para así alcanzar una mejor gestión de la información y la aplicación de una firma digital, interoperabilidad y gobierno electrónico, lo cual permitirá una mejor visibilidad y difusión de la información ante la sociedad de la información, aplicada en cualquier órgano Institucional, sistema de información, centro de información, centro de documentación, archivo, museo o biblioteca, en relación a la protección de información. Por lo

cual, el estudio analiza las similitudes de la sociedad de la información en Bolivia y seguridad para su mejor desarrollo.

Relevancia humana

Las entidades del Estado, empresas, organizaciones y personas individuales, deben tomar importancia de la información que administran para una buena gestión de la información. Así mismo, es indispensable entender las medidas de seguridad que les proporciona, no solo para una buena imagen de la entidad, sino también, para generar una confianza de seguridad y respaldo para la organización, país y sociedad en la que brinda sus servicios. De esta manera, ser capaz de generar la aportación de comprensión en confidencialidad, integridad, disponibilidad de la información, y la importancia de los datos concernientes a las personas individuales. Reconociendo, así como una sociedad que crece alrededor de la información y comprende la categoría de la seguridad y protección de la misma.

Ya en la gestión 2018, se ha impulsado el deber de protección de los datos personales en países de la Unión Europea, donde todos los países miembros y países que cooperen con los mismos deben sujetarse a la regulación establecida por el Reglamento General de Protección de Datos, determinados por los Estados miembros. Por tanto, Bolivia en su historia de cooperación y coordinación con los países miembros de la Unión Europea, tiene la necesidad de adecuar los tratamientos de protección de datos personales exigidos por estos países miembros.

Relevancia contemporánea

Los profesionales de la información, adquieren la obligación de corresponder a los nuevos requerimientos de la gestión de la información, comenzando con el avance de las tecnologías de información y comunicación, las nuevas políticas del Estado como: Gobierno Electrónico y

Ciudadanía Digital, donde ellos van a necesitar cumplir requisitos actuales para la gestión de la información.

Cabe señalar, que trabajar en la era digital para la información, implica conocer el funcionamiento de la tecnología, según las tendencias de prácticas y usos digitales para la información, de modo que, es necesario atender los aspectos de protección hacia la misma. Más aun, cuando Bolivia presenta la siguiente característica:

> *Bolivia abraza una tendencia una vez aparece la necesidad y a escala regional estamos muy atrasados en temas de protección de datos", señala el especialista en seguridad cibernética Willians Duabyakosky, quien agrega que son pocas las compañías que trabajan con metodologías y estándares internacionales y que el DPD es una profesión riesgosa y cara de pagar*. (El Deber, 2018)

La afirmación anterior, exhibe la realidad del tratamiento de la información de datos personales de la población en Bolivia, así como la necesidad de implementarla en la actualidad y cumplir con la tendencia en el tratamiento de datos personales a escalas internacionales.

Visto desde la perspectiva, de los profesionales de la información, el desarrollar nuevas habilidades para la gestión de la información. Permite, asumir los nuevos roles en servicios de la información, donde los mismos deben estar al tanto de las necesidades de sus instituciones, y evolución de las tecnologías

> *La gestión de datos de investigación aparece como una de las tendencias clave en el trabajo que desarrollará el bibliotecario universitario del siglo XXI; si bien, al tratarse de un área emergente y en continua evolución, aún no están definidas las habilidades y competencias del bibliotecario de datos, en general, la tarea del bibliotecario de datos implica una amplia comunidad de bibliotecarios con diversas capacidades, antecedentes y responsabilidades profesionales.* (Federer, 2018)

Tal como se puede apreciar, la necesidad actual del siglo XXI, implica una gestión de la información adecuada a la evolución actual de las tecnologías de la información y comunicación, donde los profesionales que gestionan la información deben tener buena disposición para ello.

1.8 Marco referencial

Antecedentes de la Agencia para el Desarrollo de la Sociedad de la información en Bolivia (ADSIB)

La Agencia para el Desarrollo de la Sociedad de la Información en Bolivia ADSIB, es una entidad descentralizada, que se encuentra en coordinación con la Vicepresidencia del Estado Plurinacional de Bolivia, la cual fue creada con independencia en gestión administrativa y técnica, mediante el Decreto Supremo N. 26553, de fecha 19 de marzo de 2002.

Misión

Desarrollar políticas, estrategias y acciones para brindar servicios fiables, innovadores y de calidad en el ámbito de las Tecnologías de la Información y la Comunicación, avanzando en la soberanía tecnológica y la inclusión de la población en el uso de la información y la tecnología.

Visión

Consolidarse como una institución líder en los procesos de desarrollo tecnológico y en la prestación de servicios en el ámbito de las Tecnologías de la Información y la Comunicación para satisfacer las necesidades de la población, avanzando hacia la soberanía tecnológica.

Según la normativa vigente tiene las siguientes funciones:

- Administrar el Servicio de Registro de Dominios .bo (https://nic.bo/), brindando asesoramiento personalizado en procesos de registro y renovación de dominios ".bo".

- Administrar el Servicio de Certificación Digital, como Entidad Certificadora Pública emite certificados que permiten firmar digitalmente documentos válidos en el Estado Plurinacional de Bolivia (https://firmadigital.bo/)
- Administrar el Repositorio Estatal de Software Libre donde se registra, socializa, preserva y custodia los sistemas desarrollados en el estado (https://softwarelibre.gob.bo/)
- Brindar la conformidad u oposición para la adquisición o donación, ampliación y/o renovación de Licencias de Software Propietario en entidades públicas.
- Miembro activo del Comité Plurinacional de Tecnologías de Información y Comunicación – COPLUTIC (https://coplutic.gob.bo/).

1.9 Marco normativo

Organización Internacional para la Normalización (ISO)

Es una red mundial que identifica que normas internacionales son requeridas por el comercio, los gobiernos y la sociedad; las desarrolla conjuntamente con los sectores que las van a utilizar; las adopta por medio de procedimientos transparentes basados en contribuciones nacionales proveniente de múltiples partes interesadas; y las ofrece para ser utilizadas a nivel mundial.

Estándar ISO/IEC 27001

La International Organization for Standardization (ISO) y la Internacional Electrotechnical Comission (IEC) forma, un sistema que se encarga de realizar normalizaciones a nivel mundial, donde los miembros de diferentes nacionalidades participan en el desarrollo de las normas. Así también, las organizaciones grandes y pequeñas tienen la posibilidad de optar de manera parcial o

total los controles de la ISO/IEC 27001, conforme a sus necesidades. Por tanto, la norma está orientada a la Seguridad de la Información empleada en una empresa u organización.

Consideramos que existen muchas normas a nivel mundial para gestionar la seguridad de la información en las empresas y organizaciones. En ese caso, es necesario considerar algunos de ellos, como el artículo del documento en línea de En Portada (2006) que detalla lo siguiente:

- Referenciales nacionales e internacionales específicos.
- Normas creadas por agentes privados para la protección de datos.
- UNE 71502
- ISO / IEC 17799
- BS 7799
- BS 15000
- ISO 27001 (p.12)

Las características de las normas velan por el interés de clientes, proveedores, empleados, accionistas, administradores entre otros, pero el dominio debe ser compatible con otras normas. En consecuencia, se debe detallar cada una de estas, comprendiendo sus características y evolución.

Cuadro 5 Evolución de las normativas de la seguridad de la información hasta el 2005

AÑO	NORMA
1995	La primera norma aprobada oficial mente fue la (BS 7799:95) y nace como un código de buenas prácticas para la gestión de seguridad de la información.

1998	Se publica la norma BS 7799-2, en la que recogen especificaciones para la gestión de seguridad de la información y se exponen requerimientos certificables por primera vez.
1999	Se expone la segunda edición, en la que se añade "e-commence" al alcance de la norma. En aquella época, la Organización Internacional de Normalización (ISO) comienza a interesarse ya por los trabajos publicados por el instituto inglés.
2000	ISO aprueba la norma ISO 17799 Parte 1, que es el Código de Práctica para los requisitos de gestión de seguridad de la información (no certificable). Esta norma está formada por un conjunto completo de controles que confirman las buenas prácticas de seguridad de la información, y que pueden ser aplicadas por toda organización con independencia de su tamaño.
2002	Se realiza la segunda revisión y se hace certificable la norma BS (BS 7799-2:2002), con el fin de armonizarla con otras normas de gestión tales como la ISO 9001:2000 y la ISO 14001:1996, así como los principios de la Organización para la Cooperación y el Desarrollo Económico (OCDE).
2002	Se publica la norma IUNE-EN ISO/IEC 17799/ 1:2002, en España.
2005	Se publica la norma ISO 27001, norma certificable y que remplazara a la actual BS 7799-2

Fuente: (En Portada, 2006)

Con respecto a la implementación de la norma ISO, Flores Barrios, Soto del Angel, Camacho Diaz, & Barrera Reyes, (2011) recalcan su importancia señalando que:

En la actualidad, la ISO/IEC 27001 es una norma apropiada para cualquier organización, grande o pequeña, de cualquier país del mundo. La norma es particularmente interesante si la protección de la

información es crítica, como en finanzas, sanidad sector público y tecnología de la información (TI)[54] *(p.45).*

Sobre la base de las ideas expuestas, queda precisa la normativa en tema de seguridad de la información, de forma que, esta norma es aplicada al desarrollo de las tecnologías de la información y comunicación, tal es el caso de la ISO 27000, que expone en sus diferentes partes en lo siguiente:

Cuadro 6 Relación de las normas de la serie ISO 27000

NORMAS	TEMATICA
ISO 27000	Gestión de la Seguridad de la Información
ISO 27001	Especificaciones para un SGSI (Certificable)
ISO 27002	Código de Buenas Practicas
ISO 27003	Guía de implantación de un SGSI
ISO 27004	Sistema de métricas e Indicadores
ISO 27005	guía de Análisis y Gestión de Riesgos
ISO 27006	Especificaciones para Organismos Certificadores del SGSI
ISO 27007	Gua para auditar el SGSI
ISO/IEC TR 27008	Guía de Auditoría de los controles seleccionados en el marco de implantación de un SGSI
ISO/IEC 27010	Guía para la gestión de la seguridad de la información cuando se comparte entre sectores u organizaciones.

[54] TI: tecnologías de la información

27002 (Controles de Seguridad de la Información	Es un código de buenas prácticas que recomienda los controles de seguridad a implementar que ayudan a cumplir los objetivos de la seguridad de la información relativos a gestionar los riesgos que incidan sobre la confidencialidad, integridad y disponibilidad de la información.
27014 (Gobierno de Seguridad de la información)	Provee una guía para implementar un gobierno de seguridad de la información, el cual garantiza la alineación con las estrategias y objetivos de la organización generando valor y responsabilidad.
27031 (Continuidad del Negocio)	Describe los conceptos y guías para garantizar la continuidad del negocio en caso de incidentes de seguridad internos o externos.
27033 (Tecnologías de la información - Técnicas de seguridad - Seguridad de red	Guía detallada sobre la aplicación de los controles de seguridad de red que se introducen en la norma ISO/IEC 27002. Se aplica a la seguridad de los dispositivos conectados en red y la gestión de su seguridad, aplicaciones de red/servicios y los usuarios de la red, además de seguridad de la información que se transfiere a través de enlaces de comunicaciones.

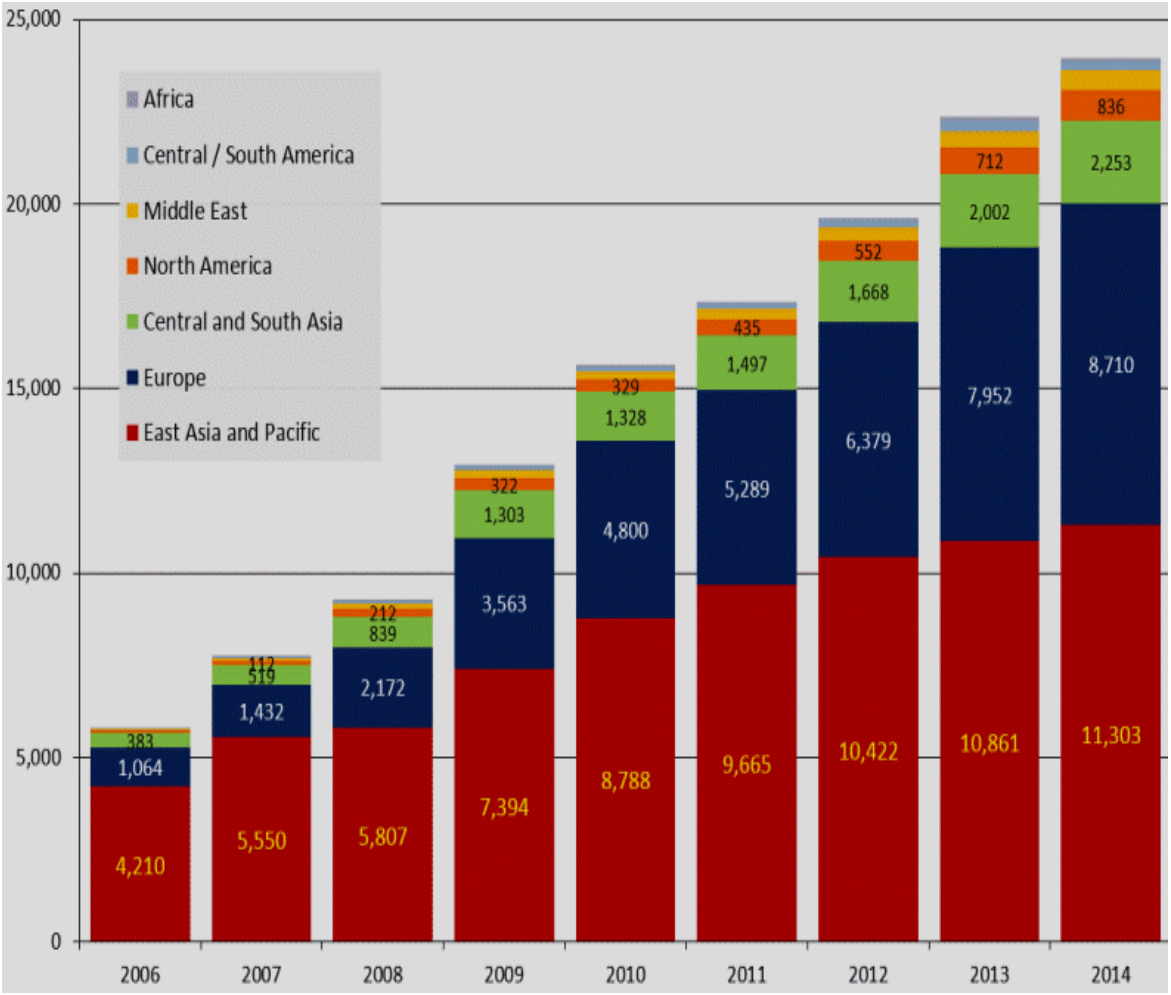
Fuente: Elaboración propia en base a Universidad Nacional Abierta a Distancia y Agetic Bolivia.

La seguridad de la información era empleada en pocas empresas y organizaciones a lo largo de la historia, conforme a las necesidades de la época se desarrollaba una forma de seguridad para la información. En efecto, las buenas prácticas en las organizaciones para una buena gestión eran necesarias.

> *La ISO 27001 proporciona requisitos para un SGSI que permitirán a la organización establecer, implantar, operar, supervisar o en términos de norma "monitorizar", revisar, mantener y mejorar un SGSI documentado en el contexto de la actividad de la organización, teniendo en cuenta sus problemáticas y riesgos de seguridad o de otro tipo, intrínsecos a su negocio. (En Portada, 2006, p. 14)*

La ISO/27001, se ha convertido en un referente a nivel mundial, considerándoselas como la principal norma en seguridad de la información. Muchas empresas han certificado bajo su estándar, por lo que la siguiente figura (1) nos permite observar la cantidad de empresas que consideraron este estándar:

Figura 1 Empresas certificadas en el mundo con la ISO/IEC 27001



Fuente: 1 Extraído del aporte del grupo de Seguridad de la Agetic Bolivia en base a ISECT, 2016

Como podemos apreciar en la figura 1 la demanda creciente en los continentes que cuentan con empresas certificadas con la ISO/IEC 27001 es cada vez mayor, por ello es importante su aplicación.

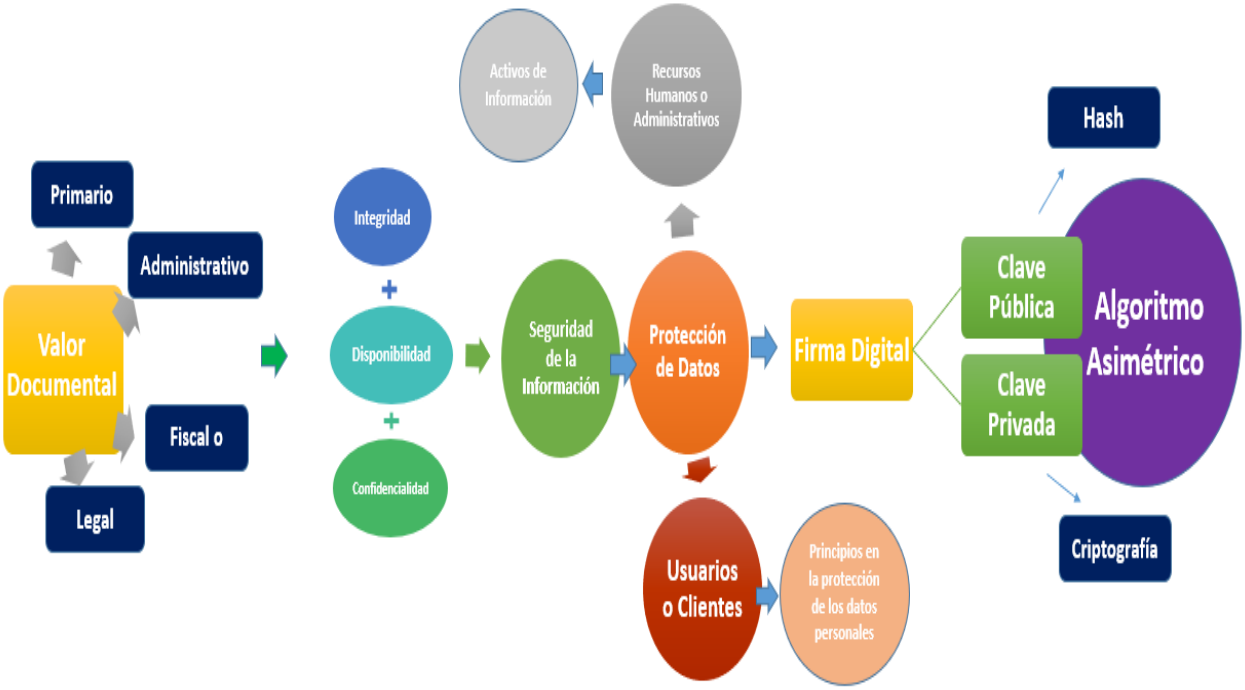
CAPITULO II - MARCO TEÓRICO

2.1 Seguridad de la información

La presente investigación se centrará en la seguridad de la información, donde es de gran importancia en las instituciones.

La seguridad de la información es un proceso mediante el cual se controla, despliega o utilizan los recursos de información necesarios para la entidad, garantizando la protección de la integridad, disponibilidad y confidencialidad de la información que genera. El gran avance de las tecnologías de la información y comunicación alcanza a ámbitos mundiales en tiempo real gracias al uso del internet.

Figura 2 Seguridad de la Información, Protección de Datos y Firma Digital en una Sociedad de la Información



Fuente: Elaboración propia

Es por ello, que el desarrollo de redes de información a nivel mundial permite que la comunicación sea más fluida, y de tránsito más rápido. Esta incursión universal de internet y redes, son el soporte de todos los servicios en la actualidad, el desplazamiento del internet permite a las empresas estar más cerca de los usuarios y clientes hacia las empresas, de este modo, se comprende que el uso de la información en la relación cliente y empresa debe tener un tratamiento muy cuidadoso, pues la información usada por estos, es de vital importancia, pues la mínima alteración llegaría a producir muchos efectos negativos entre ambos involucrados.

Al respecto, claramente se identifica que "la seguridad de la información es, por tanto, un activo[55] que tiene valor para los procesos de negocio de la empresa" (Miguel Pérez, 2015, p. 236), esto quiere decir que es de carácter prioritario para las empresas, y de principal importancia.

Entonces, al pasar el tiempo fue clara su importancia, ya que es un problema que va afligiendo a muchas empresas y entidades. Además, la seguridad de la información es la "preservación de confidencialidad, integridad y disponibilidad de la información". Según el (Instituto Boliviano de Normalización y Calidad [IBNORCA] 2010, p. 5).

De esta manera, gracias al uso de las nuevas tecnologías se obtuvo más alcances y/o accesos, así como el esparcimiento de su información. Su uso, forma parte muy importante dentro de las funciones administrativas de las empresas y entidades gubernamentales, exponiéndose por ello a ser más atacadas.

[55] Activo: cualquier bien que tiene valor para la organización.

Por otra parte, la identificación de la seguridad de la información, de instituciones como el FBI[56] nos señala que:

> *La incapacidad de acceder a los datos importantes de este tipo de organizaciones puede ser catastrófica en términos de pérdida de información confidencial o propietaria, interrupción de las operaciones regulares, pérdidas financieras incurridas para restaurar los sistemas y archivos y el daño potencial a la reputación de una organización. Las computadoras domésticas son tan susceptibles a los programas de rescate y la pérdida de acceso a artículos personales y a menudo insustituibles -incluyendo fotos familiares, videos y otros datos- puede ser devastador para los individuos también.* (Departamento Federal de Investigaciones [FBI], 2017)

Esto quiere decir, que el valor asignado a la información, como factor fundamental para una organización, es de vital importancia. Por ende, nos recomienda aplicar medidas de protección, controles y seguimiento. De tal manera, que se pueda activar una inversión o parte de un presupuesto que sea destinado netamente a la protección de la información, la cual, garantice las acciones estratégicas de aplicar confidencialidad, integridad y disponibilidad en una empresa.

> *Al ser la información el activo más valioso, éste requiere de una particular protección así como de inversión; pero por más que se invierta, siempre se estará expuesta ya que la consecución de la seguridad depende tanto de factores internos como externos, por lo que se necesita de una perfecta sincronización y es precisamente lo que no se logra. Sobre todo cuando existen y/o se han dejado vulnerabilidades en los sistemas que son aprovechadas por los delincuentes, lo cual permite que se organicen y creen organizaciones cibercriminales. (Najar Pacheco & Suárez Suárez, 2015, p. 12)*

---

[56] FBI: Departamento Federal de Investigaciones https://www.fbi.gov/

En resumidas cuentas, el uso de las nuevas tecnologías se ha vuelto un tema indispensable para cada empresa, ya que estas deben estar sujetas a los cambios y vulnerabilidades que presentan.

El Consejo Internacional de Archivos (CIA)[57] dentro del Código de Ética Profesional, menciona que:

> *Los archiveros deben velar por la protección de la privacidad de las personas físicas y jurídicas, así como la seguridad nacional, todo ello sin destruir información, especialmente en el caso de los documentos electrónicos donde es práctica habitual borrar o actualizar los datos. (Consejo Internacional de Archivos, 1996, p. 3)*

De igual manera, el IFLA[58] hace mención sobre *"*Los "registros esenciales" (documentos sin los cuales la institución y el organismo al que está adscrita no podrían funcionar) son obviamente los candidatos más importantes" (Federación Internacional de Asociaciones e Instituciones Bibliotecarias [IFLA], 2003, p. 59). De entenderlo, se convierte en un tema muy relevante para una empresa u organización, no solamente para su desarrollo, sino también para su supervivencia en el área global.

La importancia de la protección de la información, debe realizarse de manera correcta, porque las instituciones, tanto privadas como públicas son vulnerables a la manipulación de las mismas, lo que significa que el 85% de las grandes empresas son vulnerables así señala el informe de Especial directivos (2014). En este sentido, en algunas de sus manifestaciones destaca la

[57] CIA: Consejo Internacional de Archivos https://www.ica.org.com
[58] IFLA: International Federation of Library Associations and Institutions

necesidad de aumento de la sensibilización de la sociedad en materia de seguridad de la información.

- Asimismo, destaca que de acuerdo con la consultora tecnológica Necsia[59] que desarrolló un informe sobre la seguridad de la información e infraestructura tecnológica de las empresas españolas con el fin de detectar los principales peligros que estas tienen hoy en día, revela que el 15,5% de empresas realizaron un incremento en su presupuesto en el año 2014 para poder combatir los riesgos que aquejan a la seguridad de la información, tanto en las fugas de información, fraude y robo de datos. (p.5).

En efecto, resulta claro el aplicar un presupuesto en tema de seguridad de la información.

De esta forma deben señalarse los componentes más importantes identificados por parte de Especial Directivos (2014) que son:

- *Deficiente control de acceso a las aplicaciones: el 48% de los involucrados identificaron que, en su compañía, el acceso de los trabajadores a las aplicaciones debería contar con un mejor control.*
- *Existencia de vulnerabilidades web: el 47% de las empresas identifican vulnerabilidades web gracias al hacking ético[60] que permite accesos no permitidos a información importante y sensible de la compañía.*

[59] Necsia: Empresa especializada en Ciberseguridad y Transformación Digital. www.necsia.es

[60] Hacking Ético: La ética hacker es un conjunto de principios morales y filosóficos surgidos de, y aplicados a, las comunidades virtuales de hackers, aunque no son exclusivas de éste ámbito, ya que muchos de sus valores pueden aplicarse fuera del ámbito de la informática y al acto de hackear.

- *Falta de formación y concienciación: incrementar la formación y concienciación en relación a la seguridad de la información aplicado al personal interno, socios del negocio. El factor humano es de vital importancia para la prevención de ataques cibernéticos[61] avanzados.*
- *Proceso de gestión de incidentes de seguridad: la importante necesidad de mejorar ante un incidente de seguridad, respuesta identificada por un 44,6% de participantes interlocutores en el estudio.*
- *Existencia de cambios regulatorios: un 43% ha identificado la complejidad de adaptarse a los cambios regulatorios tanto normativos como legales en cada sector.*
- *Control de acceso a la red: un 42% de las empresas mencionan que están en riesgo por la falta de controles de acceso de usuarios internos y terceros, tales como proveedores e invitados a la red corporativa.*
- *Fuga de información: la fuga de datos es uno de los más importantes riesgos a los que se ve expuesta las compañías en la actualidad, así lo identifica el 41,3% de las empresas.*
- *Fraude y robo de información: un 43,3% dio razón de que existe una gran vulnerabilidad en los identificados filtros informativos, provocando el fraude y robo de la información.*
- *Falta de planificación de continuidad de negocio: un cambio significativo entre los miembros de la cúpula directiva de una compañía ocasionaría que sea estrictamente importante desarrollar una planificación para dar continuidad de negocio, según detalla el 32,5% de las empresas.*
- *Desarrollo de software: el desarrollo del uso de herramientas informáticas para mecanizar los procesos de negocio ha generado que el 39,8% de los encuestados identifique los aspectos de*

[61] Ataque Cibernético: Los ataques en grupo suelen ser hechos por bandas llamadas "piratas informáticos" que suelen atacar para causar daño, por buenas intenciones, por espionaje, para ganar dinero, entre otras. Los ataques suelen pasar en corporaciones.

seguridad de la información como aspecto importante en el ciclo de vida de desarrollo de software. (p 5-6)

Cabe recalcar que "la seguridad de la información comprende tres dimensiones principales: confidencialidad, disponibilidad e integridad". (Instituto Boliviano de normalizacion y calidad, 2010 [IBNORCA], p. 10). Debe señalarse, que estos principios dentro de la seguridad de la información adoptan medidas, políticas y documentos en relación a la protección del conjunto de datos.

Desde la perspectiva más general, la seguridad de la información es un proceso, mediante el cual se da la protección a la información y a sistemas de información, tanto en su acceso, uso, divulgación interrupción o destrucción no autorizada. Tal lo menciona el (Banco Central de Bolivia [BCB], 2017) en el siguiente ejemplo:

Figura 3 Seguridad y Protección de la Información

Fuente: Identificación de seguridad de la información del Banco Central de Bolivia (2017), expuesto por Cesar Roberto Cuenca Díaz en el grupo de seguridad conformado por la Agencia de Gobierno Electrónico y Tecnologías de la Información y Comunicación (AGETIC).

Dentro de este orden de ideas, la protección de la información abarca varios tipos de soportes, mencionados como: formato electrónico y no electrónico. En definitiva, como señala Voutssas m. & Barnard Amozorrutia (2014) la información interviene de "Un ensamble o conjunto organizado y coherente de datos procesados e interrelacionados que forman una unidad de significado más compleja que sus partes, con propósito de comunicarla en el espacio y el tiempo" (p. 133). De ahí que, las particularidades de estos dos formatos son de gran jerarquía, por ser complemento de las nuevas tecnologías de la información y comunicación.

Para el tratamiento de la información en el entorno de su evolución, es necesario percibir los distintos soportes en los que ésta se manifiesta. En efecto, se manifiesta en varios soportes dentro de una organización y esta se transmite con un carácter singular.

Por otra parte, la información electrónica es un ensamble o conjunto organizado de manera coherente asociado a las tecnologías y dispositivos que están asociados en el trabajo de corrientes eléctricas pequeñas a través de algún circuito o componente que son usados para la transmisión o procesamiento de los datos analógicos o digitales (Voutssas m. & Barnard Amozorrutia, 2014). Por ello, es necesario el uso de las tecnologías para su procesamiento y transmisión. En pocas palabras la información electrónica requiere del uso de las tecnologías de la información y comunicación.

La información en formatos no electrónicos, es identificada en soportes de medios analógicos[62], tal como se presenta el papel, pergamino, piedra, arcilla, película e incluso los antiguos medios magnéticos como ser cintas de audio y video, usadas para el almacenaje de datos

[62] Medio Analógico: Soporte físico, tal como papel, pergamino, piedra, arcilla, película o los antiguos tipos de cintas de audio y video magnéticas, usadas para almacenamiento de datos en forma analógica.

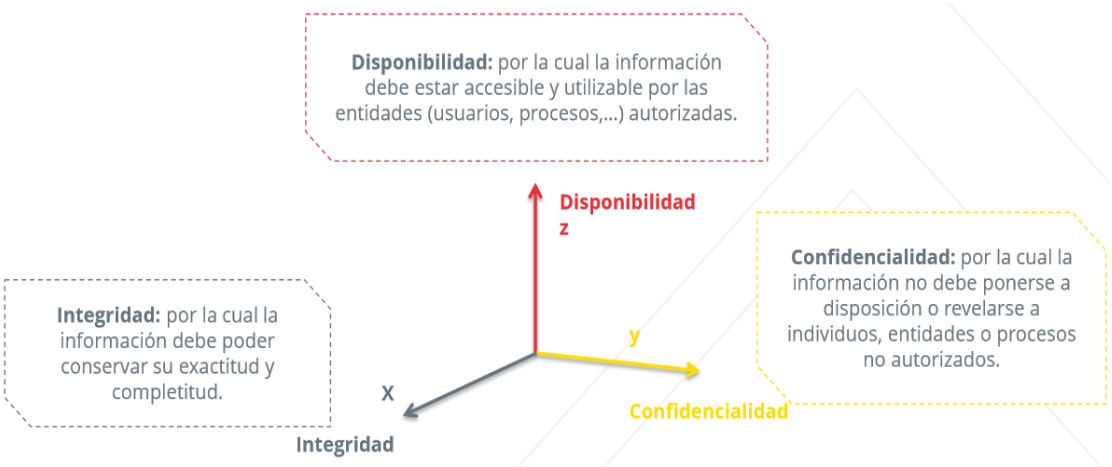
en forma analógica (Voutssas m. & Barnard Amozorrutia, 2014). Por ello, la información no electrónica cuenta con muchos distintivos en su tipo de soporte. Por consiguiente, los autores ya mencionados hacen descripción de la información en soporte de medio digital[63], que es el material físico de un medio digital, ya sea como ejemplo un disco compacto, DVD[64], cinta, disco duro, así también usado como soporte de almacenamiento de los datos digitales. Por consiguiente, este formato de información no electrónica se presenta aun como un medio de transmisión y almacenamiento de la información en varias organizaciones.

La seguridad de la información comprende dentro de su contexto la confidencialidad, integridad y disponibilidad de la información, es decir, que para mantener la seguridad de la información es necesario que la misma no deba ponerse a disposición de cualquiera, ser revelada a individuos o procesos que no son autorizados. Así también, esta debe mantener su integridad, para conservar su exactitud y completitud. De modo que, la información debe estar accesible, utilizable por las entidades, usuarios, así como para los procesos autorizados.

[63] Medio Digital: También se le llama soporte digital. Es el material físico, tal como un disco compacto, cinta o disco duro usado como soporte para almacenamiento de datos digitales.

[64] DVD: Acrónimo de Digital Videodisc o Digital Versatile Disc.

Figura 4 Principios de la Seguridad de la Información



Fuente: 2 Identificación de Confidencialidad, integridad y disponibilidad del Banco Central de Bolivia (2017), expuesto por Cesar Roberto Cuenca Díaz en el grupo de seguridad conformado por la Agencia de Gobierno Electrónico y Tecnologías de la Información y Comunicación (AGETIC).

A continuación, se hace una descripción de las características que encierra el contexto de seguridad de la información. Por su alcance, protege la información en los aspectos más importantes para una defensa a gran escala.

2.1.1 Seguridad

Para poder identificar mejor la seguridad de la información dentro de una organización y sus funciones, es necesario garantizar su atención y asistencia. Pues, dentro de estas características esta desarrollar un conjunto de estrategias y esfuerzos, en el ámbito de seguridad. Por ello, se debe proteger y resguardar la información que se administra internamente, tanto en diligencias y el valor de la información para las mismas.

En este análisis, en seguridad está involucrada también la autenticidad, responsabilidad, no repudio y confiabilidad, la ausencia de riesgo en la información o la confianza a la administración de la información, puede referir como una acción que la sociedad exige o regocija

Entre otros tipos de seguridad también existen:

- Seguridad de la información
- Seguridad informática
- Seguridad activa
- Seguridad pasiva

2.1.2 Información

Figura 5 Relación Informacional

Fuente: Elaboración propia en base a Páez Urdaneta

La información es "Un ensamble o conjunto organizado y coherente de datos procesados e interrelacionados que forman una unidad de significado más compleja que sus partes, con propósito de comunicarla en el espacio y el tiempo [Archivos]" (Voutssas m. & Barnard Amozorrutia, 2014, p. 133). Esto es, formación coherente de los datos, en su consistencia logran

un fundamento importante. En consecuencia, son necesarios para cualquier Estado, empresa u organización.

Asimismo, la información que es constantemente actualizada, necesita nuevos soportes o medios de almacenamiento, o modernización de la misma con mayor capacitad para sostenerla. En otras palabras, Voutssas m. & Barnard Amozorrutia, (2014) nos mencionan que la informacion actualizada de almacenamiento, presenta una particular caracteristica de ubicación y almacenamiento:

> *Información que indica un cambio de ubicación de un componente digital almacenado, o la ocurrencia de un problema de almacenamiento, así como la acción tomada para corregir el problema, los resultados de las acciones tomadas, o la copia de los componentes de un soporte antiguo de almacenamiento hacia uno nuevo [Archivos]. (p.133).*

En este sentido se comprende, la insuficiencia[65] de soportes antiguos de almacenamientos para las nuevas exigencias de la información y su actualización, conlleva a prever y buscar nuevos soportes de almacenamiento, copias y respaldos de la información.

2.2. Confidencialidad

La confidencialidad, es la información que solo puede ser de acceso y uso del personal autorizado, no puede ser revelada a cualquiera, la misma presenta características entre las cuales se destaca que la información no debe ser expuesta por su contenido sensible o estratégico. Ni siquiera, ser revelada a individuos, entidades o procesos no autorizados.

[65] Insuficiencia: Falta o escasez de la cantidad que se necesita de una cosa.

Dentro del procedimiento de la administración y gestión de la información se considera la primicia de la confidencialidad que es la que restringe su acceso. En consecuencia, la disposición del acceso lo despliega la gestión de la información, cumpliendo con los requisitos de protección.

Es decir, el Instituto Boliviano de Normalización y Calidad señala confidencialidad como "propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades y procesos no autorizados" (IBNORCA, 2010, p.4). Esto es, de tal forma una acción importante. En efecto, es necesario identificar la información que se sitúa en los procesos, manifestando si la misma se encuentra vulnerable a terceros.

Del mismo modo, Miguel Pérez (2015) nos plantea la siguiente definición que confidencialidad "Es la propiedad por la que la información no se pone a disposición o se revela a individuos, entidades o procesos no autorizados" (p. 237). La confidencialidad es muy importante, pues quien precisa y tiene acceso al uso de esa información, debe saber utilizarla, es decir, saber a quien debe ser revelada, ya que vincula la participación del recurso humano y los intereses de la empresa.

Dentro de este orden de ideas, el Consejo para las Tecnologías de Información y Comunicación CTIC (2017), recomienda: que la confidencialidad es la propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. La confidencialidad de la información, debe contar con la participación del personal, ya que el concepto para mantener la confidencialidad es tener mayor seguridad en los recursos humanos.

Sin duda, los documentos de procedimiento administrativo presentan en su entorno las propiedades de brindar acceso a la información pública y privada, de ahí que, varios Estados

dotan de esa cualidad a sus políticas y constituciones. Es por ello, que la confidencialidad de la información, asemeja como un factor vital a los datos y estos contemplan características estratégicas para los países que los generan. En efecto, es muy importante tratar con la confidencialidad de un Estado u organización, sea cual fuere el soporte en el que se encuentre.

En relación a las implicaciones, la confidencialidad es la característica de proteger un conjunto de datos, los cuales son de gran valor estratégico para un Estado u organización.

> *Información confidencial: toda aquella información respecto al patrimonio de las personas, o la que comprenda hechos o actos de carácter económico, contable, jurídico o administrativo, referidos a las personas físicas o jurídicas, la cual pudiera ser de utilidad para un competidor. También, aquella amparada en cláusulas contractuales de confidencialidad*. *(Sánchez Vanderkst, 2014, p. 121)*

Por ello se hace necesaria, la seguridad de la información en los Estados u organizaciones en medidas preventivas tales para resguardar la información. Puesto que, las diligencias de carácter económico, legal o de funcionario, es de valor para muchos intereses. En consecuencia, las implicancias son identificadas como:

> *Seguridad en recursos humanos, es necesario establecer mecanismos de relación, en materia de seguridad de la información, entre el recurso humano y la entidad o institución pública con el objetivo de preservar la información a la que tienen acceso durante y después de la vinculación laboral. (Consejo para las Tecnologías de Información y Comunicación [CTIC], 2017)*

Llama la atención, la relación, vinculada con entidad y recursos humanos, con el compromiso de relación para un buen desempeño laboral. De manera que, la seguridad para la información es fundamental para la organización. En efecto, es la que dispone condiciones de acceso y uso en las nuevas contrataciones. En definitiva, se deben determinar los términos y condiciones de la

relación laboral, así se plantea en el documento por parte del Consejo de Tecnologías de Información y Comunicación CTIC (2017) que realiza la siguiente mención:

> *Establecer responsabilidades en el marco de seguridad de la información del servidor público o cualquiera que tenga un vínculo laboral con la entidad o institución pública, debe formar parte integrante de la documentación de los archivos personales de cada servidor público o cualquiera que tenga un vínculo laboral con la entidad o institución pública. (s.p.)*

Así se ha verificado, el acuerdo de confidencialidad que tiene como principal objetivo prevenir fugas, divulgación no autorizada, mal uso o resguardo de la información. Es decir, el acuerdo debe ser aplicado a los "servidores públicos o cualquier persona jurídica o natural que tengan un vínculo laboral con la entidad o institución pública" (Consejo para las Tecnologías de Información y Comunicación [CTIC], 2017). En efecto, la organización debe ser capaz de priorizar la información confidencial que dispone al contratar nuevo personal, comprender que información debe disponer para que el nuevo funcionario pueda desarrollar sus actividades.

Otro punto muy importante de la confidencialidad es "la valoración de esta característica, está en función del grado de afectación que ocasionaría la revelación o divulgación de información a personas no autorizadas," Consejo para las Tecnologías de Información y Comunicación CTIC (2017). Por lo tanto, quienes administran la información, ven la necesidad de categorizar o valorizar la información, para prevenir difusión o filtración de la información.

La valoración de la información debe ser necesaria y realizada independientemente por cada entidad o institución, debido a que las mismas cuentan con niveles de acceso y uso de la información, acuerdos legales dispuestos en el país que se desarrolla o referente a sus necesidades. Además, la valoración es cuantitativa ya que mide el grado de afectación que ocasionaría para la entidad.

La escala recomendada para la valoración cualitativa de las características del activo de información se presenta en la siguiente figura:

Cuadro 7 Escala de valoración de activos

Escala de Valoración	
1	Muy Bajo
2	Bajo
3	Medio
4	Alto
5	Muy Alto

Fuente: Consejo para las Tecnologías de Información y Comunicación CTIC (2017) Guía para la metodología de gestión de riesgos, anexo B.

Por otra parte, la confidencialidad es garantizar la propiedad de la información, recalcando que ésta, sea accesible solamente a personal autorizado, tal como, lo identifica el Decreto Supremo N. 1793, que señala claramente lo siguiente:

> *Confidencialidad: Todas las personas involucradas y que intervengan en el tratamiento de datos personales, están obligadas a garantizar la reserva de la información, incluso hasta después de finalizado su vínculo con alguna de las actividades que comprende el tratamiento, pudiendo únicamente realizar el suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las tareas autorizadas. (p. 11)*

En esta perspectiva, toda acción involucrada con el tratamiento de información personal, deben ser manejados con reserva aun después de la relación o vínculo establecido con la organización.

2.2.1 Valor de la información

Debe señalarse, la jerarquía del valor de la información, la cual se comprende como fundamental en la protección de la información y su término es intuitivamente necesario, de

manera que, en ocasiones convendría profundizar más el cálculo del valor real de la información o como se le designa en la organización. Muchas decisiones de carácter de inversión o recursos entre otros hacen uso de la información para obtener mejores resultados.

Pocas organizaciones comprenden el valor de la información y la implicancia de ésta. En definitiva, al no contemplar y diseñar medidas para su adecuada protección la organización pierde un gran valor, tanto económico y de prestigio, por lo tanto, es necesario identificar el valor de la información dentro de una organización u Estado.

Tal como se puede apreciar, la valoración documental en las organizaciones desplaza información muy importante en sus operaciones. El valor de la información administrada, puesta a disposición del personal, recalca la labor de la confianza puesta en sus empleados. Sin embargo, una organización que no posea cultura de valoración de la información, en disposición para muchos funcionarios, caracterizaría una vulnerabilidad para la organización por medio de sus empleados. Por ejemplo, el uso indebido de la información distribuida a terceros.

Cuadro 8 Protegidos y Responsables de Pasar Información a la Embajada Estadounidense

Funcionarios y políticos protegidos	Cargo	Código del cable donde figura como protegido o estrictamente protegido	Fragmento
HASSENTEUFEL, OSCAR	Presidente de la Corte Nacional Electoral	06LAPAZ413	2. (SBU) El 15 de febrero, el encargado político de la embajada se reunió con el Presidente de la Corte Nacional Electoral Oscar Hassenteufel (proteger) para obtener sus puntos de vista sobre la continuada presión pública por funcionarios del MAS y diputados para que

			los líderes de la Corte Electoral renuncien.
LEMA, MARCO ANTONIO	Asesor y empleado del Comité de Hidrocarburos del Congreso	09LAPAZ698 09LAPAZ1053	7. (C) Marco Antonio Lema (proteger estrictamente), asesor de cuatro congresistas del MAS y miembro del personal en el 'Comité de Hidrocarburos del Congreso de Bolivia, explicó que el MAS en realidad nunca ganó un punto de apoyo de los verdaderos devotos de Tarija, por lo que muchos líderes del MAS son "oportunistas solo para los puestos de trabajo", como él reconoció que era.
FLORES, JAVIER F.	Estratega de Oposición	09LAPAZ658 08LAPAZ2245 08LAPAZ2285	5. (C) El estratega Nacional de oposición Javier Flores (proteger estrictamente) afirma que, detrás de las pantallas y a último momento, los congresistas de la oposición fueron capaces de conseguir que el gobierno esté de acuerdo con el levantamiento del estado de sitio en Pando, y la liberación de Prefecto de Pando, Leopoldo Fernández y los 14 presos de oposición de Pando.

Fuente: Torres Gorena, Suarez Mamani, Telleria Escobar, & Merida Aguilar, 2016

Las evidencias anteriores, identifican la susceptibilidad de la filtración de la información, ante un interés de terceros y de acceder a la información por otros Estados, que lo consideran como estratégico para sus operaciones. En efecto, se buscas aprovechar la información que no cuenta con la valoración respectiva.

2.2.2 Clasificación de la información

La clasificación de la información se encuentra arraigada y tomada de la mano con el tema de acceso a la información, que se considera como un derecho humano en muchos países, tal es el caso de Bolivia que en su Decreto Supremo N. 28168 menciona:

> *Que el acceso a la información pública, de manera oportuna, completa, adecuada y veraz es un requisito indispensable para el funcionamiento del sistema democrático y pilar fundamental de una gestión pública transparente; particularmente en el acceso a la información necesaria para investigar delitos de lesa humanidad, de violaciones a derechos humanos, delitos de daño económico al Estado y de hechos de corrupción.* (Decreto Supremo N. 28168, 2005)

La carta magna del Estado Plurinacional revela, que para la clasificación de la información es importante en la autoridad gestione que los documentos de la función pública sean resguardados por profesionales en el área, por ello se señala que se debe "Inventariar y custodiar en oficinas públicas los documentos propios de la función pública, sin que puedan sustraerlos ni destruirlos. La ley regulará el manejo de los archivos y las condiciones de destrucción de los documentos públicos." (Constitucion Politica del Estado Plurinacional de Bolivia, 2009), los mismos asumen que estos deben ser controlados por profesionales competitivos en el área, para su clasificación.

Llama la atención, la responsabilidad de "Guardar secreto respecto a las informaciones reservadas, que no podrán ser comunicadas incluso después de haber cesado en las funciones. El procedimiento de calificación de la información reservada estará previsto en la ley" (Constitucion Politica del Estado Plurinacional de Bolivia, 2009). En efecto, una organización debe contemplar la clasificación de la información, su reserva y el establecimiento correspondiente y desarrollarse aun después de cumplidas ya las funciones.

En esta perspectiva, el responsable de la clasificación es la Máxima Autoridad de la Entidad[66], quien respaldado con el apoyo de su personal podrá clasificar la información mediante resolución expresa, que contendrá como mínimo: fecha, mención al documento o información a clasificarse y el motivo y fundamento legal, considerando también si la información vincula la seguridad del Estado, ya sea esta interna o externa (Ministerio de Transparencia Institucional y Lucha contra la Corrupción). En efecto, las entidades que administres y almacenen la información como se da en sus archivos, es necesario que realicen la clasificación de la información, con la intención de, protegerla ante cualquier filtración y vulneración.

En todo caso, la clasificación de la información secreta estimada por el Estado Plurinacional de Bolivia, estará restringida por un plazo máximo de veinte años si se tratara información sensible a la seguridad externa. Asimismo, diez años cuando se trata de Información sobre seguridad interna.

La clasificación de la información se caracteriza en las siguientes partes:

- Información pública
- Información confidencial
- Información reservada
- Información secreta

Atendiendo a estas consideraciones, la clasificación de la información, en relación a la tipificación de la información propuesta al grupo de seguridad por la Agencia de Gobierno Electrónico y Tecnologías de la Información y Comunicación (2016), es la siguiente:

[66] MAE: Máxima Autoridad de Estado

Cuadro 9 Clasificación de la información identificada por la AGETIC

Nivel	Tipo	Descripción
1	Pública	Es toda información generada y poseída por la institución pública contemplada en el D.S. 28168.
2	Confidencial	Es aquella que solo puede ser accedida por cualquier persona de la institución.
3	Reservada	Es de uso exclusivo de los empleados de la institución y proveedores especiales que hayan firmado un acuerdo de confidencialidad.
4	Secreta	Es aquella que es de uso exclusivo de una persona o pequeño grupo de funcionarios.

Fuente: Agencia de Gobierno Electrónico y Tecnologías de la Información y Comunicación AGETIC.

La definición conceptual que tiene la Autoridad de Supervisión del Sistema Financiero (ASFI), expuesta en el grupo de seguridad, aportes y clasificación de la información, define los tipos de clasificación de Lin Zambrana (2016), que establece que:

- *Pública: Es la información que puede ser conocida y utilizada al interior o exterior de la Institución, sin que ello represente daños o perjuicios a la ASFI*[67].
- *Confidencial Interna: Es aquella información que puede ser conocida y utilizada al interior de ASFI.*
- *Confidencial Privada: Es aquella información que es conocida y utilizada exclusivamente por una Unidad de la ASFI.*
- *Confidencial Reservada: Información que solo puede ser conocida y utilizada por un grupo muy reducido de personal de la Institución de la ASFI.*

[67] ASFI: es una institución de derecho público y de duración indefinida, con personalidad jurídica, patrimonio propio y autonomía de gestión administrativa, financiera, legal y técnica, con jurisdicción, competencia y estructura de alcance nacional, bajo tuición del Ministerio de Economía y Finanzas Públicas, y sujeta a control social.

2.2.3 Información pública

La información pública, es considerada como la información que está al alcance de toda la sociedad, por ser un tema vinculado a la transparencia y evitar corrupción. Del mismo modo, la información pública debe ponerse a disponibilidad de todos los ciudadanos de un Estado. Es decir, información disponible que coexista en algún tipo de formato de soporte o en el proceso de inicio o conclusión en el que se encuentre y tiene a ser de libre acceso.

La información pública que se encuentre en los cuatro Órganos del Estado[68], y en los alcances de todos sus niveles, deben garantizar el ejercicio pleno acceso a la información, también así, Ministerio Público[69], Defensor del Pueblo[70], Contraloría General del Estado[71], Procuraduría General del Estado[72], Fuerzas Armadas[73], Policía Boliviana[74] (Ministerio de Transparencia Institucional y Lucha contra la Corrupción). Es decir, deben garantizar la transparencia en la

---

[68] Órganos de Estado: Los órganos del Estado son considerados los instrumentos o medios que utiliza la administración pública para realizar una determinada función estatal. Tal como, órganos legislativos, órganos ejecutivos y órganos judiciales. En efecto, los mismos buscan que una persona o personas puedan expresar su voluntad estatal.

[69] Ministerio Público: El Ministerio Público representa a la sociedad ante los órganos jurisdiccionales del Estado, gozando de autonomía funcional y administrativa en el cumplimiento de sus deberes y atribuciones. Lo ejercen el Fiscal General del Estado y los agentes fiscales, en la forma determinada por la ley.

[70] Defensor del Pueblo: Que defiende o protege a alguien o algo. Haciendo prevalecer los derechos fundamentales de los ciudadanos frente a la Administración.

[71] Contraloría General del Estado: El Tribunal Nacional de Cuentas fue creado en 1883, con la finalidad de controlar fondos públicos. Tenía como sede la ciudad de Sucre y estaba administrado por cinco jueces elegidos por la Cámara de Diputados. Sus resoluciones eran inapelables, presentaban un informe anual al Congreso Nacional y respondían de sus actos ante la Corte Suprema de Justicia. https://www.contraloria.gob.bo/

[72] Procuraduría General del Estado: La Procuraduría General del Estado es una institución jurídica pública que cumple la alta función constitucional de defensa legal del Estado boliviano. Es responsable de promover, precautelar y defender los intereses patrimoniales del Estado, sea judicial o extrajudicialmente en resguardo de la soberanía boliviana. https://www.procuraduria.gob.bo/

[73] Fuerzas Armadas: Las Fuerzas Armadas de Bolivia (FF. AA.) son una organización oficial encargada de la defensa, tanto de agresiones externas como de internas, de Bolivia. También velan por la seguridad, estabilidad y protegen la constitución boliviana.

[74] Policía Boliviana: La Policía Boliviana es la principal fuerza de seguridad del Estado Plurinacional de Bolivia. Fue creada el 24 de junio de 1826 mediante una ley reglamentaria dictada por Antonio José de Sucre. Tiene la misión específica de la defensa de la sociedad y la conservación del orden público, mediante el cumplimiento de las leyes en el territorio nacional.

administración pública, determinando procedimientos en temas de transparencia y acceso a la información que cursen en poder de los mismos. En consecuencia, las personas privadas, naturales o jurídicas que hayan suscrito algún contrato con él Estado, deben proporcionar el mismo ámbito de aplicación de procedimiento de acceso y transparencia, del mismo modo, las empresas e instituciones públicas descentralizadas, desconcentradas, autárquicas y empresas mixtas, personas privadas, naturales o jurídicas que hayan suscrito contratos con el Estado para la prestación de servicios públicos, entidades privadas en las que el Estado Plurinacional tenga participación económica y a las entidades privadas que reciban fondos o bienes, de cualquier origen, para la consecución de fines de interés público. Se denominan también, como entidades públicas, o de interés público, de forma que, quedan también obligadas a poner en conocimiento de la sociedad la información que se considere de interés público, En el Artículo 7 del proyecto de ley de Transparencia y Acceso a la Información Pública menciona el acceso a las mismas. A continuación, se mencionar algunas características de la Ley:

> *Los medios para publicar y difundir la información pública, de manera enunciativa y no limitativa, son los portales web de internet, los medios impresos, los medios de comunicación masiva, audiovisuales y todo aquel medio o recurso idóneo que permita lograr la máxima publicidad y difusión pública.* (Ministerio de Transparencia Institucional y Lucha contra la Corrupción)

En relación con las implicaciones, la información pública por su característica es transmitida de manera transparente. Es decir, que su acceso es libre a cualquiera que lo solicite. En efecto, esta información brinda la disposición de los datos característicos de una organización.

Resulta así mismo interesante, la participación que tienen los archivos en la función pública o privada, pues estos poseen la información de acceso público, así como restringido. Por tanto, el compromiso adquirido de gestionar la información es muy relevante para los profesionales y

entidades que la administran. Es decir, “Es responsabilidad de las entidades públicas y las entidades privadas que prestan servicios públicos, crear, mantener y gestionar los archivos de información pública, de acuerdo a Ley” (Ministerio de Transparencia Institucional y Lucha contra la Corrupción). En definitiva, la información más significativa está bajo el resguardo de los archivos, expresado de otra manera es donde “La información pública, en sus fases de inicio, procesamiento o conclusión, puede estar contenida en documentos escritos, fotografías, grabaciones, soporte magnético o digital, o en cualquier otro formato o soporte” (Ministerio de Transparencia Institucional y Lucha contra la Corrupción). Por lo tanto, la existencia y desarrollo de nuevos soportes de información adaptadas a tecnologías de la información y comunicación, brinda el alcance y necesidad de gestionar la información conforme a estas características. En resumen, los nuevos formatos y soportes donde se plasma la información, requieren contemplar y dar protección a esta información pública.

2.2.4 Información confidencial

Es necesario, prevenir posibles fugas de información, divulgación no autorizada, mal uso o resguardo de la información, concisamente con servidores públicos o cualquier persona jurídica o natural que asuma un vínculo profesional con la entidad o institución pública.

Como resultado, el Consejo para las Tecnologias de Informacion y Comunicacion CTIC (2017), efectúa la siguiente observacion en relación a la confidencialidad en una organización:

- *Elaborar el acuerdo de confidencialidad*.
- *Definir las restricciones y alcances del uso de la información, así como roles y responsabilidades.*
- *Coordinar con el área jurídica la legalidad del acuerdo de confidencialidad*.

- *Garantizar la anuencia del servidor público o cualquier persona natural o jurídica que tenga un vínculo laboral con la entidad o institución pública con el acuerdo de confidencialidad.*
- *Revisar y actualizar el acuerdo de confidencialidad en caso de cambios sustanciales en la clasificación de la información o a requerimiento interno.*
- *Respetar los datos de carácter personal, garantizar la privacidad y protección de la información personal identificable.*

Resumamos a continuación, las consecuencias que se presentan cuando no contempla lo confidencial en la información, estimula el riesgo a fraudes internos, escenarios de peligro entre otros, sin embargo, ninguna entidad se encuentra excluida de los peligros que se encuentran cuando no se examina la confidencialidad de la información. Tal es el ejemplo del Banco de los Bolivianos (Banco Unión), donde sobrellevo un incidente de vulnerabilidad hacia la información, que no se encontraba clasificada.

> *El 27 de septiembre, la gerencia general de la entidad con participación mayoritaria del Estado dio a conocer que Juan Pari (exgerente de Operaciones del Banco Unión, de 27 años) "vulneró los controles" de seguridad del banco y sustrajo de éste por casi un año diferentes montos que luego fueron cuantificados por la propia financiera en Bs 37,6 millones (de inicio, la Fiscalía informó de al menos Bs 43 millones)* (Castel, 2017).

Por ello se hace necesario, la confidencialidad de la información otorgada a el personal de una organización. Desarrollar políticas para la información y controles en las virtudes de información que gozan algunos funcionarios de las Entidades.

2.2.4.1 Filtración de la información

La filtración de la información en un tema crítico, que inmediatamente afecta a muchos países y organizaciones, que tal es el caso de la empresa de Facebook ha admitido que los datos de 87

millones de usuarios quedaron expuestos durante la filtración de información, obtenida por la consultora política Cambridge Analítica[75] (RT Noticias Internacionales, 2018), contenido tan crucial que el presidente y fundador de la empresa, compadeció con el tribunal de los Estados Unidos preocupados por la gran cantidad de información filtrada.

2.2.5 Información reservada

El Artículo 237, son obligaciones para el ejercicio de la función pública reconocidos por la Constitucion Politica del Estado Plurinacional de Bolivia (2009) inventariar[76] y custodiar en oficinas públicas los documentos propios de la función pública, estos deben garantizar que los mismos no puedan sustraerlos ni destruirlos. La ley regulará el manejo de los archivos y las condiciones de destrucción de los documentos públicos. Por lo tanto, la carta magna refiere el control minucioso de la información pública. En consecuencia, se debe desarrollar el análisis de seguridad de la información para las diferentes particularidades que contempla la información en los archivos.

Evidentemente, la información reconocida como reservada, caracteriza la prioridad de acceso que solo se les provee pocas personas, por ejemplo, la Autoridad de Supervisión del Sistema Financiero (ASFI) (2016), considera que la confidencial reservada, es información que solo puede ser conocida y utilizada por un grupo muy reducido de personal de la Institución. Por consiguiente, la información clasificada está bajo la custodia de sus archivos en muchas organizaciones, es decir, se debe "Guardar secreto respecto a las informaciones reservadas, que

[75] Cambridge Analítica: Cambridge Analytica (CA) fue una compañía privada que combina la minería de datos y el análisis de datos con la comunicación estratégica para el proceso electoral. La empresa fue creada en 2013 como una rama de la casa matriz Strategic Communication Laboratories (SCL), para participar en la política estadounidense.

[76] Inventariar: Hacer el inventario de una cosa.

no podrán ser comunicadas incluso después de haber cesado en las funciones. El procedimiento de calificación de la información reservada estará previsto en la ley" (Constitucion Politica del Estado Plurinacional de Bolivia, 2009). Así también, el artículo 43 del Ministerio de Transparencia Institucional y Lucha contra la Corrupción, considera información reservada a:

- Aquella cuya calidad de reservada se halle establecida mediante leyes o decretos supremos aprobados en materias distintas a seguridad del Estado.
- Aquella información que se clasifique como reservada mediante el procedimiento de clasificación establecido en la presente ley, solamente cuando se trate de seguridad del Estado, interna o externa.

2.2.6 Información secreta

El derecho de acceso a la información no podrá ser ejercido sobre la información clasificada como secreta, reservada o confidencial, por lo cual, el artículo 42 del proyecto de transparencia y acceso a la información pública lo siguiente:

> *Se considera información secreta aquella relativa a la seguridad interna o externa del Estado, cuya divulgación o difusión pueda poner en riesgo al Estado Plurinacional. La información secreta se clasificará mediante Leyes que serán promovidas por las entidades que así lo requieran. Estas leyes contendrán un listado específico de la información que consideren que debe ser secreta.* (Ministerio de Transparencia Institucional y Lucha contra la Corrupción)

Consecuentemente, la información de seguridad del Estado o secreta, debe estar respaldada por leyes desarrolladas y provistas, así como con la garantía de organismos de Estado.

2.3 Integridad

En efecto, uno de los objetivos de la seguridad de la información, es proporcionar la integridad de la misma, es decir "El deber primordial de los archiveros es mantener la integridad de los documentos que están bajo su cuidado y custodia" (Consejo Internacional de Archivos, 1996, p. 1). De ahí que, el responsable de la información, debe garantizar la integridad de la misma, sea cual fuere el soporte y cantidad en que se encuentre.

Dentro de los activos de información, la integridad está considerada como:

> *Una valoración alta de esta propiedad se da por el grado de afectación (daño grave) causado por la alteración voluntaria o no intencionada de los datos. Por el contrario, una valoración menor se da cuando su modificación no supone preocupación alguna.* (Consejo para las tecnologías de información y comunicación [CTIC], 2017)

La importancia de la integridad de la información radica en que la misma no haya sido borrada, copiada o modificada,

> *Integridad: Característica única del mensaje electrónico de datos o documento digital ambos con firma digital, que indica que los mismos no han sido alterados en el proceso de transmisión desde su creación por parte del emisor hasta la recepción por el destinatario. (Decreto Supremo N° 1793, 2011, p. 10)*

La integridad de la información es vital en el soporte donde se encuentre, pues su vulneración daña la fiabilidad de la información. Por consiguiente, la exactitud de la información tiene que ser viable para la acción para la que será usada.

2.3.1 Integridad de la información

La viabilidad de la información de según Voutssas m. & Barnard Amozorrutia (2014), es "Evaluación del costo y capacidades técnicas requeridas para la preservación permanente de un cierto cuerpo de documentos de archivo [Archivos]" (p.133). Lo que significa la posibilidad de

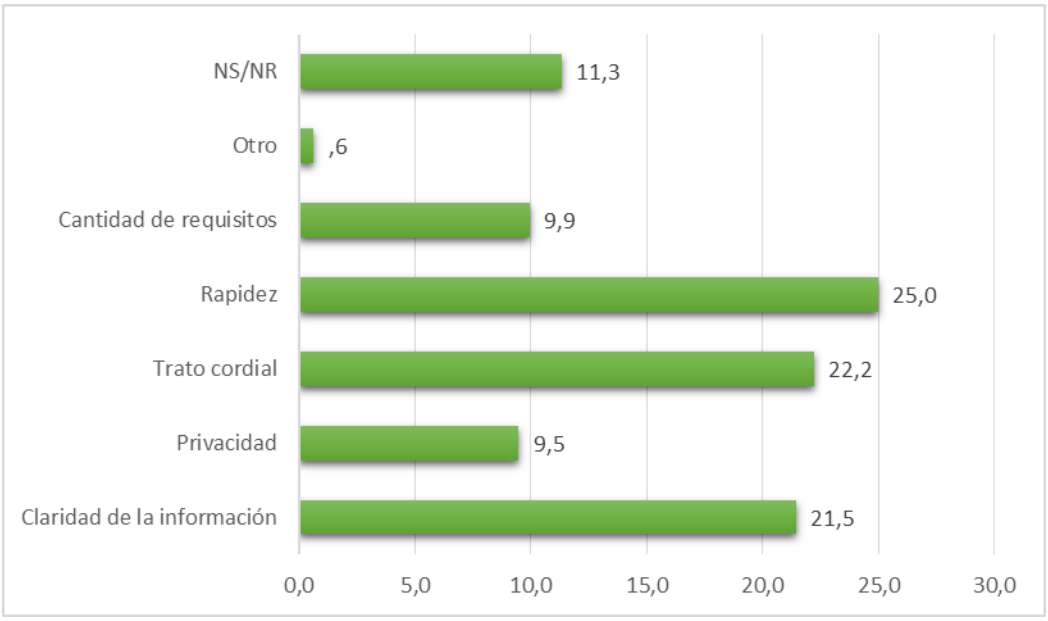
recobro de la información, en el desarrollo de nuevas técnicas para mantener la integridad de la información.

2.4 Disponibilidad

Desde la perspectiva más general, la información facilitada en cualquier soporte como el medio digital, es la que se encuentra disponible para el procesamiento y tratamiento de la información. De ahí que, el acceso de la información es vital para el funcionamiento de una organización, pues la información de la organización debe estar disponible para los clientes y el personal de la organización, sin que estos sean denegados o interrumpidos.

Tal es el caso de la población de la sociedad de la información en Bolivia, que tiene un interés a la rapidez y disponibilidad de la información. Todo ello se percibe en el siguiente gráfico:

Gráfico 2 Características más importantes de la sociedad de la información en relación a la realización de trámites en las instituciones públicas



Fuente: elaboración propia en base a las encuestas de tecnologías de la información y comunicación.

2.4.1 Acceso a la información

El acceso a la información dentro de la legislación boliviana, hace mención a que: "El acceso a la información en Bolivia se ha construido de manera desventajosa para la sociedad civil. A nivel regional, siete instrumentos jurídicos han prevalecido para determinar el grado y alcance del derecho a la información, partiendo desde la mera publicidad, hasta el acceso irrestricto a los archivos del estado" (Oporto Ordoñes & Rosso Ramirez, 2007, p. 59). En definitiva, el acceso a la información, debe estar apoyado por el uso de las nuevas tecnologías de la información y comunicación, para lograr un mayor alcance.

Cabe señalar, que el acceso libre a la información se caracteriza porque es el derecho que tienen los ciudadanos y su acceso es fundamental para el grado de desarrollo socio-económico.

Cuadro 10 Acceso a la información en las constituciones latinoamericanas

ACCESO A LA INFORMACIÓN EN LAS CONSTITUCIONES LATINOAMERICANAS		
País	Acceso a la Información en la CPE	Fecha de aprobación
Argentina	Sí	1853
Belice	Limitado	1981
Bolivia	Sí	2008
Brasil	Sí	1998
Chile	Limitado	1981
Colombia	Sí	1991
Costa Rica	Sí	1949
Cuba	No	
Ecuador	Sí	1998
El Salvador	No	
Guatemala	Limitado	1985
Honduras	No	
México	Sí	1917
Nicaragua	Sí	1987

Panamá	No	
Paraguay	Sí	1992
Perú	Sí	
República Dominicana	Sí	1996
Uruguay	No	
Venezuela	Sí	1999

Fuente: compilado por Michael Mirelman (Publicado en Neuman, 2006): Pablo Avila, Comunicación personal via e-mail el 10.04.2009, extraído de (Oporto Ordóñez, 2015)

En varios Estados, la disponibilidad de la información está garantizada, para un mejor control gubernamental, en efecto el Estado Plurinacional de Bolivia, establece este derecho para sus ciudadanos.

> *El derecho de petición, contenido en el Art. 24 complementa el alcance del derecho libre a la información, por cuanto expresa que los ciudadanos pueden exponer sus peticiones de forma libre, por escrito y/o oralmente, en su propio idioma, y con el único requisito de identificarse adecuadamente. (Oporto Ordóñez, Acceso a la información pública, archivos y bibliotecas en la Constitución Política del Estado, 2015, p. 54)*

Como resultado de lo anteriormente expuesto podemos señalar que: el acceso a la información puede ser requerida mediante solicitud o petición expresada del interesado. En consecuencia, el acceso a la información mediante el uso de nuevas tecnologías por parte del Estado, fue desarrollado para un gobierno y su sociedad, mejor conocido como Gobierno Electrónico o Gobierno Digital.

2.4.1.1 Digitalización de la información en documentos

Según Cuba (2010), señala que la digitalización de los documentos nace de la necesidad de almacenar, distribuir y consultar de manera más rápida y eficiente los mismos y así garantizar la calidad de los procesos dentro de una organización.

Así mismo, identifica que, para el futuro de los documentos, así como evitar riesgos, estos deben ser digitalizados, por ser el patrimonio documental de una entidad. Por lo tanto, es un tema crítico dentro de una organización, por lo que llega a ser muy necesaria para una mejor toma de decisiones.

Los aspectos más relevantes para la digitalización son:

- *Gastos de almacenaje.*
- *Múltiples copias.*
- *Depuración de documentos.*
- *Localización.*
- *Manipulación.*
- *Búsqueda de documentos físicos.*
- *Retraso en firmas y autorizaciones.*
- *Extravió de documentos.*
- *Exceso de fotocopias.*
- *Archivos duplicados.*
- *Falta de seguridad y confiabilidad.*
- *Humedad, polvo, polillas, mal manejo.*
- *Confusión y pérdida de documentos.*[77]
- *Costos de almacenamiento.*
- *Dificultad en la localización de documentos.*

Todo esto hace que la información se pierda y sea necesaria su digitalización (p. 89).

---

[77] Cabe señalar que, para una mejor explicación en lo citado por Cuba, se incluyó tres viñetas que caracterizan de mejor manera la necesidad de la Digitalización en archivo, en apoyo a lo señalado por el autor.

2.5. Sistema de gestión de seguridad de la información (SGSI)

La seguridad de la información es un tema muy importante en las empresas, cabe mencionar que comprender el Sistema de Gestión de Seguridad de la Información (SGSI), en la Norma Boliviana NB/ISO/IEC 27000 de IBNORCA en sus términos y definiciones, indica que esta es "Parte del sistema de gestión global (...) basada en un enfoque hacia los riesgos del negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar mantener y mejorar la seguridad de la información" (Instituto Boliviano de normalizacion y calidad, 2010, p. 5).

En otras palabras, la necesidad de dependencia de los sistemas de información y el aumento de nuevas amenazas en el Internet y nuevas tecnologías, concibe la necesidad de un sistema de gestión de seguridad de la información para las organizaciones.

Tal como lo menciona Miguel Pérez (2015), quien señala que las ventajas de gestionar la seguridad de la información en las organizaciones aporta de gran manera con las siguientes prerrogativas:

- Evita interrupciones en las cadenas de trabajo, ya sea industrial o trabajos administrativos, con el ahorro de costes que esto trae consigo.
- Descubre fraudes de los propios empleados y los previene.
- Aumenta la calidad del servicio.
- Aumenta la competitividad de la empresa al evitar los riesgos de interrupciones en el ciclo del trabajo.
- Evita fraudes externos, especialmente espionaje industrial, comercial o intelectual de nuestros competidores.
- Disminuye el daño de males mayores, como desastres naturales, robos, incendios o vandalismos.

- Evita sanciones por incumplimiento de normativa, como la LOPD[78], la propiedad intelectual, etc.

Del mismo modo IBNORCA (2010), detalla una visión general y principios de la seguridad de la información, que dice:

> *Un Sistema de Gestión de la Seguridad de la Información (SGSI), proporciona un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de la protección de los activos de la información para alcanzar los objetivos del negocio sobre la base de una evaluación del riesgo y los niveles de aceptación del riesgo de la organización diseñados para tratar y gestionar los riesgos de manera eficaz. El análisis de los requisitos para la protección de los activos de información y la aplicación de controles adecuados para garantizar la protección de estos activos de información, según corresponda contribuyen a la implementación exitosa de un SGSI* (p.9).

También, se hace la mención a los principios fundamentales que contribuyen a la implementación exitosa de un SGSI, que son:

- Concientización de la necesidad de la seguridad de la información.
- Asignación de responsabilidades para la seguridad de la información.
- Incorporación del compromiso de la dirección de las inquietudes de las partes interesadas.
- Mejora de los valores de la sociedad

[78] LOPD: La Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal, (LOPD), es una ley orgánica española que tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar. Fue aprobada por las Cortes Generales el 13 de diciembre de 1999. Esta ley se desarrolla fundamentándose en el artículo 18 de la constitución española de 1978, sobre el derecho a la intimidad familiar y personal y el secreto de las comunicaciones.

- Evaluaciones de riesgo a fin de determinar los controles adecuados para alcanzar niveles aceptables de riesgo.
- Seguridad incorporada como un elemento esencial de los sistemas y redes de información.
- Prevención y detección activa de los incidentes de seguridad de la información.
- Garantizar un enfoque completo de gestión de la seguridad de la información.
- Continúa reevaluación de la seguridad de la información y la realización de las modificaciones según corresponda.

Si bien es cierto, que la gestión de la información en los Órganos de Estado, se desarrolla en distintos soportes de información, estor órganos deben resguardar y tratar esta información, para ponerla a disposición especialmente en sus operaciones y servicios. Por ende, como lo señala el Consejo Internacional de Archivos (CIA), en el documento de Código de Ética Profesional, establece que; los archiveros deben dejar constancia documentada para justificar sus acciones en relación con los documentos, pues bien "Los archiveros deben abogar por un adecuado tratamiento de los documentos a lo largo de su ciclo vital y colaborar con los productores de los mismos en la solución de los problemas que plantean los nuevos soportes y las nuevas prácticas de gestión de la información" (Consejo Internacional de Archivos, 1996, p. 3). En conclusión, se debe examinar el nuevo alcance que tiene la información gracias al desarrollo tecnológico.

Algo semejante ocurre con el crecimiento de las nuevas tecnologías de la información y comunicación, que es uno de los más importantes involucrados que impactan directamente dentro de las organizaciones. Por su parte (Flores Barrios, Soto del Ángel, Camacho Díaz, & Barrera Reyes, 2011) hace mención de que "La información tiene una importancia fundamental para el

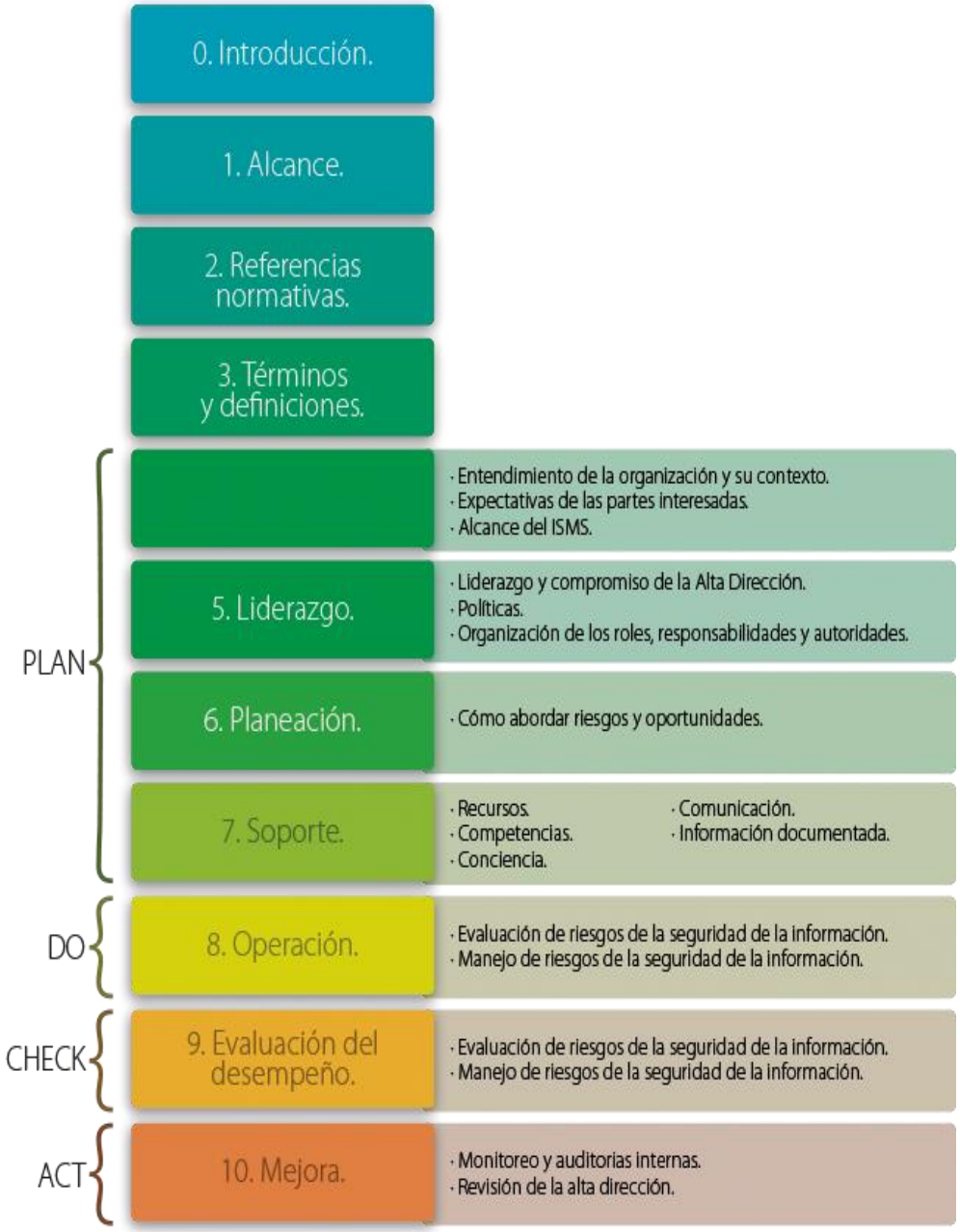
funcionamiento y quizá incluso sea decisiva para la supervivencia de todas las organizaciones a nivel global" (p. 44)

La seguridad de la información aplicada a empresas es de vital importancia, para su supervivencia, desarrollo y crecimiento con el uso de las nuevas tecnologías de información y comunicación.

En efecto, dentro de uno de sus requisitos para el aprovechamiento de nuevas tecnologías por parte de las empresas y desenvolvimiento de la misma a nivel nacional y global, comprende la importancia de la aplicación de seguridad de la información en la misma. De manera que, se observa en los resultados expuestos por parte de Flores Barrios, Soto del Ángel, Camacho Díaz, & Barrera Reyes (2011). En el estudio realizado sobre evaluación de impacto en los sistemas de gestión de seguridad en empresas de la ciudad de Tuxpan, Veracruz, se observan las siguientes derivaciones: 85% de las empresas consideran la importancia de implementar un sistema de gestión de seguridad de la información bajo la seria ISO/IEC 27001 para el control de sus activos, de igual manera un 95% ve la necesidad de organizar y certificar la seguridad de la información mediante la misma norma. (p. 46).

La seguridad de la información, cuenta con normas internacionales reconocidas para la gestión de la seguridad de la información, que tiene por objetivo el brindar buenas prácticas para la protección de los activos de información en una entidad u organización. Tal como lo ejemplifica la AGETIC, en el siguiente gráfico, destinado a la mejor comprensión en tema de estándar de seguridad de la información.

Figura 6 Estructura del estándar ISO/IEC 27001:2013



Fuente: Extraído del documento de aportes Grupo de Seguridad Agetic Bolivia

2.5.1 Sistema de gestión de seguridad de la información (SGSI)

Ahora bien, para la implentación de un sistema SGSI, es un proceso metódico laborioso y en algunos casos costoso, pues este debe ser planificado y justificado. Para ello es necesario considerar los siguientes acápites:

Considerando la seguridad de la información de una empresa u organización, esta debe ser considerada de una manera general, y no así por pequeñas partes, como un énfasis hacia algún fallo en la seguridad.

> *El éxito en la implantación de un SGSI desde cualquier perspectiva empresarial depende del compromiso y la mentalidad de cambio de los niveles ejecutivos y directivos en las organizaciones, por tanto, el alcance del sistema requiere de un nivel de concientización de las esferas estratégicas y tácticas de la estructura empresarial, de esta forma la capacitación se convierte en un medio de sensibilización que conduce a la interiorización y al compromiso de cambio como escenario de competitividad empresarial.* (Arévalo Ascanio, Bayona trillos, & Rico Bautista, 2015)

En efecto, la implementación de un sistema de gestión de seguridad de la información implica el desarrollo de varias fases en las cuales se exigen diferentes tareas para cada una de las etapas en las que se desarrolla. Tanto así, que la implementación de un SGSI dentro de una organización tiene la capacidad de ajustarse a la misma conforme a sus necesidades.

Cuadro 11 Metodología para implantar el SGSI ISO 27001:2005

FASES	ACTIVIDADES
I. Entendimiento de los requerimientos del modelo	• Taller con niveles estratégicos y tácticos
II. Determinación del alcance	• Etapa estratégica • Etapa táctica
III. Análisis y evaluación del riesgo	• Realización del análisis

	• Definición de política de seguridad de información y objetivos • Evaluación de las opciones para el tratamiento del riesgo • Selección de controles y objetivos de control • Elaboración de la declaración de aplicabilidad
IV. Elaboración del plan de continuidad del negocio	• Realizar el Business Impact Analysis • efectuar el análisis del riesgo e identificar escenarios de amenazas • Elaborar estrategias de continuidad • Diseñar plan de reanudación de operaciones • Diseñar procesos de ensayo
V. Implementar y operar el SGSI	• Elaborar el plan de tratamiento del riesgo • Determinar la efectividad de los controles y las métricas
VI. Monitorear y revisar el SGSI	• Detección de incidentes y eventos de seguridad • Realización de revisiones periódicas al SGSI
VII. Mantener y mejorar el SGSI	• Implementar las acciones correctivas y preventivas
VIII. Desarrollo de competencias organizacionales	• Entrenamiento de documentación del SGSI • Entrenamiento en manejo de la acción correctiva y preventiva • Entrenamiento en manejo de la auditoria interna
IX. Redacción del Manual de Seguridad de la Información	• Redacción del Manual de Seguridad de Información
X. Ejecución de las auditorías internas	• Realización de las auditorías internas

Fuente: Arévalo Ascanio, Bayona trillos, & Rico Bautista, 2015

2.6 Protección de los datos

A partir del desarrollo de las nuevas tecnologías, los datos personales contenidos en ficheros principalmente electrónicos, se vuelven cada vez más vulnerables a la apropiación y abuso, de aquellos que poseen o acceden a las bases de datos, con fines delictivos. Por este motivo se debe controlar el resguardo de la información, albergada en sistemas computacionales, informáticos, y en distintos soportes donde son almacenados y utilizados, lo cual busca garantizar la intimidad y privacidad de las personas físicas. Pues bien, muchas organizaciones gestionan y operan sus servicios por medio de internet, mediante correos electrónicos, correos, corporaciones, aplicaciones, páginas web institucionales, etc.

De manera que, las organizaciones, tramitan información de carácter personal de sus miembros y clientes en sus procedimientos. Por consiguiente, las mismas requieren recolectar información personal necesaria, para desarrollar sus actividades, por lo cual, las empresas u organizaciones almacenan gran cantidad de información de la vida privada o pública de las personas. En efecto, las empresas deben tomar ejercicios para salvaguardar esta información, donde las mismas comprendan la importancia de proteger esta información de forma estricta.

Pero ¿Qué es un dato personal?, un dato personal es cualquier información numérica, alfabética, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables, relativos a su identidad, estos pueden ser: nombres y apellidos, domicilio, una fotografía o video, etc. Como relativos a su existencia y ocupaciones, pueden ser: estudios, trabajo, enfermedades, etc.

Es por ello, que países miembros de la Unión Europea desarrollaron organismos, leyes y políticas que protegen los datos personales de esos países, de ahí que, también todos los países con los que se relacionan están sujetas a estas políticas de protección de datos personales, aun sin

ser miembros de la Unión Europea. Por ejemplo, Bolivia que mantiene relaciones comerciales, sobre sanidad y educación, debe regirse bajo las leyes y políticas de protección de datos de España.

España, miembro de la Unión Europea, cuenta con una Agencia Española de Protección de Datos, quien en su tutela es la que efectúa los derechos de protección de las mismas cuando estas están siendo vulneradas. Para cumplir con ello, la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal y Reglamento General Europeo de Protección de Datos, obliga a todos los profesionales, empresas, organizaciones y organismos públicos que traten con datos personales a proteger los datos personales y su circulación.

En el caso de Bolivia no se cuenta con una organización, o leyes, que garanticen la protección de los datos personales; pero en la carta magna algunos artículos, hablan de la seguridad, protección, dignidad de las personas, acciones de protección de la privacidad, etc.

Así también, el Decreto supremo N. 1793 Reglamento para el Desarrollo de Tecnologías de Información y Comunicación, el capítulo II, abarca el tratamiento de datos personales, su protección, tanto en el sector privado y privado, en toda su modalidad, incluyendo entre estas las actividades de recolección, conservación, procesamiento, bloqueo, cancelación, transferencia, consultas.

2.7 Protección de los datos en una organización

Las organizaciones y empresas son también responsables del tratamiento de datos personales que recogen, es por ello, que deberán adoptar medidas y garantías necesarias para la seguridad de los datos de carácter personal, de forma que se evite su pérdida, no integridad, uso indebido, tratamiento o acceso no autorizado ya sea en medio físico o digital, estas son, responsables de la

filtración de cualquier dato. Por lo tanto, la empresa de Facebook que sufrió la "fuga de datos de 50 millones de usuarios estadounidenses, aprovechada por la consultora Cambridge Analytics para afinar con perfiles psicológicos para atraer votos en la campaña de Donald Trump en 2016". (El País, 2018). Cabe señalar que, muchas organizaciones internacionales lucran con los datos personales, para obtener beneficios por medio de estos.

En todo caso los resultados anteriores, provocaron que "las acciones de Facebook cayeron un 19% que representa una pérdida de 119.000 millones de dólares, es la mayor pérdida de un día para cualquier compañía pública en la historia, según Thomson Reuters" (El País, 2018). Es decir, que la inadecuada protección que se proporciona a los datos personales, derivó en la caída de las acciones de la empresa. Es por ello, que la protección de datos en una organización es muy importante, debido a que, estos son un activo muy valioso de carácter económico.

2.7.1 Activos de información

La información, que resulta fundamental para las organizaciones es lo que se denomina como activo. Los activos de información son el bien más importante que posee una empresa u organización, para Ladino, Villa y López, un activo es "La información es el instrumento fundamental para el funcionamiento de las empresas y la operación de los negocios, esto hace que la información deba protegerse como el activo más importante de la organización." (Ladino A., Villa S., & Lopez E., 2011) (párr. 5)En efecto, una organización cuenta con información de valor vital la cual se encuentra en distintos soportes, así como en archivos establecidos.

En conclusión, un activo es aquello que tiene algún valor para la empresa y por lo tanto debe protegerse. Un Activo de Información incluye la información que se encuentre presente en forma impresa, escrita en papel, transmitida por cualquier medio electrónico o almacenada en equipos, incluyendo datos contenidos en registros, archivos y bases de datos. Como por ejemplo el

inventario de Activos, realizado por la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC).

Cuadro 12 Ejemplo de tipos de activos en MAGERIT

DATOS E INFORMACIÓN

Los datos, son el corazón que permite a una organización prestar sus servicios. La información es un activo abstracto que será almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos.

Nomenclatura	Tipos de datos/información
[files]	Ficheros
[backup]	copias de respaldo
[conf]	datos de configuración
[int]	datos de gestión interna
[password]	credenciales (ej. contraseñas)
[auth]	datos de validación de credenciales
[acl]	datos de control de acceso
[log]	registro de actividad
[source]	código fuente
[exe]	código ejecutable
[test]	datos de prueba

Fuente: Adaptado de Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC), publicado en el grupo de seguridad, productos, 2016, documento inventario de activos.

2.8 Seguridad de los datos en las operaciones

Dentro de toda organización, sea pública o privada, que tenga una estrecha relación con las tecnologías de la información y comunicación y con la sociedad de la información es necesaria la aplicación de la protección de los datos en las operaciones. En efecto, la accesibilidad de los datos es requerido para administrar una empresa u organización.

Cabe señalar, que una de las características en las relaciones laborales es la importancia de efectuar la protección de datos tal como se lo recalca a continuación:

> *En este vertiginoso mundo de las tecnologías de la información (TIC), se han venido planteando debates novedosos y diversos en las relaciones obrero-patronales, pero sin duda uno de los más importantes es el relativo a la privacidad y los datos personales de las partes en la relación laboral y en particular, del trabajador.* (Reynoso Castillo, 2017, p. 122).

Por ello, es necesaria e importante la protección de los datos en las operaciones, garantizando así la confidencialidad, integridad y disponibilidad. En el Estado Plurinacional de Bolivia la carta magna, recalca los derechos civiles a la privacidad, intimidad, honra, honor, propia imagen y dignidad.

2.9 Protección de los datos de los usuarios

La protección de datos de carácter personal de los usuarios y/o clientes, en una organización es muy importante, por ello se deben aplicar medidas de seguridad de toda su información, por ello, proteger los datos de los usuarios es proteger la economía de la organización, empresa, etc.

Así lo menciona Navia (como se citó en (Bustamante Paco, 2014), “el cliente es una persona que necesita consumir productos para subsistir, pero tiene el dominio de decidir una compra en el mercado. Un cliente no depende de la empresa, la empresa depende del cliente” (p. 46). En conclusión, los usuarios son como un activo más de las organizaciones, es por ello que debemos aplicar todas las medidas necesarias para garantizar la protección de sus datos personales. Una de las medidas aplicadas por el Reglamento General de Protección de Datos es la seudonimización.

2.9.1 Seudonimización

La seudonimización[79], es un proceso donde se remplazan los campos de información personal en un registro de datos, ya sea por identificadores artificiales o seudónimos, de manera que estos no puedan ser identificados con el titular.

Vista desde la perspectiva de su concepto, la seudonimización es poco conocida pero aplicada en el Reglamento General de Datos de la Unión Europea, que refleja la importancia del tratamiento de los datos personales. El Parlamento Europeo y el Consejo de la Unión Europea señalan que:

> *Esas garantías deben asegurar que se aplican medidas técnicas y organizativas para que se observe, en particular, el principio de minimización de los datos. El tratamiento ulterior de datos personales con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos ha de efectuarse cuando el responsable del tratamiento haya evaluado la viabilidad de cumplir esos fines mediante un tratamiento de datos que no permita identificar a los interesados, o que ya no lo permita, siempre que existan las garantías adecuadas (como, por ejemplo, la seudonimización de datos).* (El Parlamento Europeo y el Consejo de la Unión Europea, 2016, p. 33)

La seudonimización, se realiza a través de la identificación de las personas físicas, por medio de la minimización de sus datos. En efecto, esta información debe prevenir la exactitud en la identificación de las personas.

---

[79] Seudonimización: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

2.10 Principios de la protección de los datos

Los principios son reglas o normas para la aplicación de la protección de datos, es por ello, que cualquier organización, ya sea de carácter público o privado que almacena datos relacionados a la intimidad, privacidad personal y/o familiar, debe salvaguardarlos. Así lo indica la Constitución Política del Estado Plurinacional de Bolivia en el Artículo 130 I, que detalla:

> *Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad*. (Constitución Política del Estado Plurinacional de Bolivia, 2009, p. 47)

Es importante destacar que la Constitución Política del Estado protege la privacidad y los datos, los cuales pueden ser dados a conocer, eliminados, rectificados, impidiendo el uso de los mismos a otras personas, empresas, etc.

Tras el análisis del artículo de la Constitución Política del Estado Oporto Ordóñez (2015), realiza la siguiente aclaración en relación al artículo 130 de la Constitución.

> *Esta es una salvaguarda para la ciudadanía que puede ver vulnerado su derecho a la intimidad, al exponerse sus datos personalísimos en los bancos de datos, archivos que almacenan información nominativa individual, en cualquier formato o soporte, nuevo o por conocer*. (p. 87)

Esta aclaración es importante, porque la misma resalta la responsabilidad legal, la posesión y utilización de los datos personales y personalísimos. La misma impide que los datos se conviertan en una práctica de manipulación que afecte directamente el derecho fundamental de la intimidad y privacidad personal o familiar.

Puesto que Bolivia no cuenta con una ley que mencione los principios de protección de datos, analizaremos los de La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) de España, que menciona los siguientes principios:

- Calidad de los datos (art. 4)
- Derecho de información en la recogida de datos (art. 5)
- Consentimiento del afectado (art. 6)
- Datos especialmente protegidos (art. 7)
- Datos relativos a la salud (art. 8)

2.10.1 Calidad de los datos

Se refiere a los límites y restricciones en los que se basa la recogida y tratamiento de los datos de carácter personal. Así mismo refleja que estos no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. Por tal motivo, la recogida de datos por medios fraudulentos, desleales o ilícitos están prohibidos.

Es decir, "El principio de calidad de los datos establece los límites que tiene una organización para el tratamiento de datos de carácter personal: recogida, uso, actualización, almacenamiento y cancelación" (Miguel Pérez, 2015, p. 104). En efecto, los datos obtenidos deben ser los correctos o adecuados y no excesivos, para responder a las finalidades para las que se haya obtenido. Por lo tanto, cabe mencionar que:

> *El responsable del tratamiento de los datos personales, tanto del sector público como del privado, deberá adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, tratamiento no autorizado, las que deberán ajustarse de conformidad con el estado de la tecnología, la naturaleza de los datos almacenados y los*

riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural. (Decreto Supremo N° 1793, 2011, p. 39)

Se quiere con ello significar, la responsabilidad de los profesionales de la información, son quienes deben optar en medidas de protección necesarias para la gestión de los datos personales de la organización, en coordinación con la unidad de Recursos Humanos, hoy Talento Humano.

2.10.2 Derecho de información en la recogida de datos

Esto refiere que los interesados, tienen el derecho de ser informados sobre la recogida de datos personales, así lo menciona Miguel Pérez (2015), y que lo desgloza en los siguientes puntos:

- *La existencia de un fichero o el tratamiento de datos de carácter personal al cual se va a incorporar o tratar los datos que suministre.*
- *La identidad y dirección del responsable del fichero o tratamiento o, en su caso, de su representante.*
- *Cuál es la finalidad de los datos recogidos.*
- *Los destinatarios de la información*
- *Carácter obligatorio o voluntario de aportar los datos solicitados.*
- *Las consecuencias de la obtención de los datos o de la negativa a proporcionarlos*
- *La posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición.*

El Decreto Supremo N° 1793 detalla una caracterización en relación a los datos personales:

Las personas a las que se les solicite datos personales deberán ser previamente informadas de que sus datos serán objeto de tratamiento, de la finalidad de la recolección y registro de éstos; de los potenciales destinatarios de la información; de la identidad y domicilio del responsable del tratamiento o de su representante; y de la posibilidad de ejercitar los derechos de acceso, rectificación, actualización, cancelación, objeción, revocación y otros que fueren pertinentes. Los

datos personales objeto de tratamiento no podrán ser utilizados para finalidades distintas de las expresadas al momento de su recolección y registro. (Decreto supremo N° 1793, 2011, p. 38)

En conclusión, de manera voluntaria u obligatoria, los interesados deben ser informados sobre el tratamiento y finalidad por los cuales se recogen sus datos.

2.10.3 Consentimiento del afectado

El tratamiento de los datos de carácter personal requerirá del consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. "Los datos personales objeto de tratamiento sólo podrán ser utilizados, comunicados o transferidos a un tercero, previo consentimiento del titular u orden escrita de autoridad judicial competente." (Decreto supremo N° 1793, 2011, p. 38). En conclusión, el interesado es libre de otorgar o no el consentimiento para el tratamiento de sus datos, salvo que la ley disponga lo contrario, en este caso este no puede oponerse.

2.10.4 Datos especialmente protegidos

Sin duda los datos especialmente protegidos son los que revelan información que puede ser de carácter muy comprometedor para una persona, los mismos, deben tomarse en cuenta muy escrupulosamente conforme como la ley lo indique.

Algunas características de los datos especialmente protegidos son las siguientes:

- Ideología.
- Afiliación sindical.

- Religión.
- Creencias.
- Origen racial.
- Salud.
- Vida sexual.

Nadie podrá ser obligado a declarar sobre los puntos anteriormente señalados, y los ficheros que contengan esta información deben ser cuidadosamente tratados.

2.10.5 Datos relativos a la salud

Son aquellos datos personales relativos a la salud física o mental de una persona, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.

Muchas organizaciones, ya sea instituciones o centros sanitarios públicos o privados adquieren información relativa a la salud de las personas, las cuales acuden a estos para ser tratados. Es por ello, que estas instituciones tienen que contar con el compromiso u obligación de tratar los datos personales con responsabilidad. Otra tarea prioritaria, para estas organizaciones es la de realizar medidas de acceso a estos datos personales, considerando bajo que políticas se podrá ceder esta información.

Miguel Pérez (2015), ejemplifica cuando es necesario consentir el acceso a la información personale en el area de la salud:

- Cuando el afectado concienta expresamente la cesión.
- La cesión esté autorizada por una ley.
- Cuando la cesión sea necesaria para solucionar una urgencia que requiera acceder a un fichero.

- Para realizar estudios epidemiológicos en los términos establecidos en la legislacion sobre sanidad estatal o autonómica. (p.124)

El Parlamento Europeo y el Consejo de la Unión Europea (2016), los datos relacionados al tema de salud, deben implantarse y ser tratados de acuerdo al reglamento. Así lo indica el considerado número (35) del Reglamento (UE) 2016/679 que menciona:

> *Entre los datos personales relativos a la salud se deben incluir todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro. Se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia, de conformidad con la Directiva 2011/24/UE del Parlamento Europeo y del Consejo (1); todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro.* (p.6)

El tratamiento de la seguridad de las categorías especiales de datos personales, sin el consentimiento del interesado, puede ser necesario por razones de interés público en el ámbito de la salud pública. Los mismos no deben dar lugar a que terceros, como empresarios, compañías de seguros o entidades bancarias, traten los datos personales con otros fines.

Los datos personales relativos a la salud deben contar con especial protección ya que su divulgación daría paso a discriminaciones, agresiones, repudio hacia las personas que padezcan algún problema de salud.

A partir de estas percepciones sobre, la información personal de la salud. Tal como, el ejemplo en Bolivia del caso de Gualberto Cusi, se contempla que:

> *El ministro de Salud, Juan Carlos Calvimontes, salió este lunes para revelar el mal que padece. "En los últimos días hemos estado viendo con mucha preocupación que siguen manteniendo la posición de acusar a miembros del Gobierno y a terceras personas sobre el estado de salud del señor Gualberto Cusi, al respecto debo manifestar al pueblo en general que la enfermedad que (sufre) data de largos años de evolución, en diciembre de 2012 el señor Gualberto Cusi fue diagnosticado con el síndrome de inmunodeficiencia adquirida SIDA", dijo Calvimontes, quien convocó a una conferencia de prensa para hacer sus declaraciones. Las afirmaciones de Calvimontes, quien es médico de profesión, generaron un inmediato rechazo en las redes sociales porque la Ley 3729 del 8 de agosto de 2007 determina que las personas que sufren este mal tienen derecho a la reserva.* (Erbol, 2018)

Este hecho generó mucha polémica y al mismo tiempo discriminación hacia Gualberto Cusi, todo por revelarse la enfermedad que padecía. Este fue un hecho que vulneró la ley 3729. Dando como resultado la poca seguridad y tratamiento que existe hacia estos datos relacionados con la salud. En conclusión, los datos relativos a la salud deben ser revelados solo en casos de emergencia o para otros fines que se mencionan anterior; pero no para generar discriminación y repudio hacia las personas.

2.11 Firma digital

El concepto de firma digital nació como respuesta al avance tecnológico que ha generado nuevas formas de comunicación y comercialización, entrando así al mercado globalizado. De ahí que, las organizaciones tienen la necesidad de prestar servicios por medio de herramientas tecnológicas cada vez más avanzadas, con el fin de reducir costos, ahorrar tiempo, automatizar procesos, proporcionar información veraz y oportuna. En efecto una de estas es el internet que permite el contacto diario con millones de personas, donde toda la información se encuentra disponible y los tiempos de respuesta son cada vez menores.

En consecuencia, para garantizar la seguridad de los datos en la sociedad de la información, es necesario disponer de diversos métodos, uno de ellos es la firma digital; pero ¿que entendemos por este concepto? A continuación, se caracterizará todo lo referido a la firma digital. En los siguientes conceptos:

a) Según la (Real Academia Española, 2017), define la firma como:

- Rasgo o conjunto de rasgos, realizados siempre de la misma manera, que identifican a una persona y sustituyen a su nombre y apellidos para aprobar o dar autenticidad a un documento.

- Razón social o empresa.

b) Así mismo (Conde & Arteaga, 2011), aclara que firma es el "Nombre o apellido de una persona, que se pone, con rúbrica o sin ella, al pie de un escrito para darle validez y autenticidad. Designa el nombre de una casa de comercio y razón social." (p. 131)

En conclusión, la firma es el nombre, apellido y conjunto de rasgos, que una persona o empresa escriben con su propia mano al pie de un documento, para otorgarle validez, no repudio

y autenticidad al mismo, con fines identificativos, jurídicos, bancarios, representativos y diplomáticos.

Del mismo modo, digital es entendido como:

- Referente a los números dígitos.
- Dicho de un aparato o de un sistema: Que presenta información, especialmente una medida, mediante el uso de señales discretas en forma de números o letras.

Así también, "Se refiere a la representación de datos de forma discreta (discontinua) a diferencia de analógico, que denota la representación en forma continua" (Conde & Arteaga, 2011) (p. 93)

En resumen, digital es en conjunto de datos de un sistema, representados de forma discreta, por medio de señales, números y letras.

Así mismo algunos autores definen firma digital como:

a) (Lopez, Botero, & Durango, 2011). "La firma digital es equivalente a la firma manuscrita y permite incorporar las garantías de seguridad: autenticidad, confidencialidad, integridad y no repudio. Además, identifica (con una llave criptográfica) a una persona autora y emisora (certificada) de un documento informático." (p. 9)

Esto quiere decir, que la información ya no necesariamente tiene que estar en un soporte físico como el papel, simplemente es almacenada en un dispositivo electrónico, la firma digital es una secuencia de caracteres alfanuméricos asociados a un mensaje que garantiza la integridad, la autenticidad y el no repudio del mensaje.

En consecuencia la firma digital es un procedimiento, que consiste en aplicar a un documento digital, la clave privada del firmante (a través de la utilización de la criptografía asimétrica), la cual es de su exclusivo conocimiento y solo él tiene acceso, de modo que no puede negar su autoría (no repudio), permitiendo al receptor por medio del procedimiento de verificación, acreditarle identidad o autoría al firmante (autenticación) y detectar cualquier alteración del documento digital con posteridad a la firma (integridad).

A la vista, una firma digital se representa por una extensa e indescifrable cadena de caracteres (letras y números), que es el resultado del procedimiento matemático aplicado al documento.

b) Por otra parte, García plantea la siguiente definición:

La firma digital es una modalidad de firma electrónica que utiliza una técnica de criptografía asimétrica y que tiene la finalidad de asegurar la integridad del mensaje de datos a través de un código de verificación, así como la vinculación entre el titular de la firma digital y el mensaje de datos remitido. (García, 2008, p. 12)

Es decir, que la firma digital, es la firma electrónica que utiliza criptografía, que permite garantizar la identidad del firmante, integridad, confidencialidad y el no repudio de la información.

c) Paredes (2006) nos dice:

Una firma digital es un documento que permite garantizar la integridad de un documento y se puede relacionar de manera única al firmante con su firma, ya que realiza ésta con la llave privada y únicamente el firmante posee esa llave, esto se traduce en que se verifica la autenticidad del firmante. (p.13)

En conclusión, la firma digital es una modalidad de firma electrónica, equivalente a la firma manuscrita, representada de forma discreta por medio de un conjunto de datos en forma de números, letras o códigos basados en técnicas criptográficas. La información ya no tiene que estar en un soporte físico como el papel, simplemente es almacenada en un dispositivo electrónico, este identifica a una persona, sustituye a sus nombres y apellidos, representa la razón social de una empresa, etc. Al mismo tiempo permite garantizar las medidas de seguridad: autenticidad, confidencialidad, integridad y no repudio de la información, para darle validez y autenticidad a un documento, con el fin de garantizar que éste no ha sido alterado o modificado de ninguna forma desde su producción y firma.

La firma digital posee algunos atributos, según (Lopez, Botero, & Durango, 2011) estos son:

- Es única
- Es verificable
- Está bajo control exclusivo del iniciador
- Está ligada a la información del mensaje
- Está de acuerdo con la reglamentación. (p. 9)

Estos atributos permiten garantizar la eficacia de la firma digital, como garantía de la seguridad de la información.

2.12 Medidas de seguridad de la firma digital

La firma digital cumple con las siguientes medidas de seguridad:

2.12.1 Integridad

Algunos autores la definen como:

- Suárez (2013) nos dice que “Consiste en asegurar que la información no ha sufrido cambios no autorizados, ya sea de manera accidental o intencional, una vez firmado.” Pág. 36
- Al mismo tiempo Suárez indica que es una “Característica que indica que un mensaje de datos o un documento electrónico no han sido alterados desde la transmisión por el emisor hasta su recepción por el destinatario.” (Suárez, 2013, p. 31)

Es decir, que la integridad garantiza que la información no haya sido modificada, alterada, cambiada desde su transmisión por el emisor hasta el receptor.

2.12.2 Autenticación

La autenticación es el proceso de confirmar que algo y/o alguien es quien dice ser. Los siguientes autores la definen como:

- Para Suárez (2013), “Consiste en identificar al emisor del mensaje y sus atributos principales, asegurando que es la persona que figura como firmante en el documento” (P.36)
- De igual manera para Suárez es un, “Proceso técnico que permite determinar la identidad de la persona que emite un mensaje de datos firmado electrónicamente, vinculándolo con dicho mensaje (…)” (Suárez, 2013, p. 31)

En conclusión, la autenticación garantiza la identidad del emisor, permitiendo al receptor verificar con certeza que el documento procede del firmante.

2.12.3 No repudio

Otra de las medidas de seguridad de la firma digital es el no repudio, este garantiza que el firmante no rechaza la identidad de la firma. Como lo explica Suárez (2013)

Esta característica está ligada a la anterior, pues al autenticar la identidad del firmante, se evita que el emisor del mensaje pueda negar haberlo firmado. De esta manera se garantiza que el firmante está de acuerdo con el contenido del documento o se vincula con él de alguna forma (como autor, como revisor, dándose por enterado, etc.) (p. 36).

Esta medida, garantiza la autoría del firmante, permitiendo que este no niegue ni desconozca la información del documento, el cual tiene valor legal. No puede desconocer haber firmado un documento ante la evidencia de la firma. Garantizando el conocimiento y cumplimiento de la información del documento.

2.12.4 Confidencialidad

La última medida de seguridad es la confidencialidad, en su propuesta Torres (2016) nos plantea la siguiente definición:

La información sólo puede ser accedida y utilizada por el personal de la empresa que tiene la autorización para hacerlo. En este sentido se considera que este tipo de información no puede ser revelada a terceros, ni puede ser pública. Por lo tanto, debe ser protegida y es la que tiende a ser más amenazada por su característica. (p. 11)

Para Suárez (2013) "Consiste en impedir que la información del documento, contrato o firma, sea vista por usuarios no autorizados" (p. 37). En resumen, la confidencialidad garantiza y mantiene en secreto la información desde que es enviada por el emisor hasta el receptor. Evitando que terceros puedan acceder a ella.

2.13 Infraestructura de la firma digital

Es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución segura de operaciones criptográficas (como el cifrado, la firma digital, el

no repudio de transacciones electrónicas). Esta infraestructura se divide en dos partes el hardware y software.

2.14 Software

El software es el soporte lógico de un sistema, comprende los componentes lógicos. Este está escrito en lenguajes de programación.

Según el (Diccionario de la Real Academia de la Lengua Española) es: "Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora."

Según Conde & Arteaga (2011) en su glosario define el software como:

- *Conjunto de programas y sistemas operativos que forman el material intelectual necesario para el uso y funcionamiento de la computadora.*
- *Componentes lógicos (programas) de un ordenador. Se llama también lógica.*
- *Conjunto estructurado de instrucciones que permiten al computador ejecutar los trabajos que se le piden. Estas instrucciones se expresan en lenguaje que el computador entiende directamente, con el nombre del lenguaje de máquina y que está fundado en la numeración binaria, o en un lenguaje evolucionado, que se llama lenguaje de programación, que el computador traduce el lenguaje de máquina.* (p. 252)

En resumen, es el conjunto de programas de parte lógica, escrita en un lenguaje de programación, que hace posible el funcionamiento del mismo.

2.15 Hardware

Por otra parte, el hardware es la parte física, que constituye una computadora o un sistema informático.

Según el (diccionario de la real academia de la lengua española) “conjunto de aparatos de una computadora”

Para Conde & Arteaga (2011) en su glosario define el Hardware como, “todo el equipamiento físico (dispositivos, mecánicos, magnéticos, eléctricos y electrónicos) que constituye una computadora. También se denomina ferretería.”

En conclusión, el hardware es la parte física de un ordenador o sistema informático y todos ellos son: los componentes que logran que este funcione, está formado por elementos eléctricos, electrónicos, electromecánicos y mecánicos, como ser los circuitos de cables y de luz, placas, y cualquier otro material.

2.16 Criptografía

La criptografía es el arte y la técnica de escribir con procedimientos o claves secretas, de tal forma que lo escrito solo sea legible para quien pueda descifrarlo o tenga las claves de acceso. Según la Real Academia Española (2017), lo define como: “Del gr. κρυπτός kryptós 'oculto' y -grafía. Arte de escribir con clave secreta o de un modo enigmático.”

Por su parte (García, 2008) etimológicamente lo define como: “La palabra criptografía proviene del griego “kryptos” que significa ocultar y “grafos” que significa escribir, literalmente sería “escritura oculta.” (p. 10)

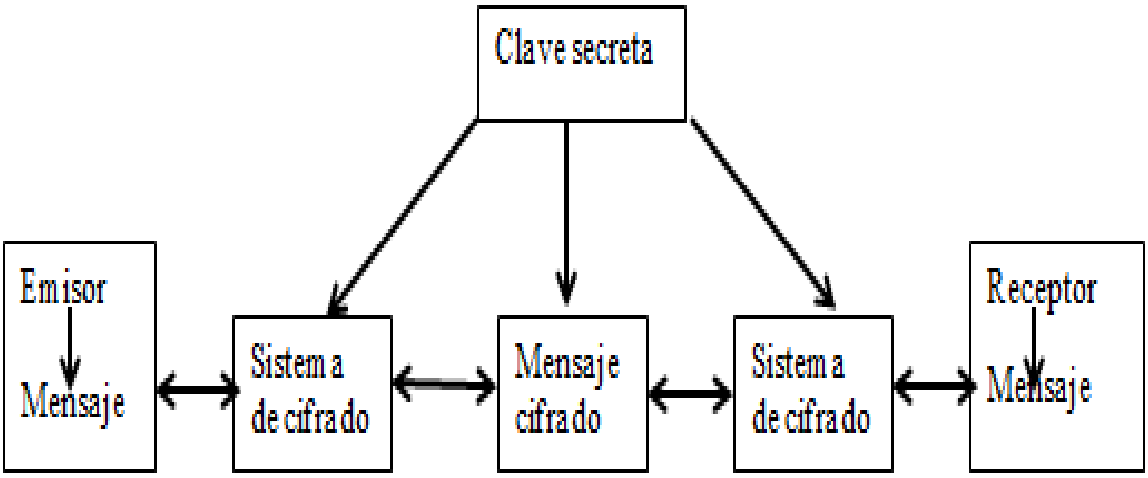
2.16.1 Criptografía simétrica

Es el tipo de criptografía que utiliza solo una clave para cifrar y descifrar el mensaje, tanto el emisor como el receptor deben conocer la misma. Este tiene un nivel débil de seguridad, porque la clave debe ser transmitida, diciéndola en alto, mandándola por correo electrónico o haciendo una llamada telefónica, esto pone en riesgo la seguridad de la información.

Según García (2008), este tipo de criptografía se usa para cifrar y descifrar mensajes, se basa en el uso de una única clave conocida de antemano por ambas partes. La seguridad de este tipo de criptografía radica principalmente en mantener en secreto la clave y no se preocupa necesariamente por el algoritmo de cifrado, es decir, que no es de mucha ayuda conocer el algoritmo que se utilizó (p. 6).

Esto quiere decir, que solo necesita una sola clave tanto para el emisor como para el receptor. Este tipo de clave conocida como secreta se debe de compartir entre las personas que se desea que vean los mensajes.

Figura 7 criptografía simétrica



Fuente: Elaboración Propia

2.16.2 Criptografía asimétrica

La criptografía asimétrica se basa en el uso de dos claves: la pública, que se podrá difundir sin ningún problema a todas las personas que necesiten mandarte algo cifrado y la privada, que no debe de ser revelada nunca. Este tipo es más seguro debido a las 2 claves.

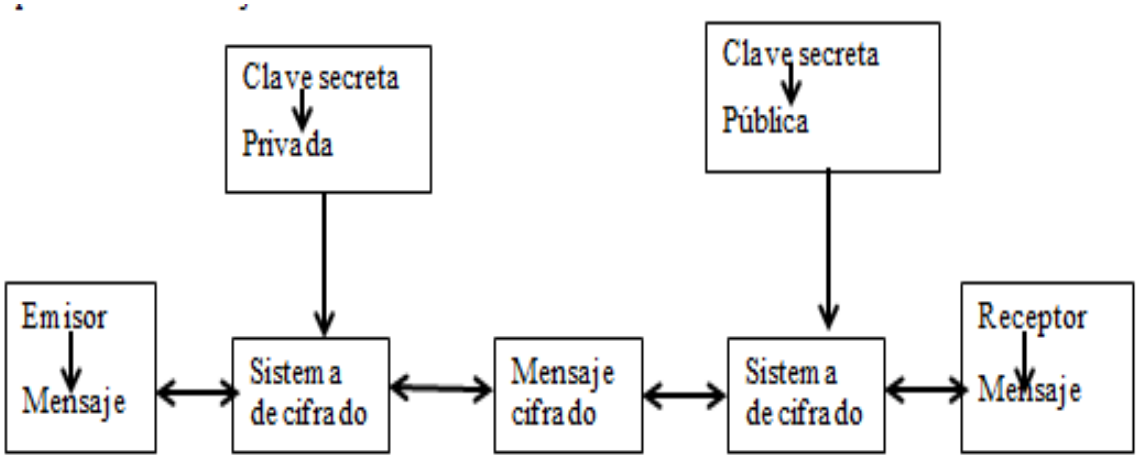
Por esto García (2008), define a la criptografía asimétrica como:

La que utiliza un par de claves (clave pública y clave privada) para el envío del mensaje, una para cifrar y otra para descifrar el mensaje; lo que se cifra en emisión con una clave, se descifra en recepción con la clave inversa. (p.7)

Ambas claves son propias de cada persona, la clave privada no se transmite nunca y se mantiene secreta. La clave pública, por el contrario, se puede y se debe poner a disposición de cualquier persona, pues con esa finalidad fue creada.

Es importante destacar que para este tipo de criptografía lo que se cifra con una llave se puede descifrar con la otra llave. Como se observa en la imagen:

Figura 8 Criptografía asimétrica



Fuente: Elaboración Propia

Del mismo modo Suárez (2013) nos plantea la siguiente definición:

Es una técnica basada en el uso de un par de claves únicas; una clave privada y una clave pública relacionadas matemáticamente entre sí de tal manera que una no pueda operar sin la otra y de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada. Se puede cifrar un mensaje con la clave pública y descifrar con la privada, dando

confidencialidad al mensaje, ya que sólo podrá ser visto por el usuario con la correspondiente clave privada. (p. 30–31)

Este tipo de criptografía es más segura, se debe a que se basa en el uso de 2 claves una privada para el emisor que no debe ser revelada, manteniendo su confidencialidad y otra pública para el receptor, que puede ser revelada a los receptores necesarios.

2.16.3 Clave pública

Para Suárez (2013) "en un sistema de criptografía asimétrica, es aquella usada por el receptor de un mensaje de datos para verificar la firma digital puesta en dicho mensaje y que puede ser conocida por cualquier persona." (p. 32). En conclusión, esta clave puede ser revelada a los receptores necesarios para descifrar el mensaje.

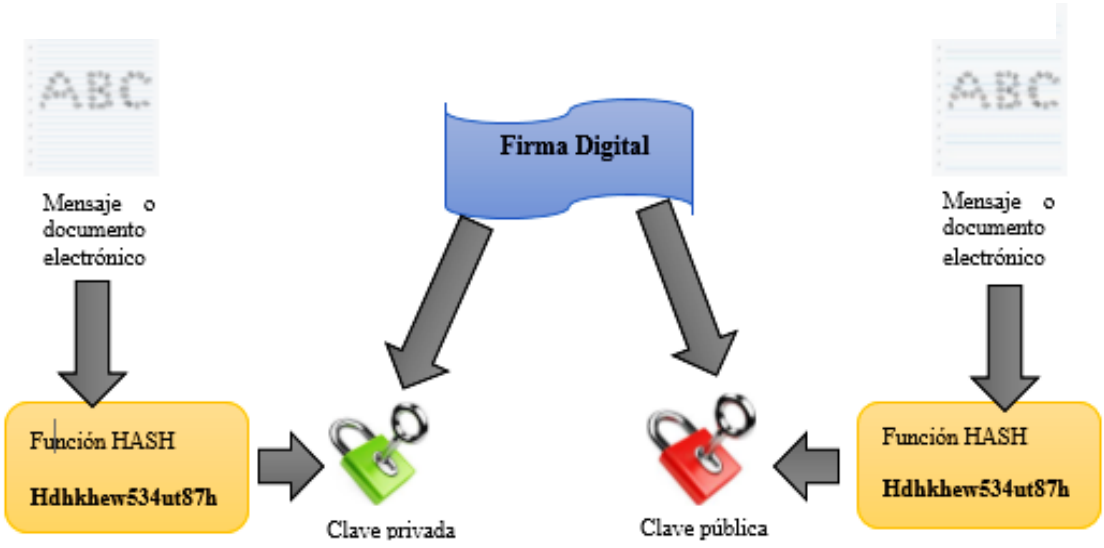
2.16.4 Clave privada

Por otro lado, la clave privada "En un sistema de criptografía asimétrica, es aquella que se emplea para generar una firma digital sobre un mensaje de datos y es mantenida en reserva por el titular de la firma digital." (Suárez, 2013, p. 33). En efecto, esta clave no debe ser revelada y debe mantenerse en secreto para garantizar la seguridad de la firma digital.

2.16.5 Hash

Cuando se firma un documento, se genera una huella digital única, llamada "hash", es creada usando un algoritmo matemático que transforma cualquier bloque de datos en una serie de caracteres. El hash es específico para cada documento; pero hasta el más mínimo cambio en el documento resultará en un hash diferente.

Figura 9 Ejemplo de aplicación de hash en la información



fuente Elaboración propia

El análisis precedente, contempla la aplicación de un Hash para la buena protección de la información, donde "La cadena Hash, la cual es una secuencia de valores derivados consecutivamente de una función Hash y un valor inicial. Debido a las propiedades de la función hash, es relativamente fácil calcular sucesivamente valores encadenados" (Montiel, Hernandez, Lizama, Lizama, & Simancs, 2017, p. 24). En efecto, esta cuenta permite garantizar la integridad de unos datos necesarios, estratégicos o especialmente protegidos.

Por ejemplo, el hash del nombre, Brian, es: 75c450c3f963befb912ee79f0b63e563652780f0. Muchos cometen el error de confundir "Brian" con "Brain" (cerebro, en inglés) lo cual genera otro Hash 8b9248a4e0b64bbccf82e7723a3734279bf9bbc4. (Kaspersky Daily, 2014) Ambos hash cuentan con 40 caracteres de longitud, porque ambas cuentan con 5 caracteres. Al generar un hash de un documento entero se cuentan todos los caracteres, al igual que los espacios. Que se dividen en bloques de 40 caracteres cada uno.

2.17 Certificado digital

Es un documento electrónico, generado por una entidad o autoridad de certificación. Este vincula las claves tanto pública y privada, con la persona natural o jurídica, para confirmar su identidad. Autores como García (2008) lo definen como:

> *Un documento electrónico generado y firmado digitalmente por una entidad de certificación, la cual vincula a un par de claves con una persona determinada, confirmando su identidad. La información que contiene el certificado digital son datos que identifican indubitablemente al suscriptor, los datos que identifiquen a la Entidad de Certificación, la clave pública, la metodología de verificación de la firma digital del suscriptor, el número de serie del certificado, la vigencia del certificado y la firma digital de la Entidad de Certificación. Cualquier información adicional debe ser solicitada a la entidad pertinente, la cual deberá comprobar fehacientemente la veracidad de ésta.* (p. 33)

En resumen, este certificado digital, es el documento electrónico que permite garantizar las medidas de seguridad de la firma digital, dándole valor legal. Obligando a cumplir obligaciones y responsabilidades suscritas en los documentos firmados digitalmente.

El certificado digital permite garantizar:

- *Identidad y capacidad de las partes que tratan entre sí sin conocerse (emisor y receptor del mensaje),*
- *Confidencialidad de los contenidos de los mensajes (ni leídos, ni escuchados por terceros),*
- *Integridad de la transacción (no manipulada por terceros),*
- *Irrefutabilidad de los compromisos adquiridos.*
- *No Repudio: ofrece protección a un usuario frente a que otro usuario niegue posteriormente que en realidad se realizó cierta comunicación.* (Lopez, Botero, & Durango, 2011, p. 10)

2.18 Entidad Certificadora en Bolivia

Una de las entidades para la certificación de la firma digital, es la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB), entidad certificadora dentro del sector público y población en general, conforme a la Ley N 164 General de Telecomunicaciones, Tecnologías de la información y Comunicación[80], cabe recalcar que:

Un certificado digital emitido por la ADSIB le permite al signatario o usuario realizar firmas digitales avanzadas y autenticar su identidad con validez legal, vincula un documento digital o mensaje electrónico de datos y garantiza la integridad del documento digital o mensaje electrónico con mensaje digital. Agencia para el Desarrollo de la Sociedad de la Información en Bolivia ADSIB (2017).

Esta entidad otorga 3 tipos de certificado digital que son:

Cuadro 13 Tipos de certificado digital

Tipo	Uso
Persona natural	Firma de documentos, protección de correo electrónico, autenticación de sitio web, firma de código informático
Persona jurídica	En representación de una persona jurídica: firma de documentos, protección de correo electrónico, autenticación en sitio web, firma de código informático
Cargo público	Como servidor público: firma de documentos, protección de correo electrónico, autenticación en sitio web, firma de código informático

Fuente: Adsib, firma digital, tipos de certificado digital

[80] Ley N 164 General de Telecomunicaciones, Tecnologías de la Información y Comunicación

CAPITULO III - MARCO METODOLÓGICO

La metodología puntualiza la aplicación del estudio final, que define: cuándo, dónde y cómo se realizará la concentración de recolección de datos.

3.1 Diseño metodológico

La investigación es cuantitativa y de diseño **deductivo**, porque se tomarán datos generales para llegar a lo concreto. Por tanto, hace uso de la base de datos abierta de la Encuesta TIC, que permite el análisis de la sociedad de la información en Bolivia, el diseño ayudara a la recolección de datos sobre la sociedad que crece y se desarrolla alrededor de la información y su clasificación en acceso y uso de las herramientas TIC, asimismo, el enfoque cuantitativo, permite, analizar desde el problema hasta afirmar o refutar la hipótesis planteada en la investigación, sobre todo, implica una recolección de datos a través de estadísticas, números medibles y analizable, también se utilizó la Encuesta de Opinión Nacional en Tecnologías de la Información y Comunicación, que permite el análisis y la categorización del acceso y uso de las herramientas TIC por parte de distintos grupos poblacionales.

El tipo de estudio del presente trabajo **descriptivo,** ya que estudia las propiedades, las características y perfiles de las personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que, en el presente caso, es la sociedad de la información en Bolivia.

3.2 Sujeto

El primer grupo de la población está compuesta por el Comité de Calidad, Seguridad de la Información y de Emergencia de la ADSIB, conformados por 9 funcionarios con las funciones de garantizar, coordinar, evaluar, aprobar iniciativas de calidad de los servicios y seguridad de la información. El cual, está conformado por los siguientes miembros:

- Directora o Director Ejecutivo de la ADSIB
- Asesor Legal
- Jefe de la Unidad de Innovación y Desarrollo
- Jefe de la Unidad de Infraestructura de Servicios
- Jefe de la Unidad Administrativa Financiera
- Jefe de la Unidad de Gestión de Servicios
- Profesional en Seguridad de la Información
- Profesional en Calidad de los Servicios
- Otros designados por la Dirección Ejecutiva

El segundo grupo está compuesto por la Sociedad de la Información en Bolivia, Identificado mediante la Encuesta de Opinión Nacional sobre Tecnologías de la Información y Comunicación[81], realizado por la Agencia de Gobierno Electrónico y Tecnologías de la Información y Comunicación (AGETIC), con la característica en Datos Abiertos[82], para ser utilizados de forma libre y sin restricciones, con el fin de promover el acceso a información pública, la participación social, la innovación y la mejor toma de decisiones.

Es por ello, que obteniendo la ponderación de la muestra de 5033 internautas encuestados, que corresponde a la población de mayores de 14 años, donde el resultado ajustado por departamento

[81] Encuesta de Opinión Nacional en Tecnologías de la Información y Comunicación: https://datos.gob.bo/dataset/encuesta-nacional-de-opinion-sobre-tic

[82] Datos Abiertos en Bolivia: https://datos.gob.bo/about

y localidad (urbana/ rural), y su aplicabilidad permitieron obtener estadísticas y frecuencias con representatividad a nivel nacional, departamental y estrato geográfico para la población mayor de 14 años, con el fin de analizar la relación que existe entre esta sociedad y la seguridad de la información y protección de datos personales.

Selección de la Muestra

Para la identificación de la muestra (grupo de la población o universo), es necesario delimitarla para generalizar los resultados y establecer parámetros con lo siguiente:

Probabilística aleatoria

Será probabilística estratificada, tomando en cuenta el número de población internauta de la sociedad de la información en Bolivia que son 5033, plasmado en la Encuesta de Opinión Nacional en Tecnologías de la Información y Comunicación proporcionado por la AGETIC, donde la misma estuvo dirigida a los internautas de 14 y más años de edad, de las áreas urbana y rural de Bolivia. En efecto, la población Internauta es aquella persona que tuvo acceso a Internet al menos una vez en los últimos 30 días previos a la encuesta.

En contraste, el nivel de confianza que tiene de la encuesta aplicada por la AGETIC es de un 95%, sin embargo, se tiene un error de la muestra de ±1.3% para el conjunto de la muestra a nivel nacional y de ±4% a nivel departamental, usando fórmulas estándar para el cálculo de error de muestreo. Cabe señalar, que la investigación está orientada a describir el conjunto de la muestra a nivel nacional. Además, el tipo de muestra empleado por la AGETIC en la encuesta es muestreo

Multietápico[83] por conglomerados[84]. Tamaño de la muestra. 5.536 encuestas (base agregada conformada por 5.033 encuestas a Internautas y 503 a No Internautas). Asimismo, la encuesta fue realizada en fecha de 3 al 18 de diciembre de 2016.

Como resultado, la encuesta fue publicada en diciembre de 2017 y proporciona una aplicabilidad y alcance para investigar a la sociedad de la información boliviana, en relación al comportamiento y uso que facilitan las tecnologías de la información y comunicación, en la creación, distribución y manipulación de la información.

No probabilística

Esta muestra es dirigida al subgrupo de la población en la que los elementos no dependen de la probabilidad, sino de las características de la investigación. La cual elige a toda la población en temas de seguridad compuesta por el Comité de Calidad, Seguridad de la Información y de Emergencia de la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB). (Ver anexo 3)

Materiales

La fuente de información más valiosa en el uso y recolección de datos, fueron los distintos materiales que se obtuvieron, desarrollaron y encontraron. En efecto, esta información se obtuvo

[83] Multietápico: Se trata de combinar dos o más diseños muestrales.
Habitualmente la primera etapa en un muestreo multietápico consiste en la aplicación de un muestreo por conglomerados. Una vez seleccionados los conglomerados, en cada uno de ellos se puede aplicar un muestreo aleatorio simple, estratificado, sistemático o un segundo muestreo por conglomerados.
Como puede deducirse, en dos o tres etapas (no suele haber más) hay bastantes posibilidades de combinar los diseños muestrales estudiados.

[84] Conglomerados: es una técnica utilizada cuando hay agrupamientos "naturales" relativamente homogéneos en una población estadística.

a través: reuniones, participaciones, encuestas, análisis en bases de datos libres y fuentes bibliográficas los cuales fortalecieron el desarrollo y entendimiento del estudio.

Se utilizaron instrumentos como: Encuesta Nacional de Opinión sobre Tecnologías de la Información y Comunicación, con el de obtener información representativa a nivel nacional, urbano/ rural y departamental, sobre el acceso y usos de Tecnologías de Información y Comunicación (TIC), servicios de Gobierno Electrónico y equipamiento de la población internauta de 14 o más años de edad, proporcionado por la Agencia de Gobierno Electrónico y Tecnologías de la Información y Comunicación (AGETIC), de las cuales se interpretaron 46 preguntas en relación al tema de investigación. Asimismo, se realizó una entrevista al el Comité de Calidad, Seguridad de la Información y de Emergencia conformado por 9 funcionarios de la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB), donde se abarcaron preguntas abiertas en relación a la seguridad de la información y protección de datos personales. (Ver anexo 2)

También se participó en el grupo de Seguridad del Consejo para las Tecnologías de Información y Comunicación del Estado Plurinacional de Bolivia (CTIC-EPB), en el desarrollo de los Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las Entidades del sector público.

Procedimientos.

El análisis de la información e investigación se desarrolló en la perspectiva de observación y estudio de la Sociedad de la Información en Bolivia, además, contemplando la seguridad de la información y protección de datos personales a nivel internacional como nacional. Asimismo, se revisó y participó en la colaboración de los documentos del grupo de Trabajo de Seguridad de la Información, conformado por la Agencia de Gobierno Electrónico y Tecnologías de la

Información y Comunicación. En consecuencia, la investigación vislumbro el enfoque cuantitativo y descriptivo, por lo cual se hizo uso de la base de Datos Abiertos de la Encuesta Nacional de Opinión sobre Tecnologías de la Información y Comunicación, permitiendo la identificación y análisis de la sociedad de la información en temas de seguridad de la misma.

La clasificación que se hace de la sociedad de la información, por los distintos comportamientos que genera la población internauta, a partir de los datos plasmados en la encuesta TIC, se estableció una sociedad específica, que se desarrolla y crece alrededor de la información y su relación a su actividad económica, donde se relaciona al uso de las tecnologías de la información y comunicación, con su información personal e información que almacena y gestiona de su actividad laboral, que parte de igual forma de los datos plasmados en la encuesta TIC.

CAPÍTULO IV - RESULTADOS

En el presente capítulo de la investigación, se presenta una descripción de lo encontrado por medio de la entrevista realizada al grupo de seguridad de la Agencia para el Desarrollo de la sociedad de la Información en Bolivia (ADSIB), en relación a las medidas de seguridad de la información, protección de datos personales y firma digital.

En la segunda fase se describen los resultados obtenidos a través del manejo estadístico de los datos. Atendiendo al objetivo general de la investigación, así como considerando a los objetivos específicos, se muestra lo encontrado en la primera fase de la investigación, en la cual la información obtenida gracias a la encuesta nacional de opinión sobre tecnologías de información y comunicación realizada por la Agencia de Gobierno Electrónico y Tecnologías de la Información y Comunicación (AGETIC), cuya base de datos libres nos proporciona información en relación al uso de las tecnologías de la información y comunicación que está ajustada por departamento y localidad (urbana/rural).

4.1 Seguridad de la información en la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia.

La Agencia para el desarrollo de la Sociedad de la Información en Bolivia, es una entidad pública, creada el 19 de marzo de 2002, mediante el Decreto Supremo 26553.

La misma constituye como una entidad descentralizada bajo tuición de la Vicepresidencia del Estado Plurinacional de Bolivia. La ADSIB es la encargada de proponer políticas, implementar estrategias y coordinar acciones orientadas a reducir la brecha digital en el país, a través del impulso de las Tecnologías de la Información y Comunicación en todos sus ámbitos, teniendo

como principal misión favorecer relaciones del Gobierno con la Sociedad, mediante el uso de tecnologías adecuadas.

En este punto se describe la entrevista realizada al Comité de Calidad, Seguridad de la Información y Emergencia de la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB).

Cuadro 14 ¿Cuenta la ADSIB con políticas de acceso a la información?

RESPUESTA
Específicamente con ese nombre no, pero se tiene niveles de control tanto en ambientes de sistemas y procedimentales enmarcados dentro del marco normativo legal como ser la Resolución Administrativa Regulatoria RAR -DJ-RA TL LP 32/2015 emitido por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT), y la ley N° 164, Ley General de Telecomunicaciones y Tecnologías de Información y Comunicaciones y el Decreto Supremo reglamentario N° 1793.
Adicionalmente se cuenta con una Política de Protección de Datos Personales, en el cual se indica que se regirán por los siguientes principios:
Principio de Finalidad.- La utilización y tratamiento de los datos personales por parte de las entidades certificadoras autorizadas, deben obedecer a un propósito legítimo, el cual debe ser de conocimiento previo del titular;
Principio de Veracidad.- La información sujeta a tratamiento debe ser veraz, completa, precisa, actualizada, verificable, inteligible, prohibiéndose el tratamiento de datos incompletos o que induzcan a errores;
Principio de Transparencia.- Se debe garantizar el derecho del titular a obtener de la entidad certificadora autorizada, en cualquier momento y sin impedimento, información relacionada de la existencia de los datos que le conciernan;
Principio de Seguridad.- Se debe implementar los controles técnicos y administrativos que se requieran para preservar la confidencialidad, integridad, disponibilidad, autenticidad, no repudio y confiabilidad de la información, brindando seguridad a los registros, evitando su falsificación, extravío, utilización y acceso no autorizado o fraudulento;
Principio de Confidencialidad.- Todas las personas involucradas y que intervengan en el tratamiento de datos personales, están obligadas a garantizar la reserva de la información, incluso hasta después de finalizado su vínculo con alguna de las actividades que comprende el tratamiento, pudiendo únicamente realizar el suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las tareas autorizadas.

Fuente: Elaboración Propia

Sobre la base de las ideas expuestas, la ADSIB, cuenta con niveles de inspección que se efectúa en ambientes de sistemas o de procedimiento, donde se recalcan las medidas para salvaguardar la inviolabilidad de las telecomunicaciones y protección de la información establecidos por medio del artículo 56 de la ley Número 164, donde se establece la inviolabilidad y secreto de las comunicaciones.

Por su parte, la ADSIB desarrolló un documento en el cual se conciben los términos y condiciones para la provisión de servicio de firma y certificado digital, en el cual la entidad certificadora cumple los requisitos técnicos, con la exigencia de términos y condiciones de servicio con los suscriptores de la Resolución Administrativa Regulatoria RAR -DJ-RA TL LP 32/2015.

Cuadro 15 ¿Cree usted que es necesario la regulación de acceso a la información de la ADSIB, para el personal trabajador, también así para los clientes u usuarios?

RESPUESTA
La ADSIB tiene medidas de protección para el acceso de la información tanto para el personal operador del servicio y usuarios finales las mismas están en base a las POLÍTICAS DE CERTIFICACIÓN (CP) y DECLARACIÓN DE PRACTICAS DE CERTIFICACIÓN (CPS), Políticas de Seguridad y procedimientos internos.

Fuente: Elaboración propia

Considera que, los controles de seguridad se enmarcan en los lineamientos establecidos en la Resolución Administrativa RAR -DJ-RA TL LP 31/2015 emitida por la ATT.

Donde la ubicación del Centro de Datos de la ADSIB está en el Edificio de la Vicepresidencia del Estado Plurinacional de Bolivia, ubicado en el centro de la ciudad de La Paz, entre las calles Ayacucho y Mercado No 308.

Del mismo modo, la construcción del Centro de Datos reúne y mantiene los requisitos de operación que para este tipo de facilidades impone la normativa en materia de seguridad. El

Centro de Datos opera las veinticuatro (24) horas del día, los trescientos sesenta y cinco (365) días del año.

Adicionalmente el Centro de Datos reúne condiciones y características de construcción para hacer frente a diferentes situaciones de emergencia. Igualmente, mantiene un perímetro de seguridad y cuenta con cinco (5) niveles de acceso biométrico.

Cuadro 16 ¿Cree usted que se puede dejar de poner a disposición de los empleados toda la información suficiente para que puedan desarrollar su trabajo?

RESPUESTA
No, la información relacionada al servicio es procesada en diferentes etapas para la emisión del certificado digital, etapas que son realizadas por usuarios que tienen un rol específico dentro de cada proceso hasta la emisión del certificado digital, tomando en cuenta los principios de confidencialidad e integridad de la información. Cabe recalcar que para el procesamiento solo se maneja información vital para las diferentes consultas y las respuestas obtenidas por los servicios web se rigen bajo estos parámetros.

Fuente: Elaboración propia

Si bien es cierto que, la disposición de la información al personal para que puedan desarrollar su trabajo, la ADSIB regula la información relacionada al tipo de servicio que procesa. Donde cada personal tiene un rol específico, donde se consideran los principios de confidencialidad e integridad de la información.

Cuadro 17 ¿Considera usted de que si no se da toda la información de la ADSIB a los empleados estos podrían realizar su trabajo?

RESPUESTA
Para el funcionamiento del servicio los usuarios operadores tienen la información necesaria para procesar la información según el rol que tengan.

Fuente: Elaboración propia

La afirmación anterior, donde la ADSIB considera brindar toda la información a los empleados para realizar sus responsabilidades, reflexiona que, para un buen funcionamiento del servicio los operadores tienen acceso a la información necesaria para procesar el rol que posean.

Cuadro 18 ¿Usted idéntica algún el tipo de información que la ADSIB se debería proteger? Y si lo hace mencione las medias ADSIB realiza para protegerla.

RESPUESTA
Al hablar de Certificación Digital se entiende que todo el proceso de registro, hasta la emisión del certificado es crítico, es decir en todo ese periodo la información proporcionada por el usuario es protegida por las diferentes amenazas, vulnerabilidades e identificando un nivel de riesgo para cada una de ellas, toda esta información se encuentra en las POLÍTICAS DE CERTIFICACIÓN (CP), DECLARACIÓN DE PRACTICAS DE CERTIFICACIÓN (CPS) y otros documentos relacionadas a la gestión de la información que son internas.

Fuente: Elaboración propia

Expresó por otra parte, la ADSIB que es consciente del tipo de información que corresponde proteger, donde la gestión de la información interna se expresa en las políticas de certificación y declaración de prácticas de certificación.

Cuadro 19 ¿La ADSIB cuenta con controles y clasificación de la información? Podría mencionar algunas

RESPUESTA
Se tiene documentación respecto a ese tema, en función de la criticidad de la información manejada. Por ejemplo, la información relacionada a cada certificado tiene una criticidad alta por tanto su almacenamiento debe tener medidas de seguridad tanto físicas como lógicas, los procedimientos de actualización del servicio y copias de seguridad tienen controles de protección dentro de dispositivos de almacenamiento como ser cajas fuertes de seguridad.

Fuente: Elaboración propia

Otra tarea prioritaria, es la de mantener controles y clasificación de la información, donde la ADSIB cuenta con documentación para este efecto, respecto a la seguridad física así como logística, que cuentan con un respaldo de seguridad y controles de protección en dispositivos de almacenamiento y cajas fuertes de seguridad.

Cuadro 20 ¿La ADSIB cuenta con medidas de seguridad de la información en las operaciones? Podría mencionar algunas

RESPUESTA

Justamente este control se encuentra en las políticas de seguridad del servicio y tiene como fin garantizar y asegurar la consistencia de las tareas operacionales y su seguridad, todos los procedimientos operativos y de gestión de cambios, capacidad y respaldos asociados a la prestación del Servicio de Certificación Digital están debidamente documentados. Las actualizaciones, revisiones, correcciones y tratamiento de los mismos son realizadas con la periodicidad que los propios documentos lo determinan.
Si se presenta un cambio significativo relacionado a infraestructura, configuración, sistemas de información u otras aplicaciones en ambientes centro de datos relacionados al servicio, estas son debidamente documentadas antes de su ejecución y aprobadas por la Dirección Ejecutiva de la ADSIB.

Fuente: Elaboración propia

De acuerdo con la ADSIB, la misma cuenta con medidas de seguridad de la información en las operaciones, expresado en el documento de las políticas de seguridad del servicio, que garantiza la seguridad de las tareas operacionales.

Cuadro 21 ¿La ADSIB cuenta con alguna medida de protección de la información ante un incidente que atañe la seguridad de la información?

RESPUESTA
La ADSIB cuenta con Políticas de Gestión de Incidentes y su tratamiento.

Fuente: Elaboración propia

Por su parte, la ADSIB cuenta con Políticas de Gestión de Incidentes, que reaccionan con acciones ante algún incidente que atañe la seguridad de la información.

Cuadro 22 ¿La ADSIB realizo alguna capacitación al personal responsable, administrativo, o también así a los clientes u usuarios en temas de seguridad en el último año?

RESPUESTA
La capacitación es un tema fundamental en este tipo de servicios, el personal involucrado en la prestación del servicio tiene un plan capacitación anual coordinado y gestionado por el Comité de Calidad del Servicio justamente para mejorar el nivel de seguridad y servicio prestado, además de ser un requisito requerido por el ente regulador ATT.

Fuente: Elaboración propia

Estas evidencias, con que cuenta la ADSIB, demuestran las capacitaciones en relación a la seguridad de la información, tanto al personal involucrado, como en la prestación de servicios. También estaría cumpliendo con lo establecido por el ente regulador ATT.

Cuadro 23 ¿La entidad ha implementado lineamientos contra modificaciones o pérdida accidental de información?

RESPUESTA
Justamente se hizo una valoración de los activos de información relacionadas al servicio y dentro de las amenazas y vulnerabilidades de tomaron en cuenta estos aspectos que fueron reflejados en las políticas de seguridad, Política de Gestión de Incidentes y el Plan de Contingencia.

Fuente: 3 Elaboración propia

Llama la atención, el importante análisis sobre la valoración de los activos de información que tiene la ADSIB, donde identificó las posibles amenazas y vulnerabilidades solucionadas en las políticas de seguridad, políticas de gestión de incidentes y el plan de contingencia. En relación a posibles pérdidas accidentales de información.

4.2 Protección de datos personales en la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia.

La Agencia para el Desarrollo de la Sociedad de la Información en Bolivia, considera que es relevante analizar y considerar la implementación de regulación integral sobre la protección de los datos personales que gestionan a través de las Tecnologías de la Información y Comunicación, para condescender seguridad y protección a la intimidad del usuario que aprovecha la misma.

Cuadro 24 ¿La entidad ha implementado lineamientos, normas y/o estándares para proteger la información personal y privada de los ciudadanos que utilicen sus servicios?

RESPUESTA

Claro que sí, dentro de los lineamientos descritos por el ente regular en este caso la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transporte (ATT) para funcionar como Entidad Certificadora Publica se requiere que se cumpla la RAR ATT-DJ-RA-TL LP 32/2015 requisitos, términos y condiciones, Modelos de Contrato de Adhesión y otros aspectos para la prestación de servicios de certificación digital y la RAR ATT-DJ-RA-TL LP 31/2015 Documentos Públicos de la Entidad Certificadora Raíz; justamente dentro de estos requisitos se encuentra un documento denominado "Políticas de Protección de Datos Personales" que se encuentra inmersa en las Políticas de Certificación del Servicio de Certificación Digital.

Fuente: Elaboración propia

Estos resultados revelan, que la ADSIB, cuenta con compromiso de implementación de lineamientos, normas para proteger la información personal privada de los ciudadanos, expresada en los documentos descritos por el ente regulador que es la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT).

Cuadro 25 ¿Qué importancia tienen los datos personales para la ADSIB en la sociedad de la información?

RESPUESTA
La ADSIB entiende que los datos personales relacionados al servicio de certificación digital son un activo de información sumamente importante por tanto tiene implementadas medidas de seguridad tanto tecnológicas como procedimentales para su resguardo, preservando siempre la confidencialidad de las mismas.

Fuente: Elaboración propia

De las evidencias anteriores, la ADSIB reconoce la responsabilidad que se debe proporcionar a los datos personales, tanto en relación a su servicio de certificación digital, así como al de su personal administrativo e involucrados, por lo cual mantienen implementadas medidas de seguridad tanto tecnológicas como operacionales.

Cuadro 26 ¿Qué medidas de protección realiza la ADSIB ante la recogida de datos personales de los clientes, usuarios y personal administrativo?

RESPUESTA
Ante todo, respetar la normativa actual respecto al tratamiento de datos personales en materia de telecomunicaciones y el marco jurídico aplicable dentro del estado boliviano.

Respecto a la protección de los datos personales de los usuarios del servicio de certificación digital se tiene medidas tanto procedimentales como tecnológicas regidas por las Políticas de Certificación (CP) y Declaración de Practicas de Certificación (CPS).

Fuente: Elaboración propia

Como señalamos, la ADSIB mantiene una normativa en relación al tratamiento de datos personales en concordancia con las tecnologías de la información y comunicación y materia de telecomunicaciones, también así, lo expresa en los documentos relacionados por las políticas de certificación y declaración de prácticas de certificación.

Cuadro 27 ¿Cuáles son los datos personales especialmente protegidos por la ADSIB?

RESPUESTA
La ADSIB como Entidad Certificadora Pública considera que es relevante analizar y considerar la implementación de regulación integral sobre la protección de los datos personales que cursan a través de las TIC's, para otorgar seguridad y protección a la intimidad del usuario que navega en la red, en ese entendido todos los datos personales que contempla los tres tipos de certificados: cargos públicos, personas jurídicas y personas naturales se encuentran protegidos. Todos los datos requeridos para la emisión de certificados digitales se encuentran descritas en las Políticas de Certificación (CP) y Declaración de Practicas de Certificación (CPS) en las secciones Identificación y Autenticación y Requisitos mínimos para la obtención de Certificados Digitales.

Fuente: Elaboración propia

Como resultado revela, que la ADSIB adquiere todos los datos personales que contempla los tres tipos de certificados: cargos públicos, personas jurídicas y personas naturales, los mismos se encuentran especialmente protegidos, los cuales se encuentran descritos en las Políticas de Certificación (CP) y Declaración de Prácticas de Certificación (CPS) en las secciones Identificación y Autenticación y Requisitos mínimos para la obtención de Certificados Digitales.

Cuadro 28 ¿La ADSIB conoce o regula los datos obtenidos por terceros de la firma digital y la sociedad de la información?

RESPUESTA
No, solo conoce los datos estrictamente relacionados al Servicio de Certificación Digital.

Fuente: Elaboración propia

Sin embargo, el alcance de caracterización de datos por parte de la Sociedad de la Información de la ADSIB, sólo identifica los datos relacionados al Servicio de Certificación Digital.

Cuadro 29 ¿La ADSIB mantiene controles de protección en la recogida de datos, uso de datos, actualización y su almacenamiento? Podría mencionar algunas

RESPUESTA
En la interacción usuario-servicio desde la plataforma tecnológica del servicio de certificación digital solo se despliega los datos necesarios para dicha interacción, las mismas son almacenadas/actualizadas en equipos bajo medidas de seguridad, entre estas medidas se encuentran procedimientos de copias de seguridad cifradas en sitios externos, sistemas de copias de seguridad automatizadas descritas en las Políticas de Seguridad de la Información relacionada al servicio.

Fuente: Elaboración propia

Las evidencias revelan, que la ADSIB brinda protección en la recogida de datos, actualización y mantenimiento, un ejemplo es la certificación digital que solo despliega los datos necesarios para dicha interacción, las mismas son almacenadas/actualizadas en equipos bajo medidas de seguridad.

Cuadro 30 ¿La ADSIB considera que se da protección a los datos personales de las personas en las recientes invenciones y métodos de negocio de la sociedad de la Información en Bolivia?

RESPUESTA
Se protegen los datos personales solo de los servicios prestados.

Fuente: Elaboración propia

La situación descrita, revela que la ADSIB mantiene protegidos los datos personales de los servicios prestados por la entidad, una observación o recomendación es la de crear políticas de protección de datos personales más orientada a la sociedad de la información en Bolivia.

Cuadro 31 ¿Conoce usted las normas, leyes nacionales o internacionales relativas a la protección de los datos personales en lo que respecta al tratamiento y uso de las mismas? Podría mencionar algunos

RESPUESTA

La Ley N°164, Ley General de Telecomunicaciones, Tecnologías de Información Y Comunicación, en su Art. 56 (Inviolabilidad y Secreto de las Telecomunicaciones) señala: “En el marco de lo establecido en la Constitución Política del Estado, los operadores de redes públicas y proveedores de servicios de telecomunicaciones y tecnologías de información y comunicación, deben garantizar la inviolabilidad y secreto de las comunicaciones, al igual que la protección de los datos personales y la intimidad de usuarias o usuarios, salvo los contemplados en guías telefónicas, facturas y otros establecidos por norma”.

Por otro lado, el Art. 56 del Decreto Supremo N°1793 Reglamento para el Desarrollo de Tecnologías de Información y Comunicación, a fin de garantizar los datos personales y la seguridad informática de los mismos, adopta las siguientes previsiones:

a) La utilización de los datos personales respetará los derechos fundamentales y garantías establecidas en la Constitución Política del Estado;

b) El tratamiento técnico de datos personales en el sector público y privado en todas sus modalidades, incluyendo entre éstas las actividades de recolección, conservación, procesamiento, bloqueo, cancelación, transferencias, consultas e interconexiones, requerirá del conocimiento previo y el consentimiento expreso del titular, el que será brindado por escrito u otro medio equiparable de acuerdo a las circunstancias. Este consentimiento podrá ser revocado cuando exista causa justificada para ello, pero tal revocatoria no tendrá efecto retroactivo.

c) Las personas a las que se les solicite datos personales deberán ser previamente informadas de que sus datos serán objeto de tratamiento, de la finalidad de la recolección y registro de éstos; de los potenciales destinatarios de la información; de la identidad y domicilio del responsable del tratamiento o de su representante; y de la posibilidad de ejercitar los derechos de acceso, rectificación, actualización, cancelación, objeción, revocación y otros que fueren pertinentes. Los datos personales objeto de tratamiento no podrán ser utilizados para finalidades distintas de las expresadas al momento de su recolección y registro;

d) Los datos personales objeto de tratamiento sólo podrán ser utilizados, comunicados o transferidos a un tercero, previo consentimiento del titular u orden escrita de autoridad judicial competente;

e) El responsable del tratamiento de los datos personales, tanto del sector público como del privado, deberá adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, tratamiento no autorizado, las que deberán ajustarse de conformidad con el estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural. El Decreto Supremo N°1391, Reglamento General a la Ley N°164, Sector de Telecomunicaciones, en el Art. 176 establece:

Artículo 176.- (Protección de los Datos Personales).

I. El personal de operadores y proveedores de servicios de telecomunicaciones y tecnologías de información y comunicación, está obligado a guardar secreto de la existencia o contenido de las comunicaciones y a la protección de los datos personales y la intimidad de los usuarios.

II. Los operadores y proveedores de servicios están obligados a adoptar las medidas más idóneas para garantizar, preservar y mantener la confidencialidad y protección de los datos personales de los usuarios del servicio, salvo en los siguientes casos:

a) De existir una orden judicial específica;

b) Con consentimiento previo, expreso y por escrito del usuario titular;

c) En casos que la información sea necesaria para la emisión de guías telefónicas, facturas, detalle de llamadas al titular acreditado, o para la atención de reclamaciones, provisión de servicios de información y asistencia establecidos por el presente Reglamento, o para el cumplimiento de las obligaciones relacionadas con la interconexión de redes y servicios de apoyo.

III. El operador o proveedor de servicios deberá coadyuvar en la identificación de los presuntos responsables de vulneraciones a la inviolabilidad, secreto de las comunicaciones, protección de los datos personales y la intimidad de los usuarios, que su personal pudiera cometer en las instalaciones del operador o proveedor.

IV. La ATT aprobará los procedimientos y medidas utilizadas por los operadores y proveedores para salvaguardar la inviolabilidad y secreto de las comunicaciones y a la protección de los datos personales y la intimidad de los usuarios.

> V. Queda prohibido que los operadores y proveedores de servicios permitan el acceso a registros o bases de datos de sus usuarios, ya sea de manera individual o a través de listas de usuarias, usuarios o números, con fines comerciales o de publicidad, salvo autorización previa, expresa y escrita de la usuaria o usuario que desee recibir dicha publicidad.
>
> Asimismo, de conformidad a lo establecido en el artículo 43 inciso i) del D.S 1793, la Entidad Certificadora mantendrá la confidencialidad de la información proporcionada por los titulares de certificados digitales limitando su empleo a las necesidades propias del servicio de certificación, salvo orden judicial o solicitud del titular del certificado digital, según sea el caso.
>
> Finalmente, el Art. 43 inciso b) del Decreto Supremo N°1793, Reglamento para el desarrollo de Tecnologías de la Información y Comunicación, de fecha 13 de noviembre de 2013, señala: "Desarrollar y actualizar los procedimientos de servicios de certificación digital, en función a las técnicas y métodos de protección de la información y lineamientos establecidos por la ATT".

Fuente: Elaboración propia

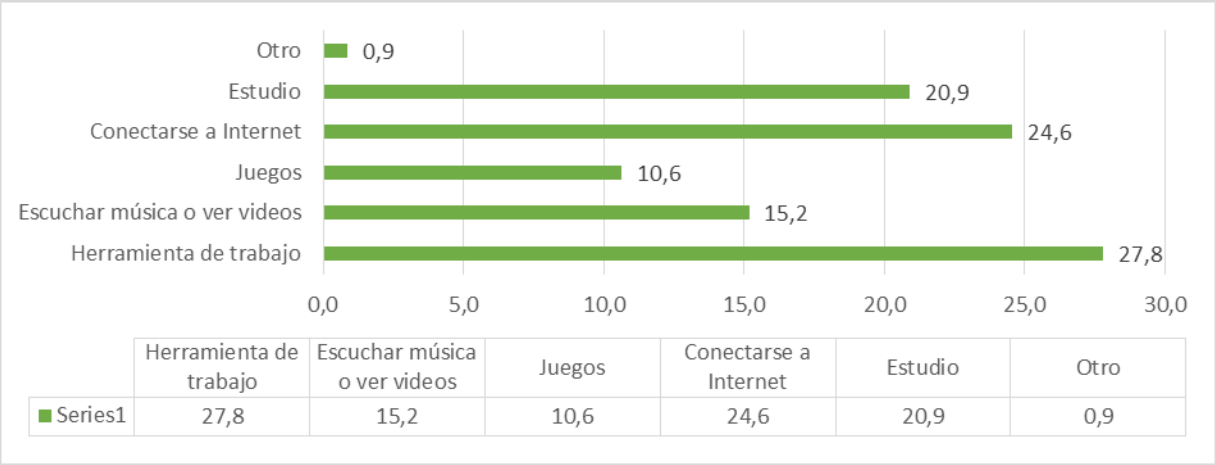
De las evidencias anteriores, es claro el compromiso de la ADSIB en relación a la protección de los datos personales en proporción a los servicios que brinda y en sus operaciones.

4.3 Acceso y uso de la información Sociedad de la información en las Tecnologías de la Información y comunicación.

Tras comprender la participación de la sociedad de la información como un conjunto de personas que viven bajo normas comunes, cuyas acciones de supervivencia y desarrollo están basados en un intenso uso, distribución, almacenamiento y creación de recursos de la información y conocimiento mediante las nuevas tecnologías de información y comunicación. Pues esta es, una sociedad que crece y se desarrolla alrededor de la información; la sociedad de la información es necesaria y representa un nuevo sistema para el desarrollo social, cultural, tecnológico, y económico.

Uno de las características más esenciales de esta sociedad es el uso de las nuevas tecnologías de la información, como ser ordenadores o computadoras y su uso o funciones que esta realiza con la misma. Tal es el caso donde podemos apreciar en el siguiente gráfico.

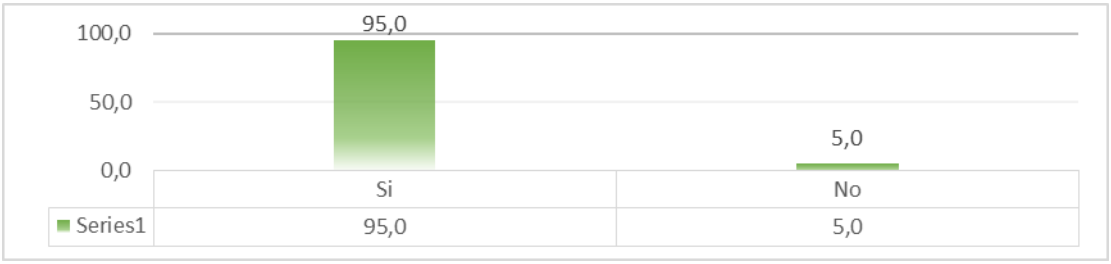
Gráfico 3 Uso del ordenador o computadora



Fuente: Elaboración propia en base a las encuestas Tic.

En la sociedad de la información en Bolivia en el uso del ordenador o computadora, es utilizada un 27,8% como herramienta de trabajo, 15,2% para escuchar música o ver videos, 10,6% juegos, 24,6 % conexión a internet, 20,9 % estudio y otro con 0,9%.

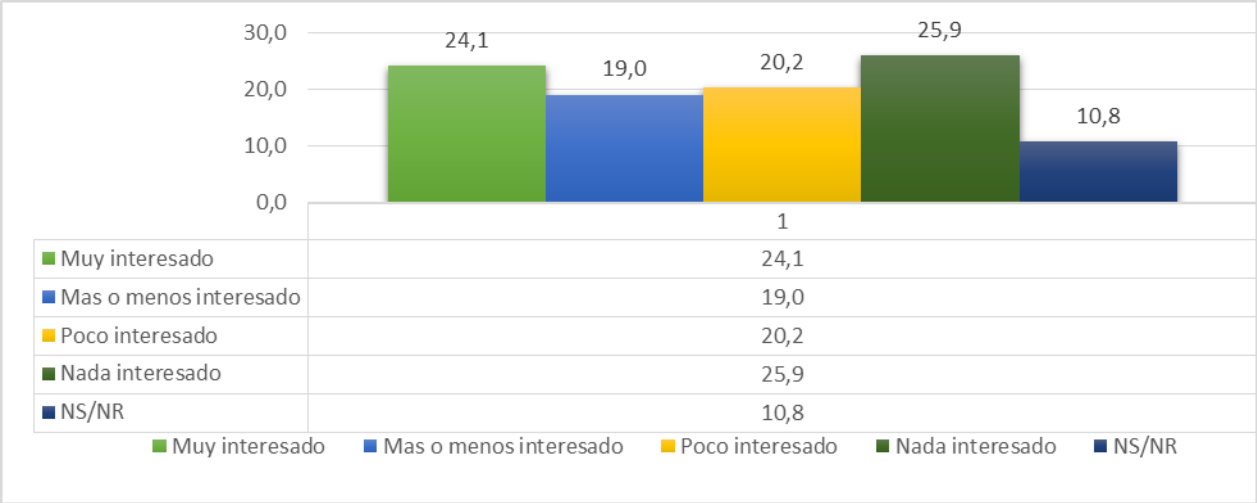
Gráfico 4 Personas que cuentan con internet en su celular



Fuente: 4 Elaboración propia en base a las encuestas Tic.

De un total de n encuestados un 95 % de personas que cuentan con internet en su celular, y un 5% que no cuenta con la misma.

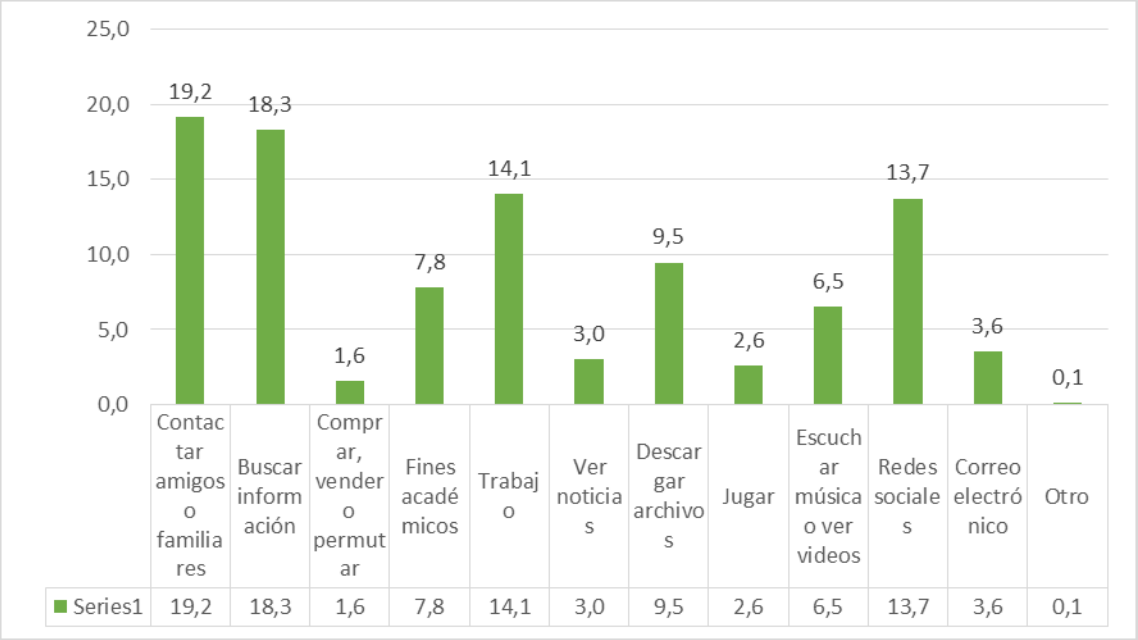
Gráfico 5 Intereses hacia el acceso a internet



Fuente: Elaboración propia en base a las encuestas Tic.

Sobre el interés hacia el acceso a internet, se puede observar que un 24,1% se encuentra muy interesado, un 19% que más o menos está interesado, un 20,2% poco interesado, el 25,9% nada interesado y finalmente con un 10,8% de personas que no saben o no responden.

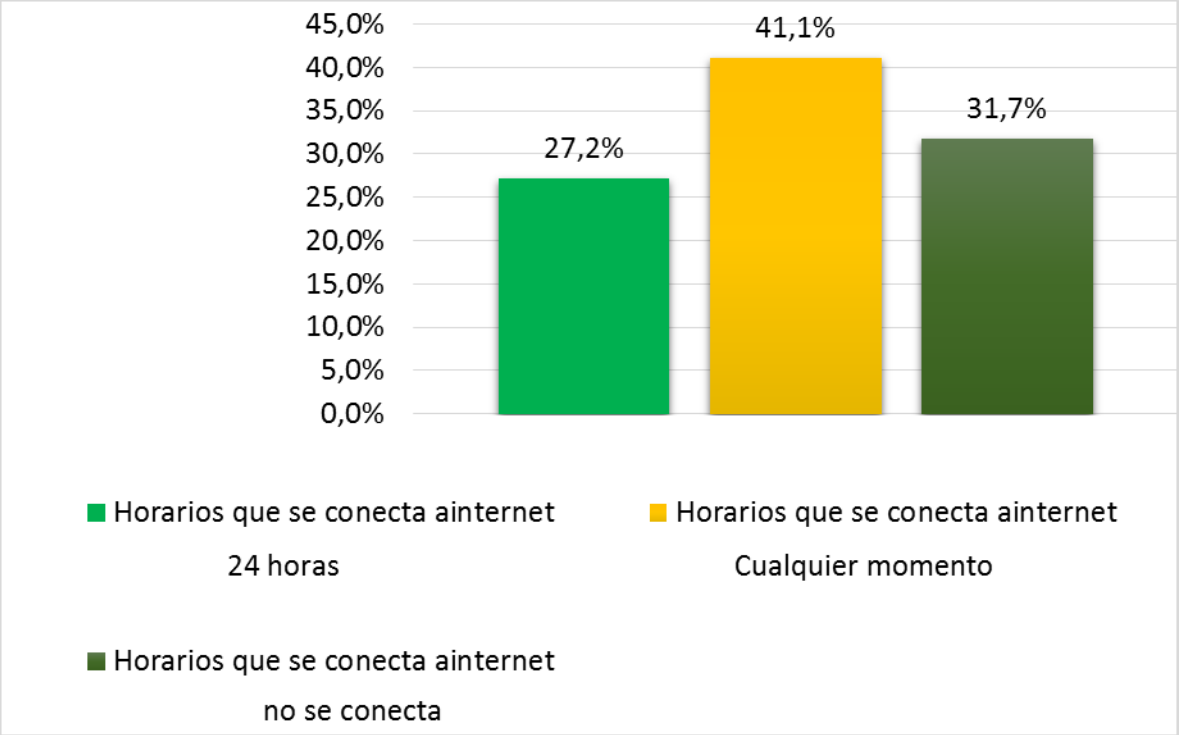
Gráfico 6 Uso del internet por parte de la Sociedad de la Información en Bolivia



Fuente: Elaboración propia en base a la encuesta Tic.

Podemos apreciar que el uso del internet por parte de la Sociedad de la Información en Bolivia, es para diversas actividades como: contactar con amigos o familiares con un 19,2%, búsqueda de información con un 18,3%, comprar, vender o permutar con un 1,6%, para fines académicos un 7,8%, trabajo con un 14,1%, para ver noticias 3%, descargar archivos un 9,5%, jugar 2,6%, escuchar música o ver videos un 6,5%, visitar redes sociales con un 13,7% y finalmente revisar el correo electrónico con un 3,6%.

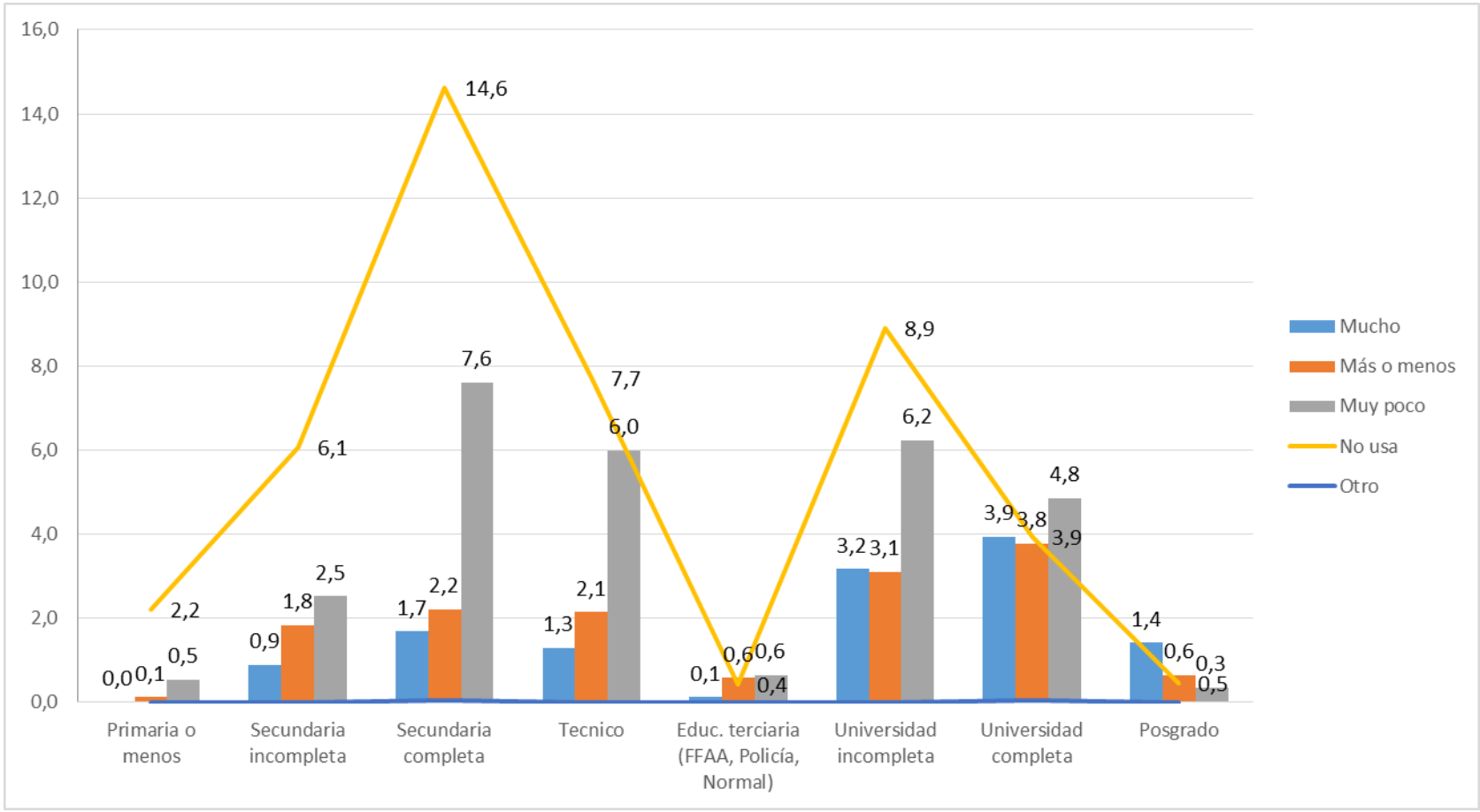
Gráfico 7 Horarios en los que la sociedad se conecta a internet



Fuente: Elaboración propia en base a la encuesta Tic.

Según el grafico el Horarios en los que la sociedad se conecta a internet es un 27,2% se conecta a internet las 24 horas, un 41,1% son los que se conectan en cualquier momento, y por último con un 31,7% no se conecta a internet.

Gráfico 8 Nivel de instrucción de los entrevistados en relación al uso del internet en su actividad económica

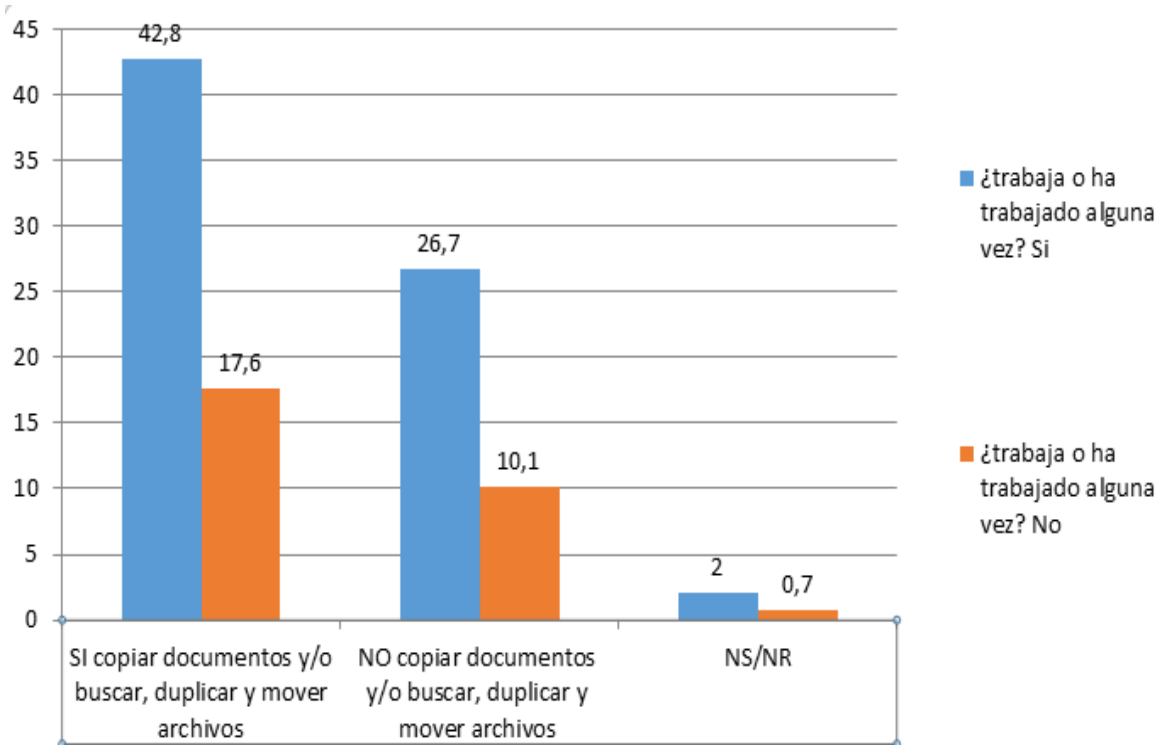


Fuente: Elaboración propia en base a las encuestas Tic.

Los porcentajes más altos en relación a las personas que usan mucho internet en su actividad económica son aquellas que tienen la universidad completa con un 3,9%, 3,2% las que tienen universidad incompleta, las que más o menos usan internet son 3,8% tienen la universidad completa, 3,1% tienen la universidad incompleta, las que usan muy poco internet son 7,6% que tienen la secundaria completa, 6,2% tienen la universidad incompleta, 6% tienen un nivel técnico, el 14,6% no usa los cuales cuentan con la secundaria completa, 8,9% la universidad incompleta, 7,7% cuentan con el nivel técnico, 6,1% tienen la secundaria incompleta.

4.4 Filtración de la información

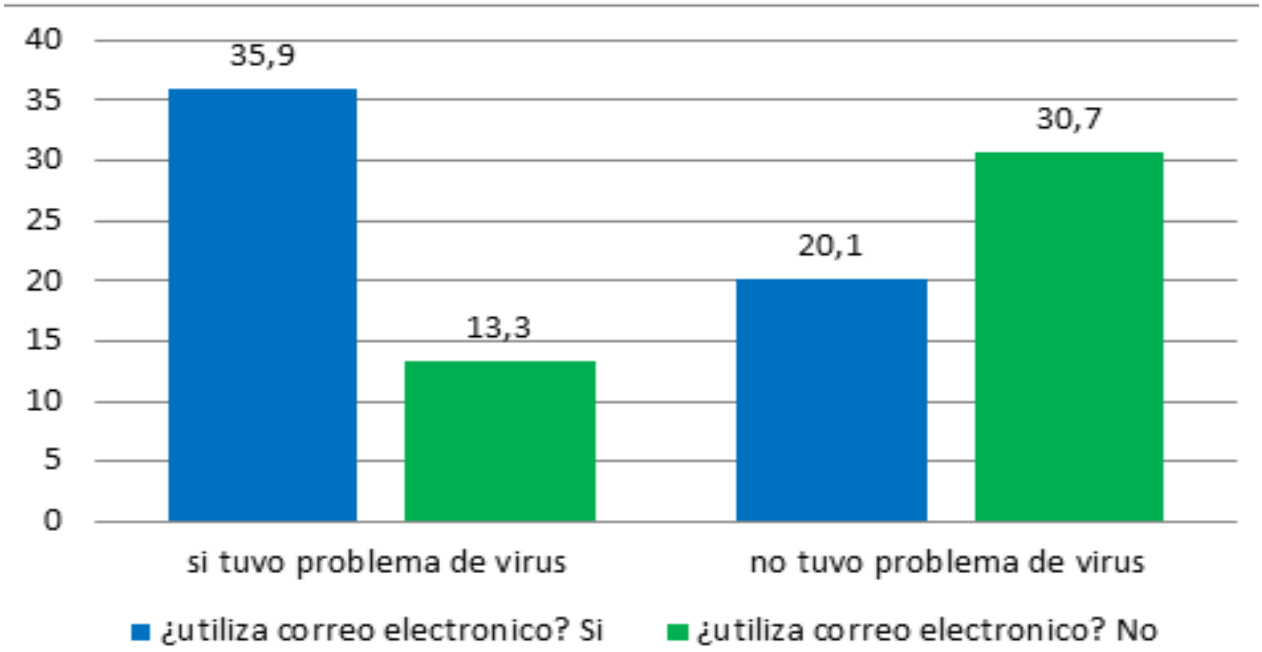
Gráfico 9 Personas que trabajan en relación a copiar documentos y/o buscar, duplicar y mover archivos



Fuente: Elaboración propia en base a las encuestas Tic.

Las personas que trabajan son 42,8%, las que no 17,6% las cuales copian documentos y/o buscan, duplican y mueven archivos, 26,7% de personas son las que trabajan, 10,1% las que no, estas no copian documentos y/o buscan, duplican y mueven archivos.

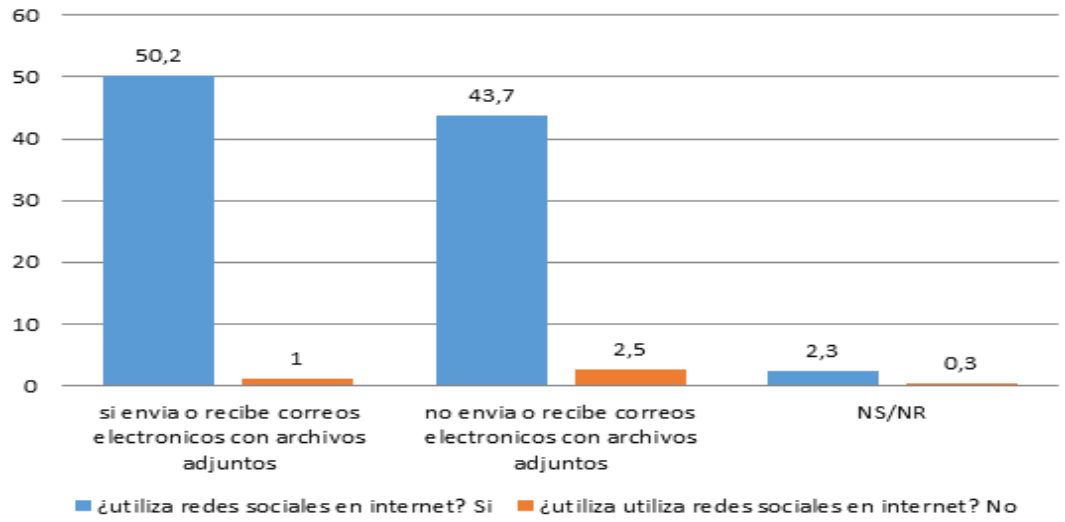
Gráfico 10 Uso del correo electrónico en relación a problemas de virus en la computadora



Fuente: Elaboración propia en base a las encuestas Tic.

Se observa que el 35,9% de personas si utiliza el correo electrónico, el 13,3% no lo usa, estos si presentaron problemas por virus en sus computadoras, así mismo 20,1% de personas que, si utilizan correo electrónico, el 30,7% que no lo usan, no tuvieron problemas por virus en sus computadoras.

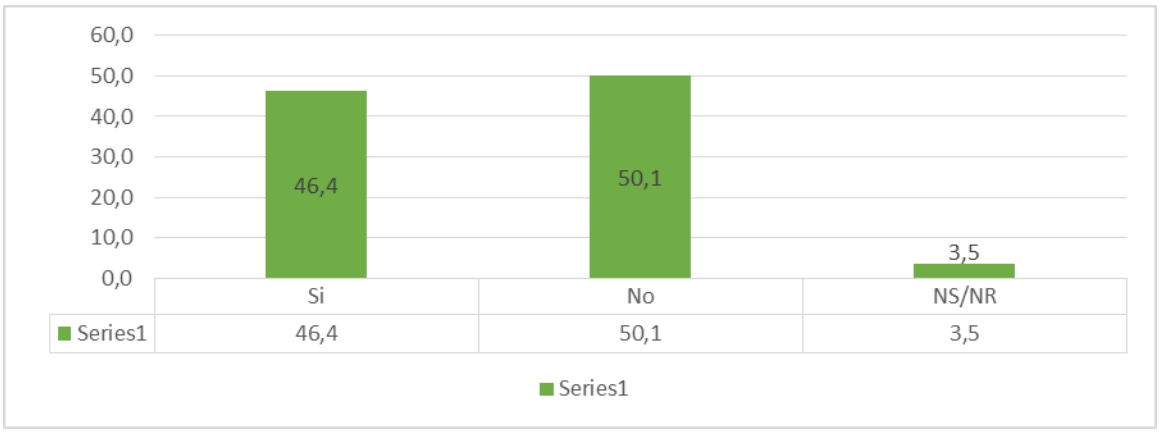
Gráfico 11 Uso de redes sociales en relación a enviar y recibir correos electrónicos con archivos adjuntos



Fuente: Elaboración propia en base a las encuestas Tic.

Las personas que si utilizan redes sociales en internet son 50,2% y las que no 1,0%, las cuales envían y reciben correos electrónicos con archivos adjuntos, 43,7% personas que utilizan redes sociales y 2,5% que no, no envían ni reciben correos electrónicos con archivos adjuntos.

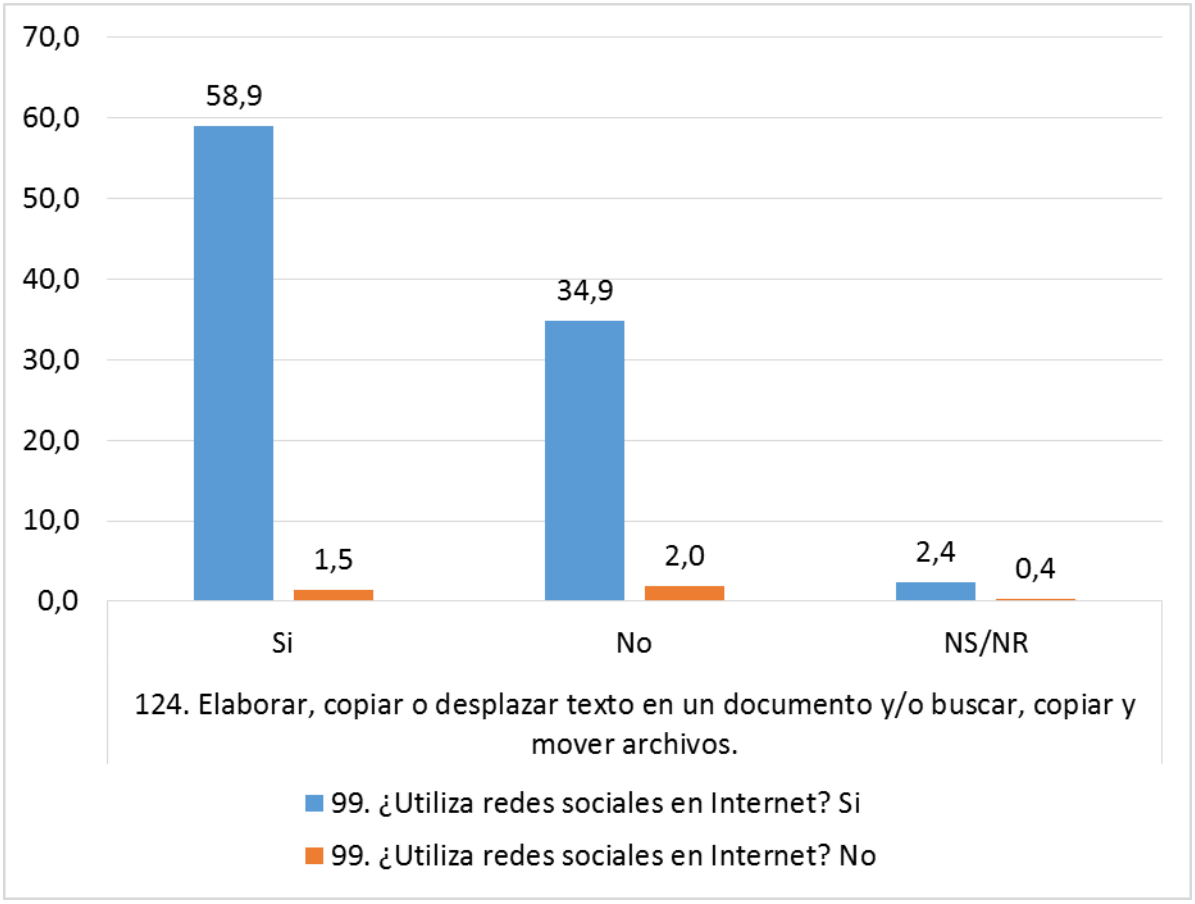
Gráfico 12 Personas que conectan nuevos dispositivos y/o transfieren archivos entre la computadora y otro dispositivo



Fuente: Elaboración propia en base a las encuestas Tic.

Las personas que si conectan nuevos dispositivos y/o transfieren archivos entre la computadora y otro dispositivo son un 46,4%, mientras tanto que un 50,1% dice no hacerlo, y finalmente un 3,5% no sabe o no responde.

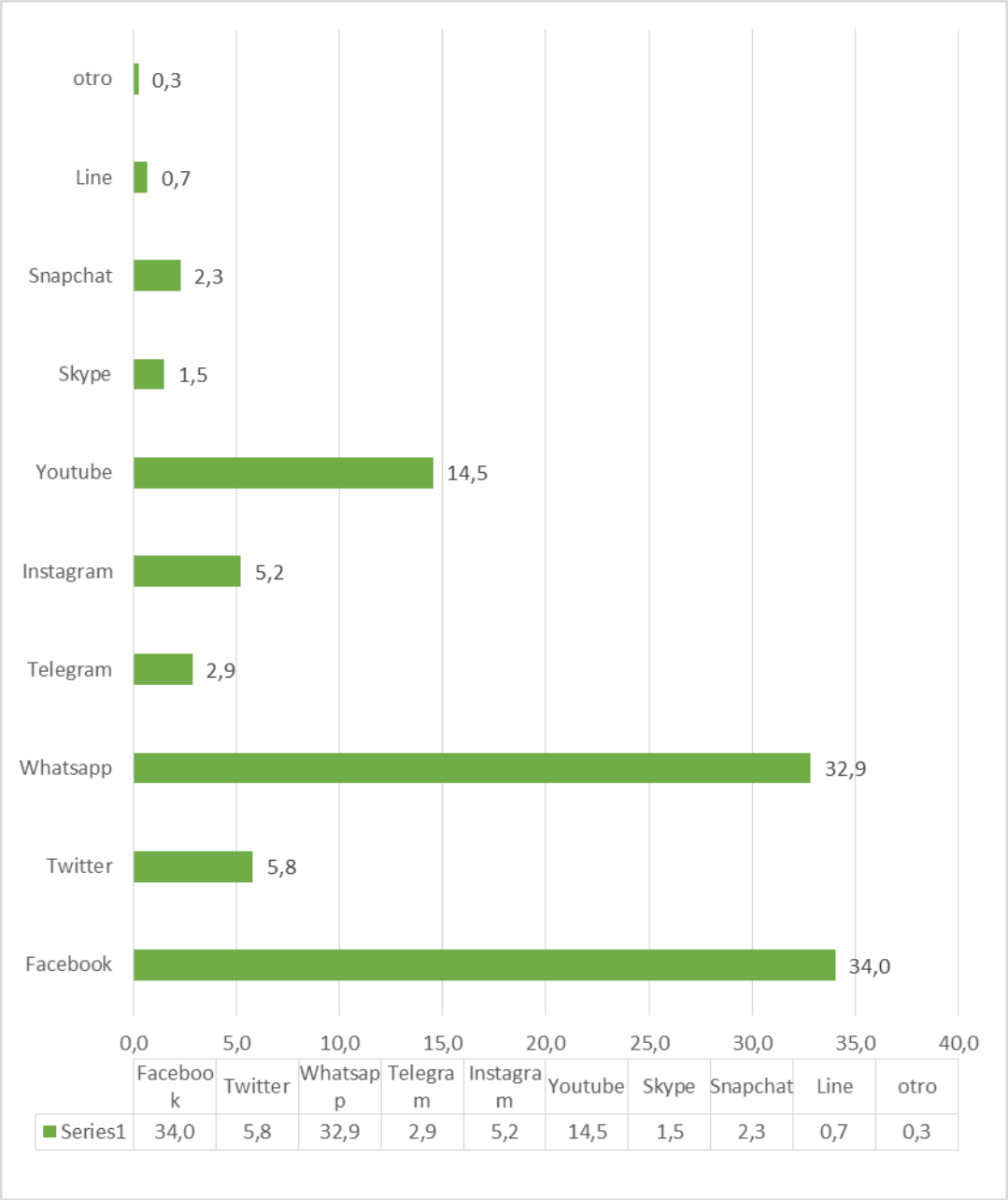
Gráfico 13 Personas que usan las redes sociales en relación a copiar o desplazar y/o buscar, copiar o mover archivos



Fuente: Elaboración propia en base a las encuestas Tic.

Las personas que usan las redes sociales en internet son 58,9% y 1,5% no, las cuales, realizan copias o desplazan y/o buscan, mueven archivos, 34,9% personas si utilizan las redes sociales y 2,0% no estas no realizan copias, desplazan y/o buscan, mueven archivos.

Gráfico 14 Presencia en uso de las redes sociales

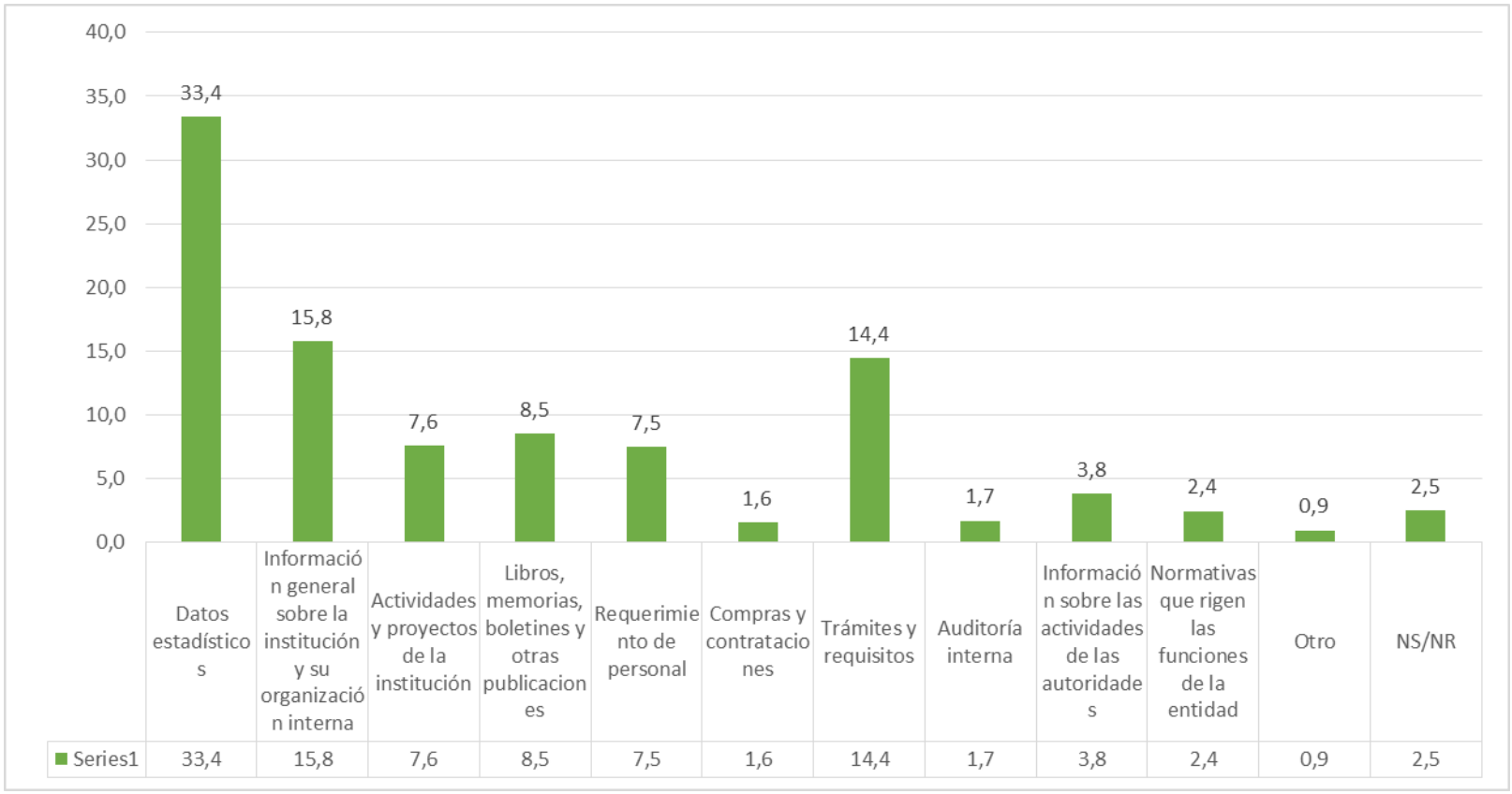


Fuente: Elaboración propia en base a las encuestas Tic.

En el gráfico se observa el uso de las redes sociales en Bolivia, Facebook con un 34%, Twitter con un 5,8%, WhatsApp con un 32,9%, Telegram 2,9%, Instagram con un 5,2%, YouTube con un 14,5%, Skype 1,5%, Snapchat con un 2,3%, Line 0,7% y otro 0,3%

4.5 Sensibilidad en los servicios de información

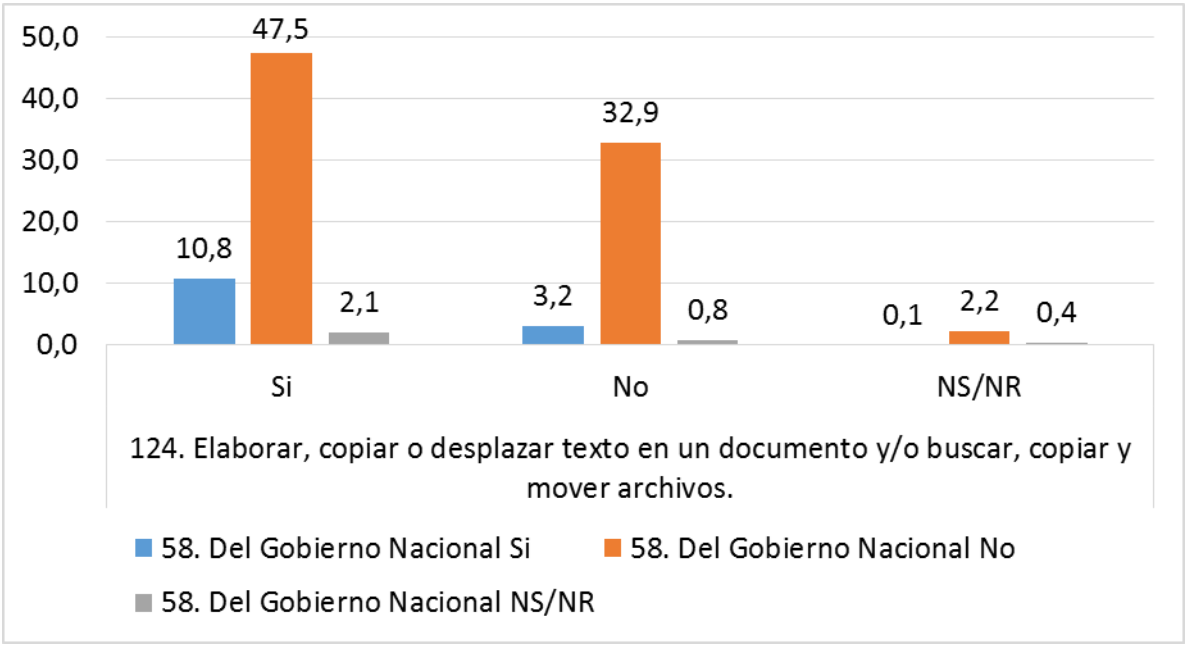
Gráfico 15 Requerimiento principal de las personas hacia del tipo de información que debería estar disponible en internet de las instituciones públicas



Fuente: Elaboración propia en base a las encuestas Tic.

Los requerimientos principales de las personas hacia el tipo de información que debería estar disponible en internet en las instituciones públicas revela en primer lugar con un 33,4% datos estadísticos, información general sobre la institución y su organización interna con un 15,8%, actividades y proyectos de la institución 7,6%, libros, memorias, boletines y otras publicaciones con un 8,5%, requerimiento de personal 7,5 %, compras y contrataciones 1,6%, un 14,4% información relacionada a Trámites y requisitos, 1,7% auditoria interna, información sobre las actividades de las autoridades 3,8%, normativas que rigen las funciones de la entidad 2,4%, otro 0,9% y no sabe no responde 2,5%.

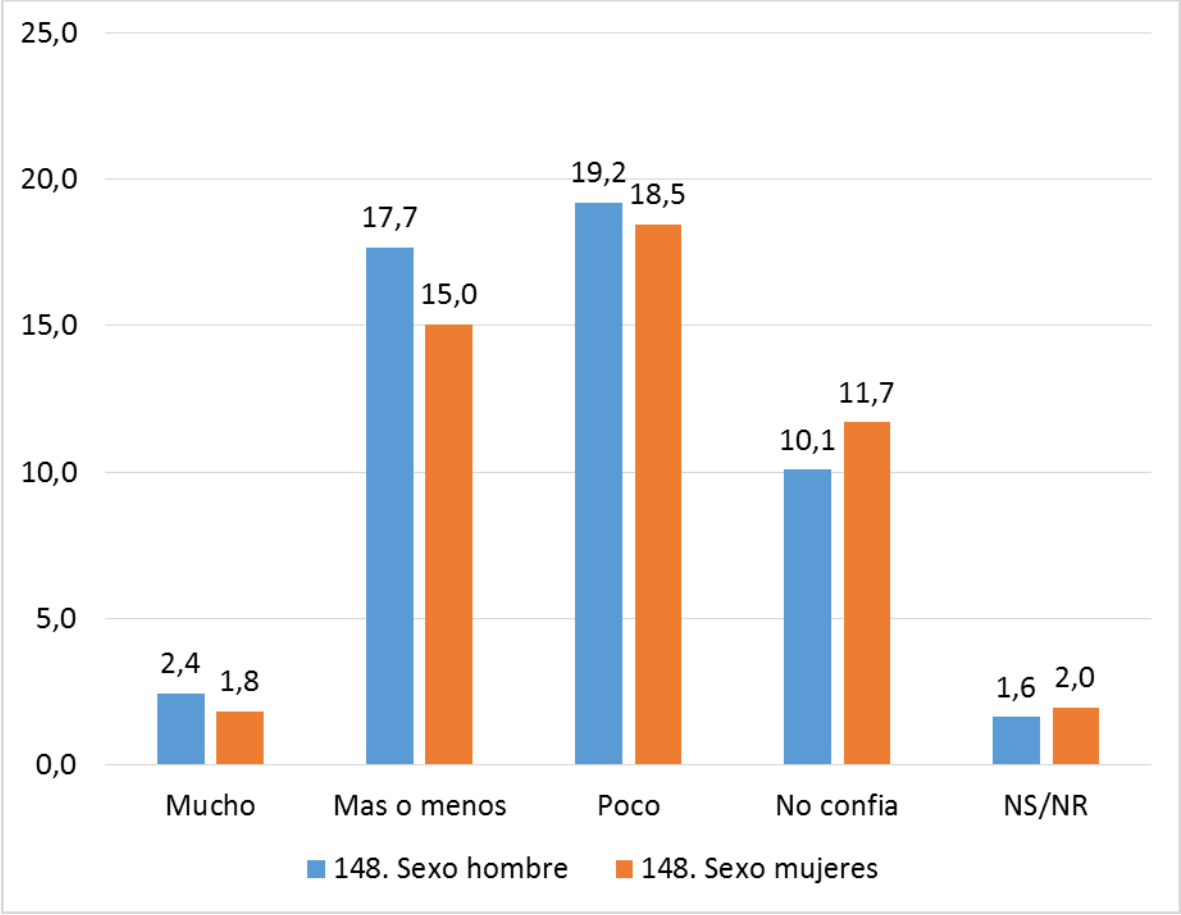
Gráfico 16 Personas que copian o buscan archivos de la página web del Gobierno Nacional



Fuente: Elaboración propia en base a las encuestas Tic.

Como se señala en el siguiente gráfico, las personas que si copian o buscan archivos y visitan la página web del gobierno nacional son 10,8% y un 47,5% si copian o buscan archivos, pero no visitan la página web y las personas que no copian o buscan archivos y visitan la página web del gobierno nacional son 3,2% y un 32,9% no copian o buscan archivos y no visitan la página web.

Gráfico 17 Confianza en la información de las redes sociales en relación al sexo

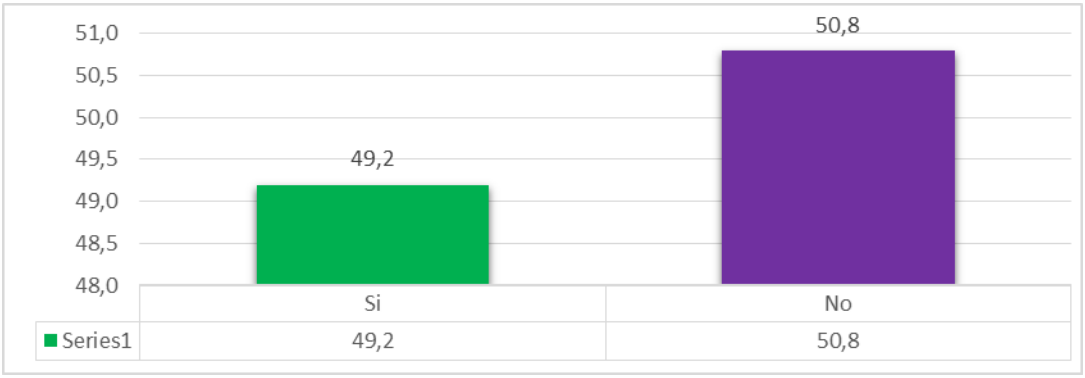


Fuente: Elaboración propia en base a las encuestas Tic.

En relación a la confianza de la información en las redes sociales de acuerdo al sexo por parte de la sociedad de la información en Bolivia, 2,4% varones y 1,8% mujeres confían mucho, Más o menos 17,7% varones y 15% mujeres, Poco 19,2% varones y 18,5% mujeres y los que no confían son 10% varones y 11,7% de mujeres.

4.6 Medidas de seguridad de la base de datos en sensibilidad a ataques cibernéticos

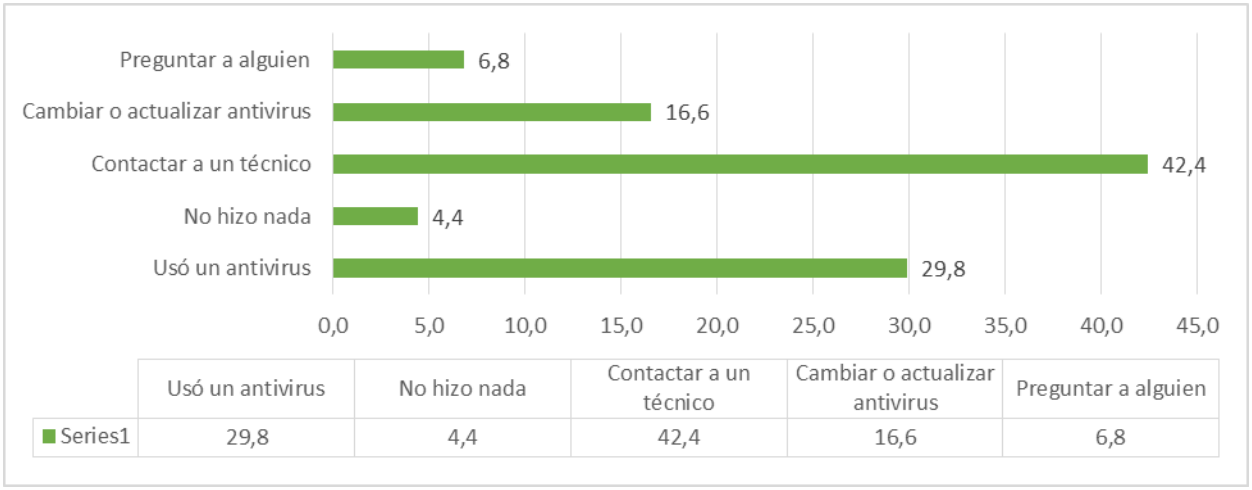
Gráfico 18 Personas que presentaron problemas de virus en su computadora



Fuente: Elaboración propia en base a las encuestas Tic.

Un 49,2% de las personas internautas menciona que sufrieron problemas de virus en su computadora, y un 50,8% menciona no haberlas sufrido.

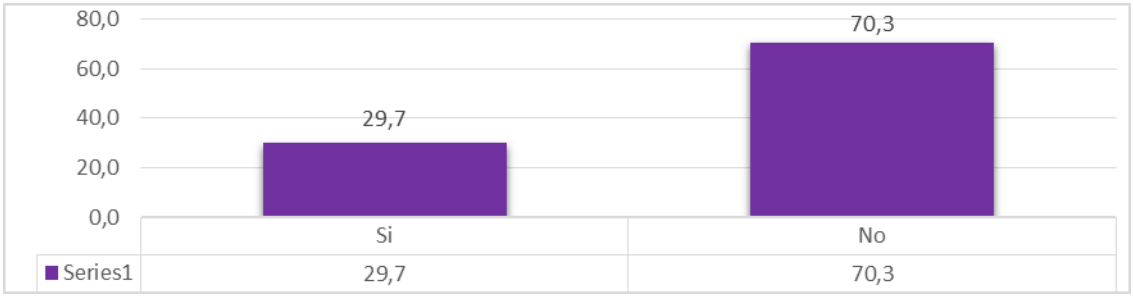
Gráfico 19 Acciones que tomaron las personas ante un problema de virus



Fuente: Elaboración propia en base a las encuestas Tic.

Las acciones presentadas por las personas que sufrieron algún tipo de virus en su computadora fueron, un 29,8% usó algún antivirus, un 4,4% no hizo nada, un 42,4% contactar a un técnico, cambiar o actualizar antivirus 16,6% y preguntar a alguien un 6,8%.

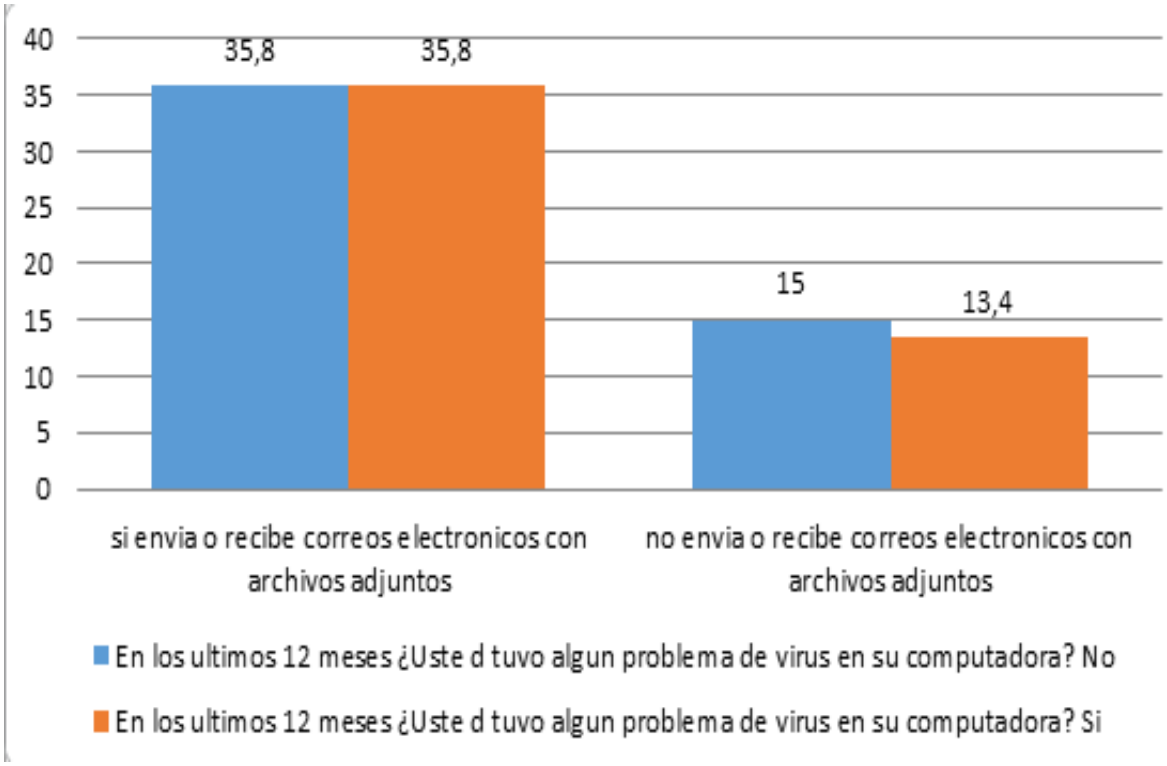
Gráfico 20 Conocimiento de que si existen otras personas que sufrieron un ataque de virus



Fuente: Elaboración propia en base a las encuestas Tic.

Sobre el conocimiento de que si existen otras personas que sufrieron un ataque de virus, un 29,7% reconocieron que si conocían alguna persona que haya sufrido ataque de virus, y que un 70,3% resalta que no conoce personas que hayan sido víctimas de estos ataques.

Gráfico 21 Personas que trabajan y que tuvieron problemas con virus en su computadora

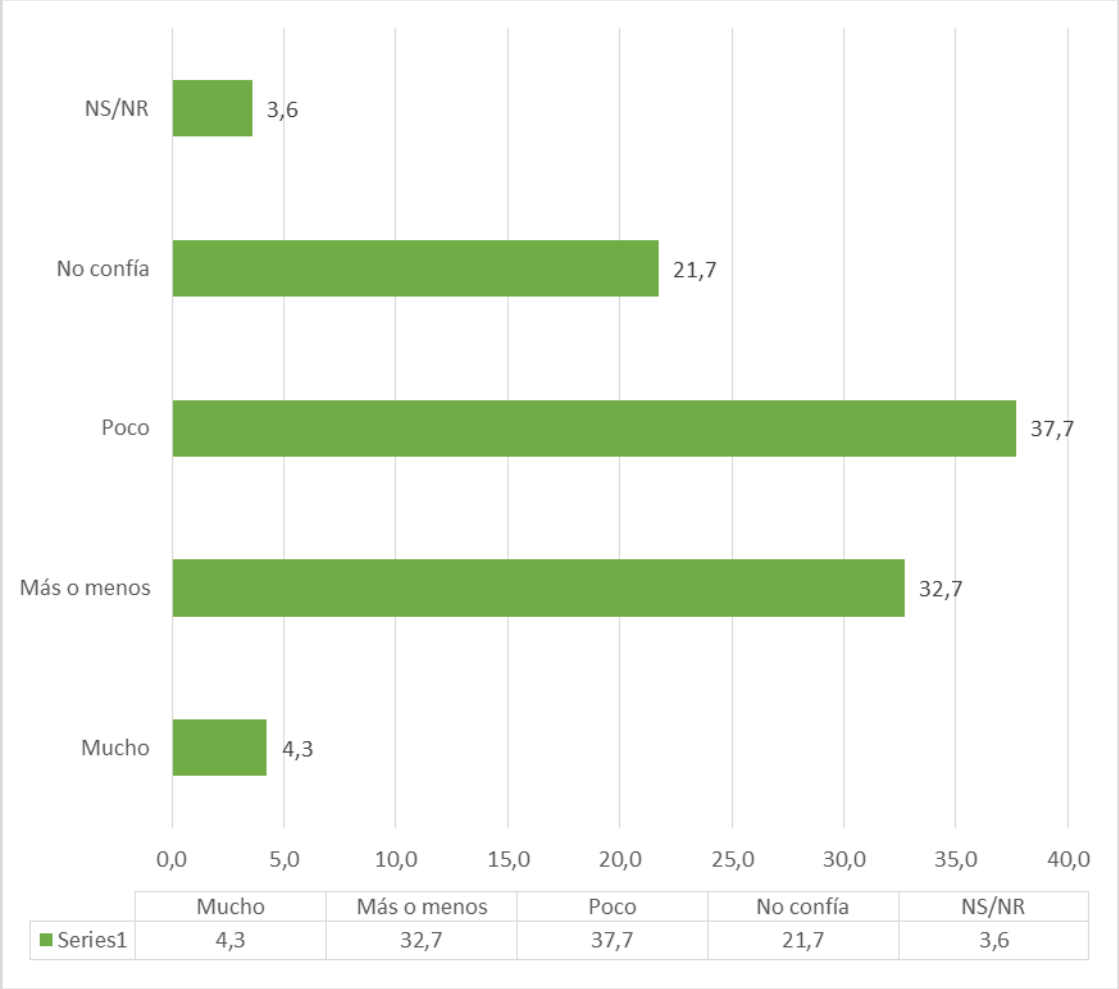


Fuente: Elaboración propia en base a las encuestas Tic.

Se presenta una igualdad en las personas que trabajan y que sufrieron algún problema de virus en su computadora, y las que no con un 35,8%, en el caso de las personas que no trabajan se presenta una mínima diferencia, entre las que sufrieron algún problema de virus en su computadora con un 13,4% y las que no con un 15%.

4.7 Daño a la imagen de la entidad

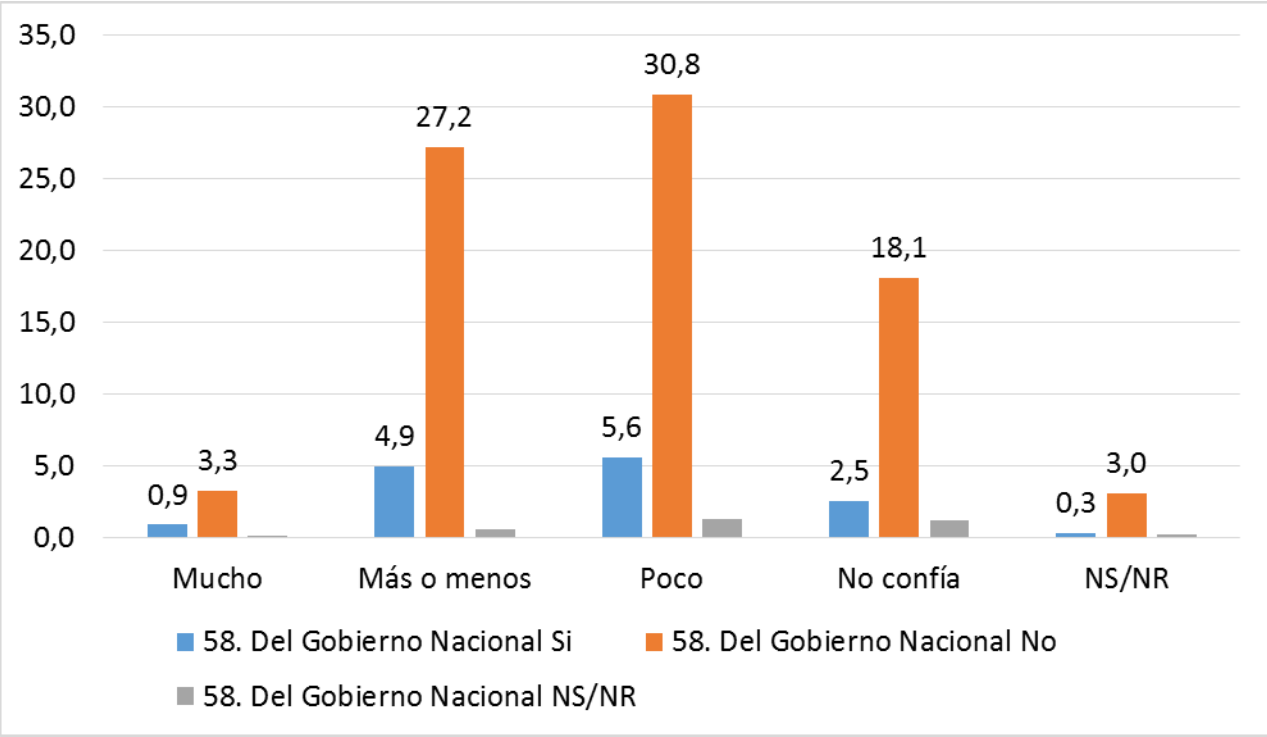
Gráfico 22 Confianza de las personas en la información de las redes sociales



Fuente: Elaboración propia en base a las encuestas Tic.

De las personas encuestadas el 4,3 % confía mucho en la información de las redes sociales, más o menos un 32,7%, poco un 37,7%, un 21,7% no confía y un 3,6% no sabe no responde.

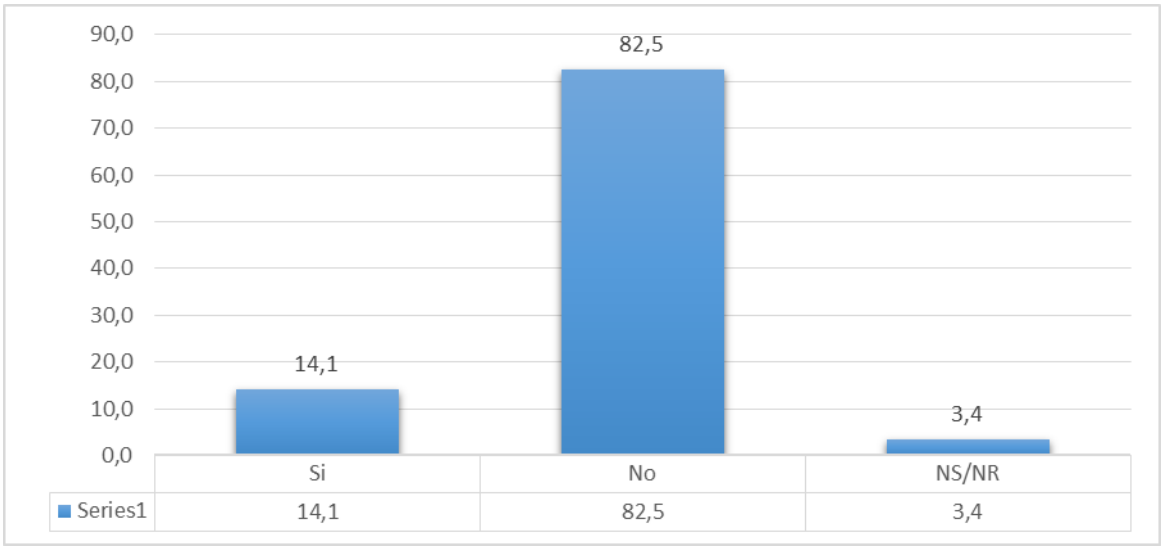
Gráfico 23 Personas que confían en la información de las redes sociales de la página del Gobierno Nacional



Fuente: Elaboración propia en base a las encuestas Tic.

Las personas que confían en la información de las redes sociales de la página del Gobierno Nacional tal como lo ilustra el siguiente gráfico demuestra que 0,9% personas si confía mucho, 3,3% no confía mucho, Más o menos 4,9% dijeron que si, 27,2% mencionaron que no, poco 5,6% dijeron que si, y 30,8% respondieron que no, 2,5% dijeron que no confían y un 18,1% mencionaron que no.

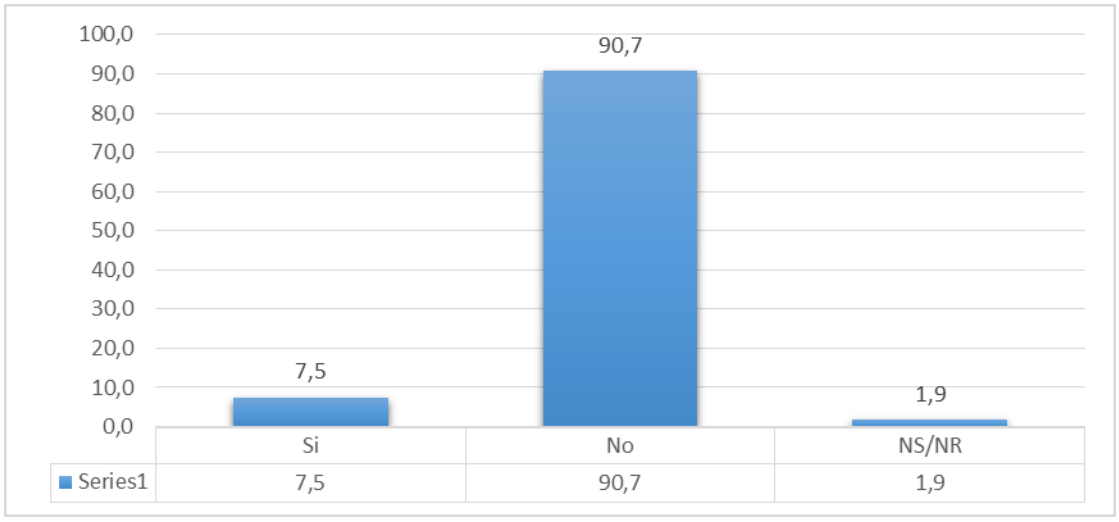
Gráfico 24 Población que visita la página web del Gobierno Nacional



Fuente: Elaboración propia en base a las encuestas Tic.

Podemos apreciar que la población que si visita la página web del gobierno nacional es de un 14,1%, 82,5% no visita y 3,4% no sabe no responde.

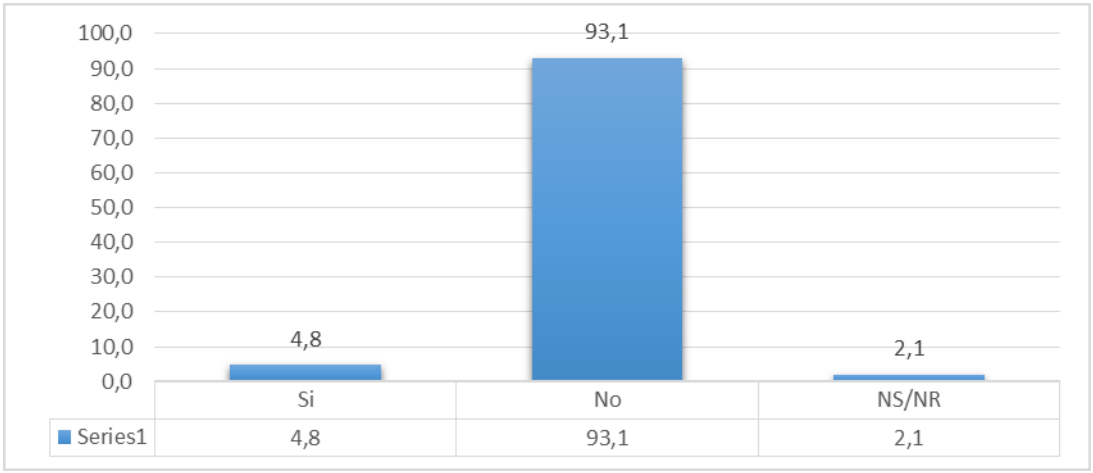
Gráfico 25 Población que visita páginas web de la Gobernación (Prefectura)



Fuente: Elaboración propia en base a las encuestas Tic.

Por otra parte, la población que si visita páginas web de la Gobernación (Prefectura) es un 7.5%, un 90.7% dice que no y un 3,4% no sabe no responde.

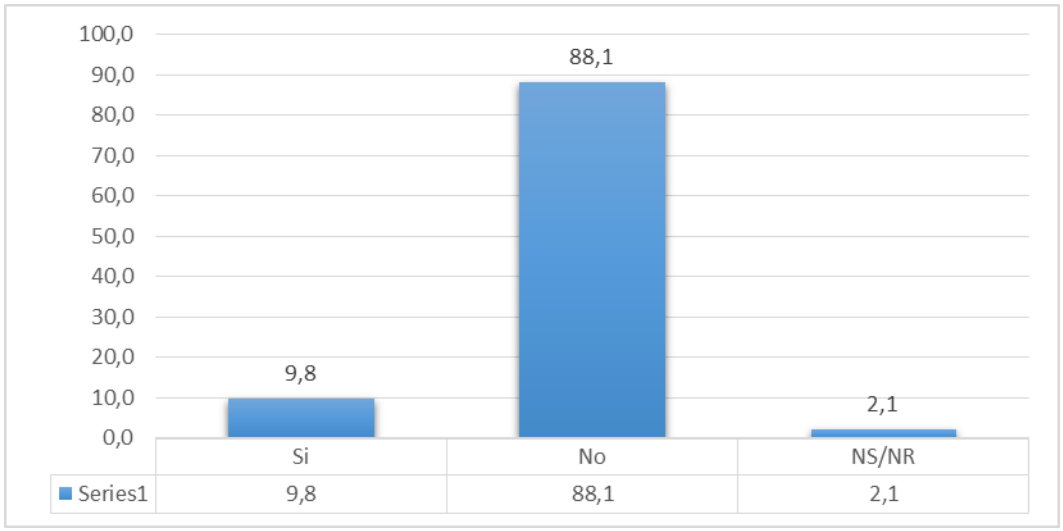
Gráfico 26 Población que visita la página web del Poder Judicial



Fuente: Elaboración propia en base a las encuestas Tic.

Observamos también, que la población que si visita la página web del Poder Judicial es un 4.8%, 93.1% dice que no y 2,1% no sabe no responde.

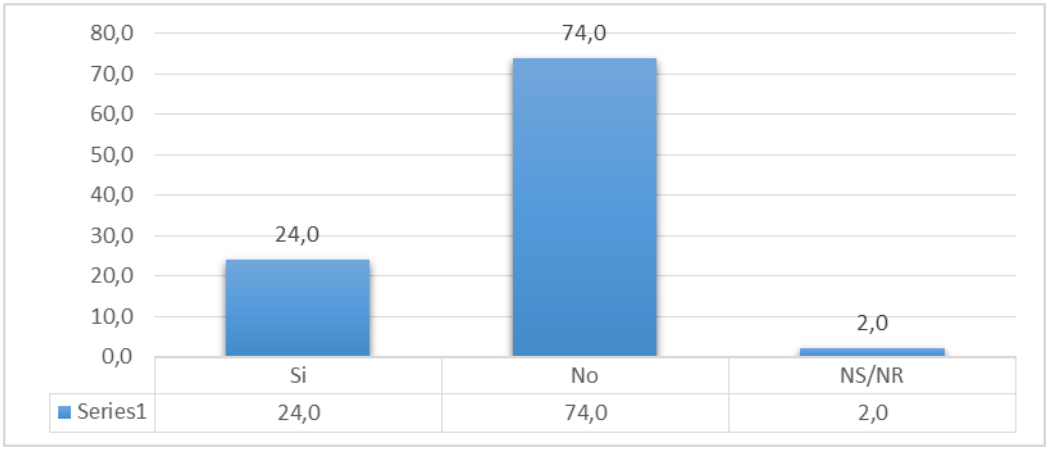
Gráfico 27 Porcentaje de la población que visita la página web del Tribunal Supremo Electoral



Fuente: Elaboración propia en base a las encuestas Tic.

Así mismo la población que si visita la página web del Tribunal Supremo Electoral es un 9,8%, no visitan 88,1% y 2,1% no sabe no responde.

Gráfico 28 Porcentaje de la población que visita la página web de las Universidades

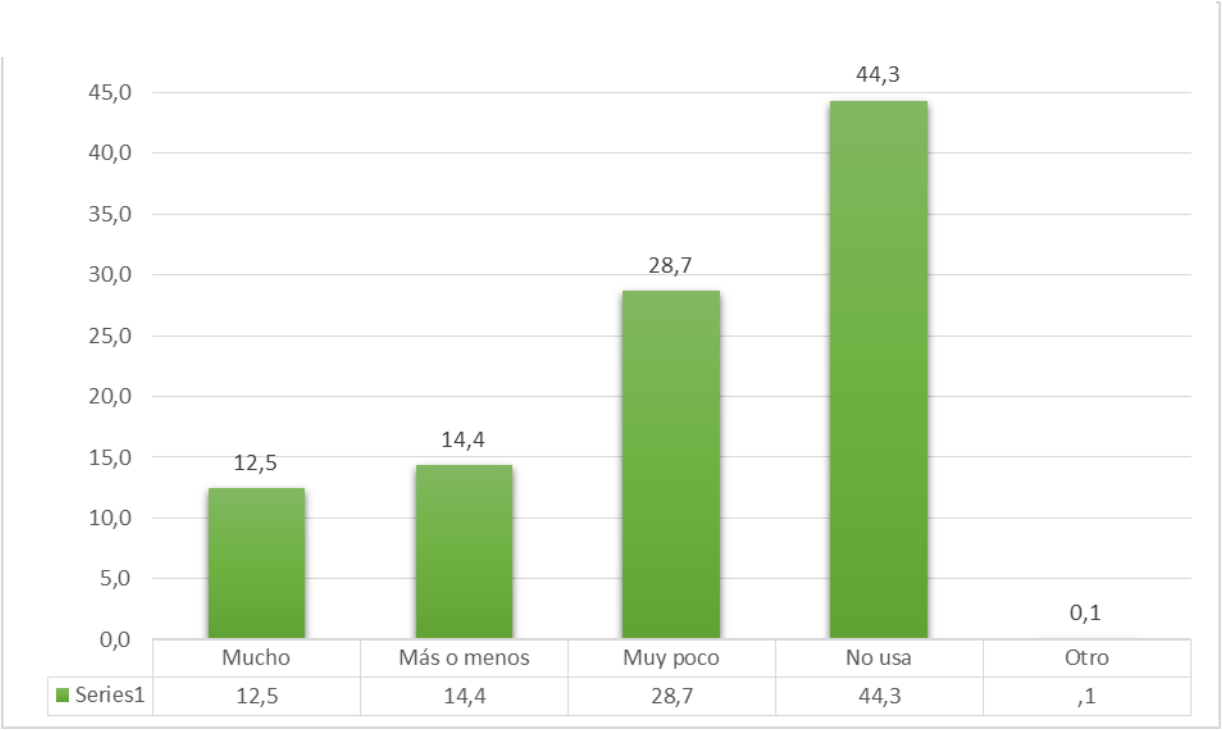


Fuente: Elaboración propia en base a las encuestas Tic.

Según el gráfico la población que si visita páginas web de las Universidades es un 24%, un 74% dice que no y un 2% no sabe no responde.

4.8 Daño económico

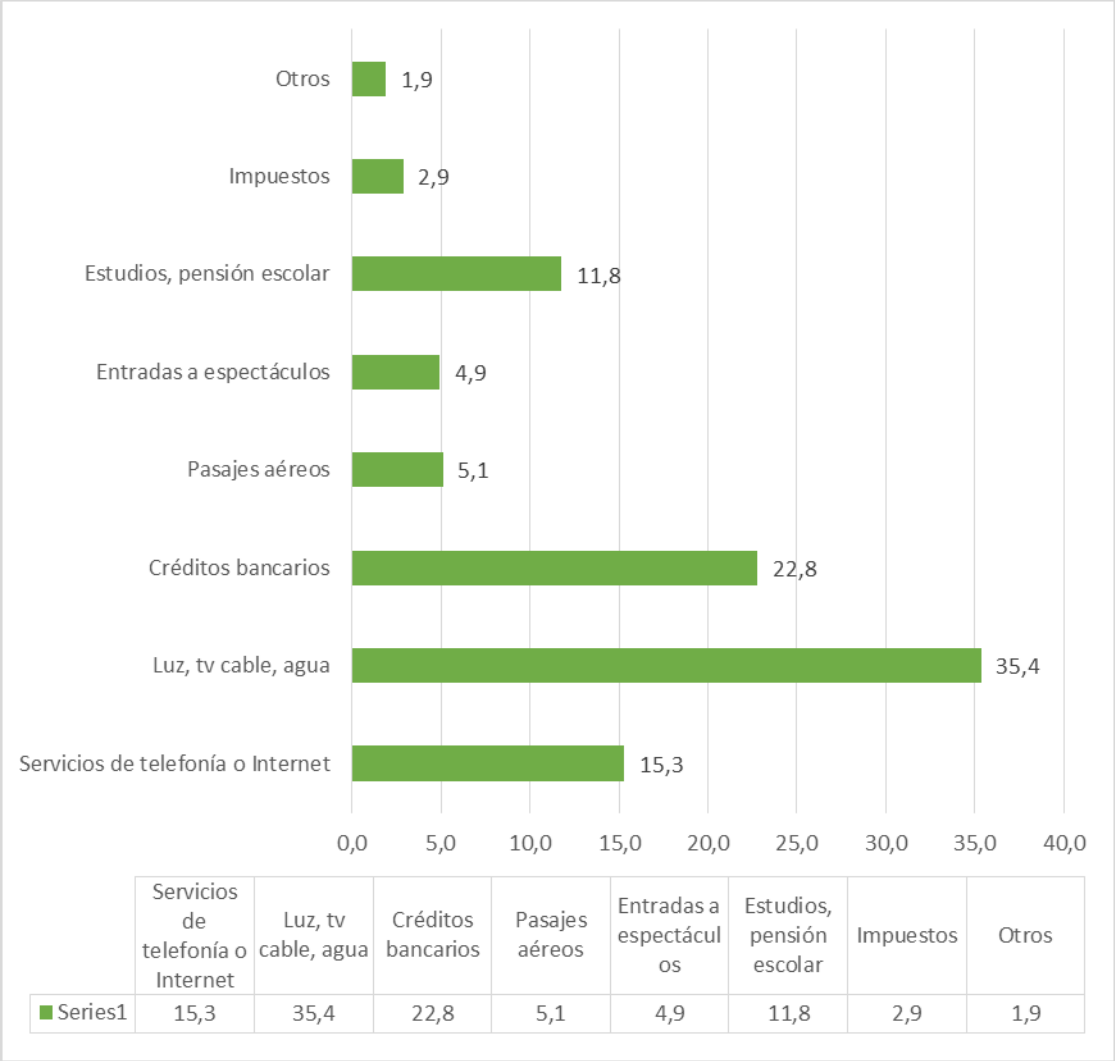
Gráfico 29 Uso del Internet para su actividad económica o laboral



Fuente: Elaboración propia en base a las encuestas Tic.

Con respecto al uso del internet para su actividad económica o laboral un 12,5% usa mucho, más o menos 14,4%, muy poco 28,7%, no usa un 44,3% y 0,1% otro.

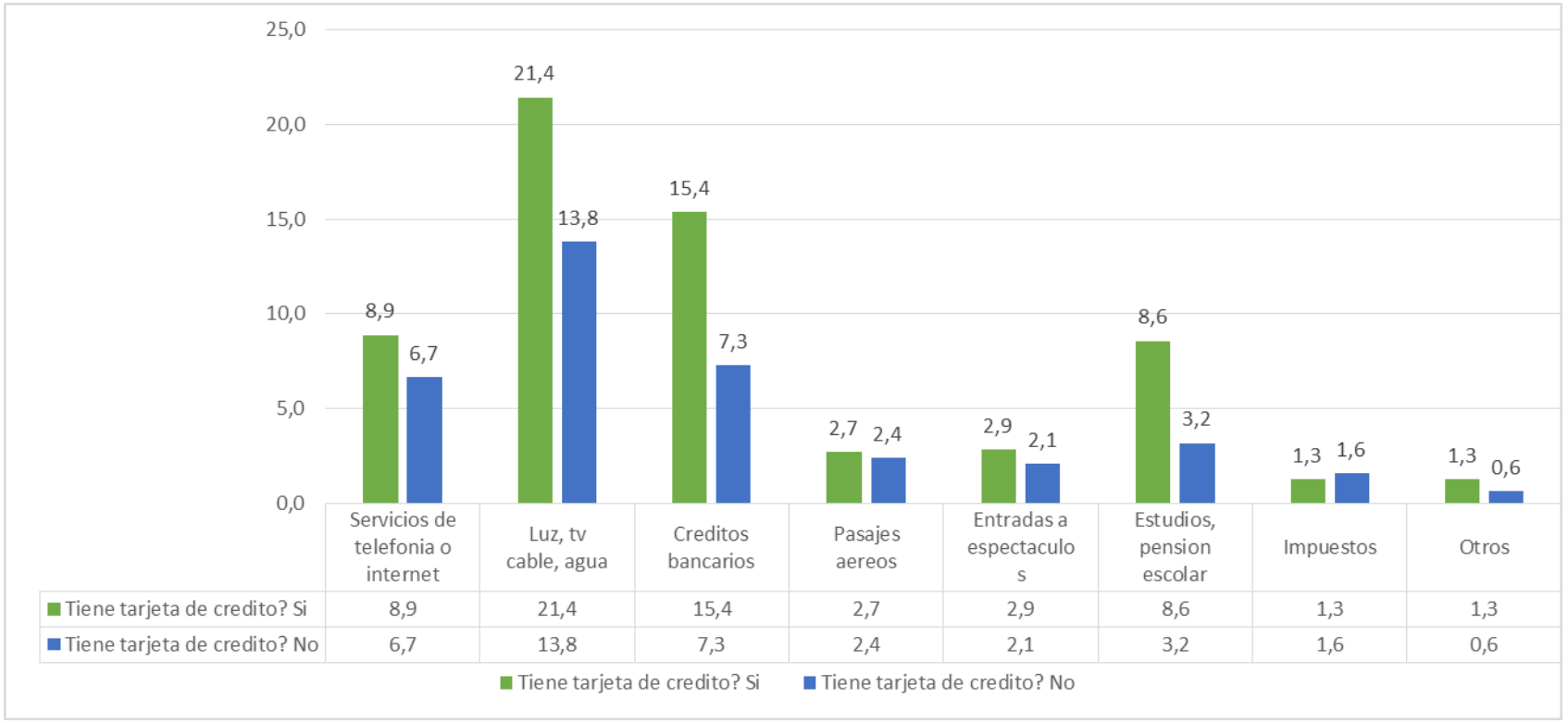
Gráfico 30 Población que realiza pagos a través de internet



Fuente: Elaboración propia en base a las encuestas Tic

La población que realiza pagos a través de internet se detalla en el siguiente gráfico, un 15,3% realiza pagos de servicios de telefonía o internet, 35,4% luz, tv cable o agua, 22,8% créditos bancarios, 5,1% pasajes aéreos, 4,9% pagos de sus estudios, pensión escolar, 11,8% impuestos, 2,9% y 1,9% otro.

Gráfico 31 Pagos por internet realizados con tarjeta de crédito

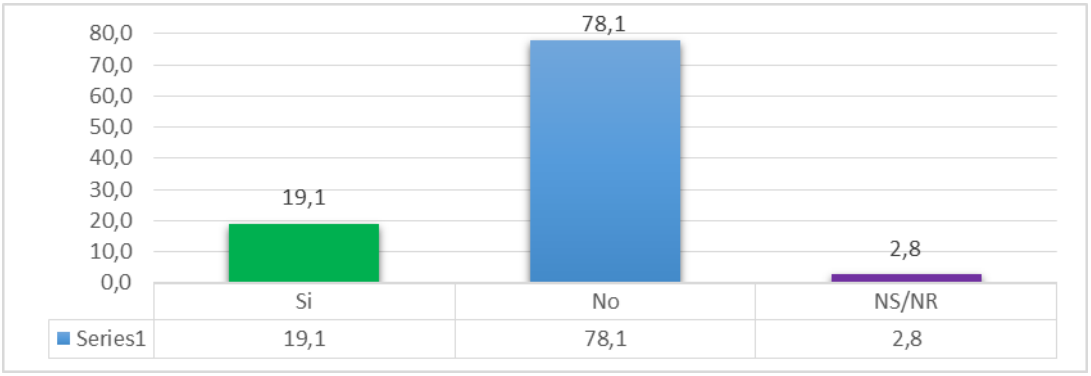


Fuente: Elaboración propia en base a las encuestas Tic

Según el gráfico las personas que realizan pagos de servicios de telefonía o internet con tarjeta de crédito a través de internet es un 8,9%, los que no realizan pagos con tarjeta de crédito son 6,7%, pagos de luz, tv cable, agua 21,4%, 13,8% no realiza pagos, créditos bancarios 15,4%, 7,3% no realiza pagos, pasajes aéreos 2,7%,2,4% no realiza pagos, entradas a espectáculos 2,9%, 2,1% no realiza pagos, estudios, pensión escolar 8,6%, 3,2% no realiza pagos, impuestos 1,3%, 1,6% no realiza pagos.

4.9 Diligencias de la sociedad de la información en trámites

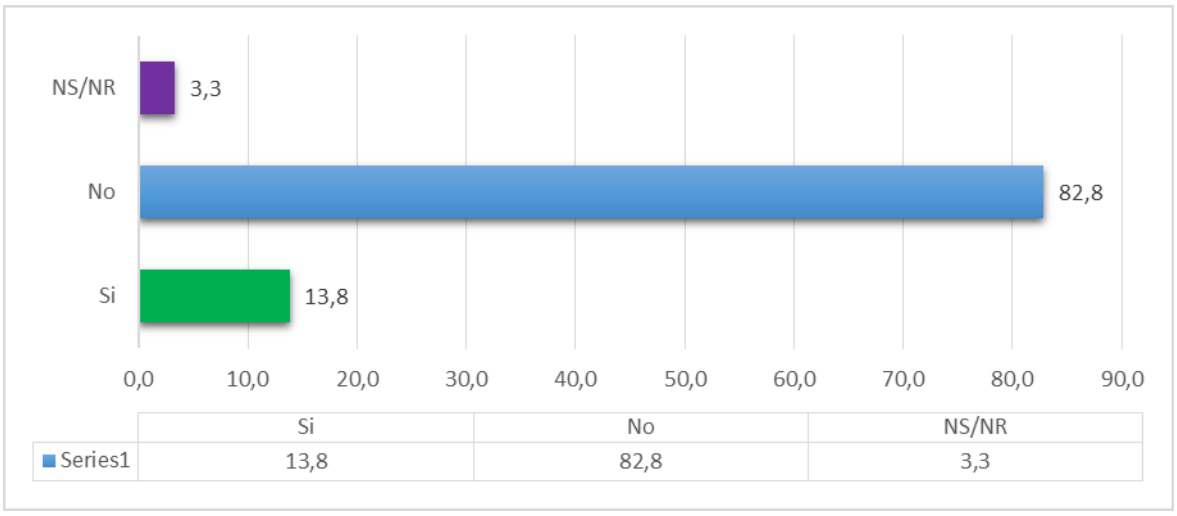
Gráfico 32 Personas que recaban información o requisitos sobre trámites en el sector público



Fuente: Elaboración propia en base a las encuestas Tic

El 19,1% si recaban información o requisitos sobre trámites en el sector público, y un 78,1% menciona que no y un 2,8% no sabe no responde.

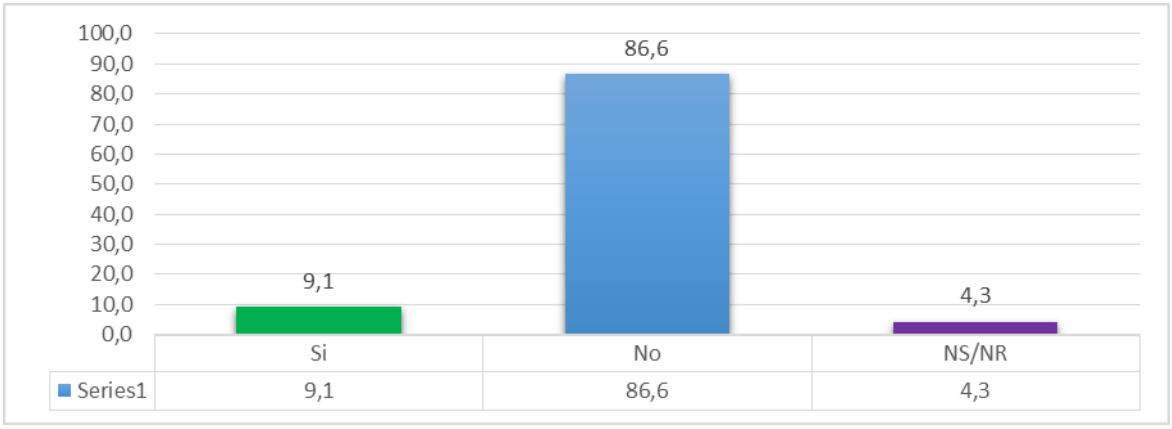
Gráfico 33 Completar y enviar formularios de trámites en el sector público



Fuente: Elaboración propia en base a las encuestas Tic

En cuanto, a completar y enviar formularios de trámites en el sector público, un 13,8% de las personas señala que si, un 82,8 % no lo realiza y 3,3 % no sabe no responde.

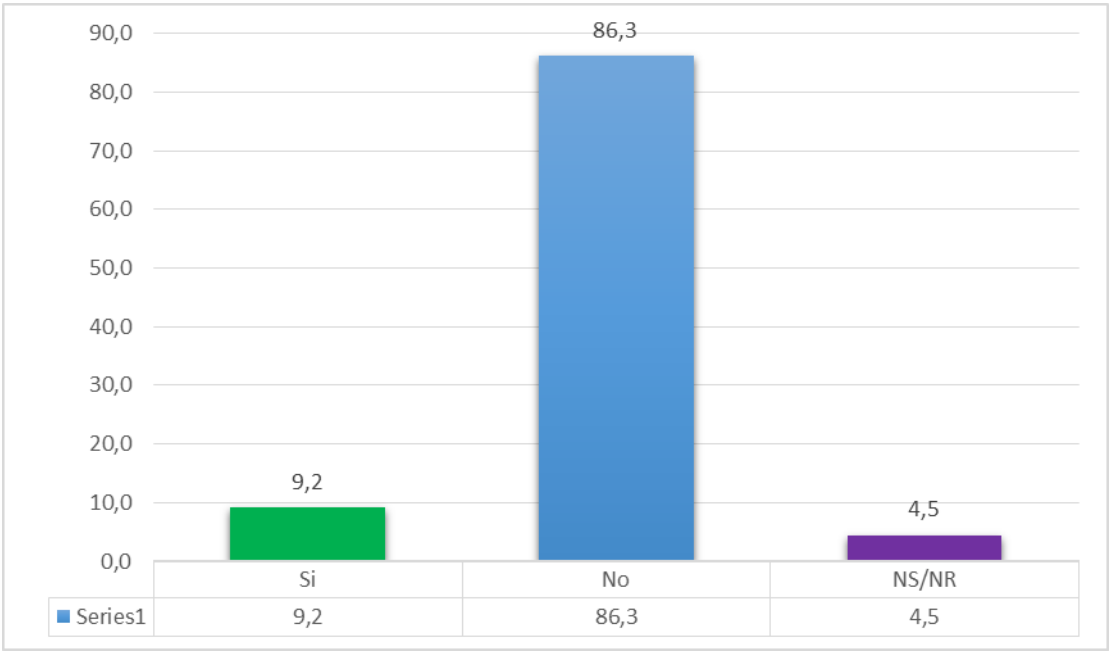
Gráfico 34 Realizar sugerencias, consultas, solicitudes o reclamos a organismos del estado



Fuente: Elaboración propia en base a las encuestas Tic

El 9,1% de personas realizan sugerencias, consultas, solicitudes o reclamos a organismos del estado, 86,6% no realiza y 4,3 no sabe no responde.

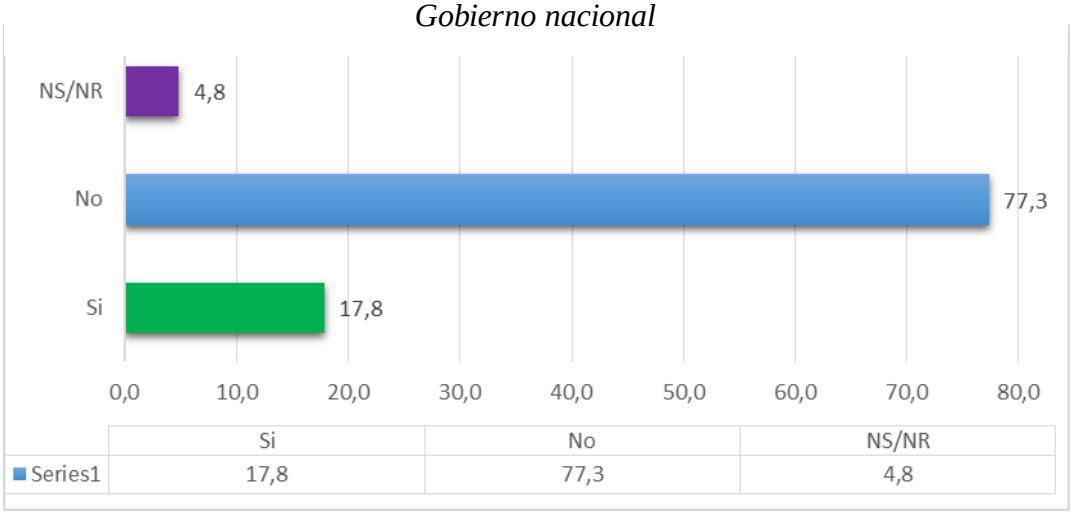
Gráfico 35 Realizar trámites completamente a través de internet



Fuente: Elaboración propia en base a las encuestas Tic

Como se observa en el gráfico, el 9,2% si realiza trámites a través de internet, un 86,3, no lo hace y 4,5 no sabe no responde.

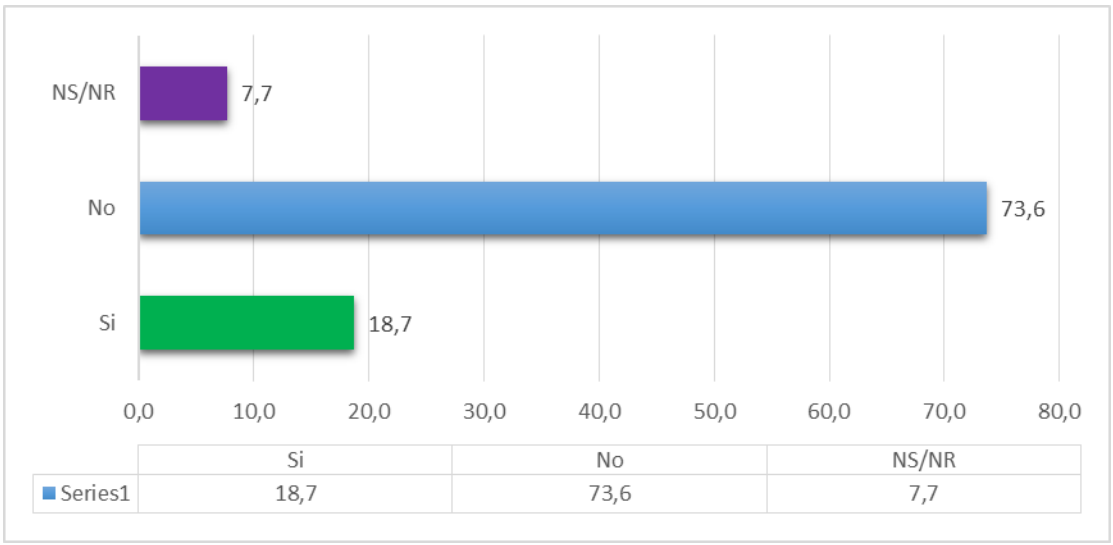
Gráfico 36 Porcentaje de la población que realiza trámites en las páginas web del Gobierno nacional



Fuente: Elaboración propia en base a las encuestas Tic

La población que si realiza trámites en las páginas web del Gobierno Nacional es un 17,8%, un 77,3% explica que no y un 4,5% no sabe no responde.

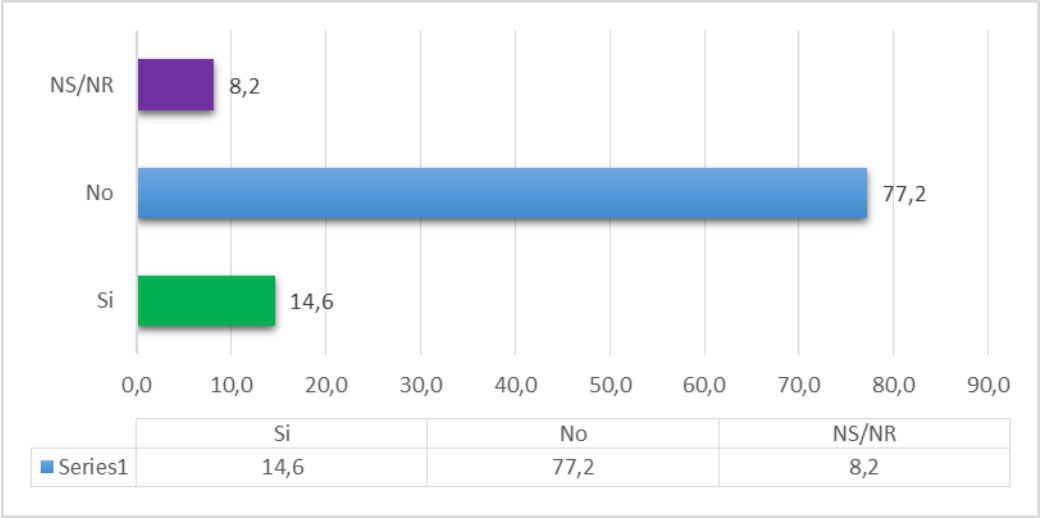
Gráfico 37 Porcentaje de la población que realiza trámites en las páginas web del Gobierno Municipal



Fuente: Elaboración propia en base a las encuestas Tic

De la misma forma la población que si realiza trámites en la página web del Gobierno Municipal es un 18,7%, un 73,6% dice no hacerlo y un 7,7% no sabe no responde.

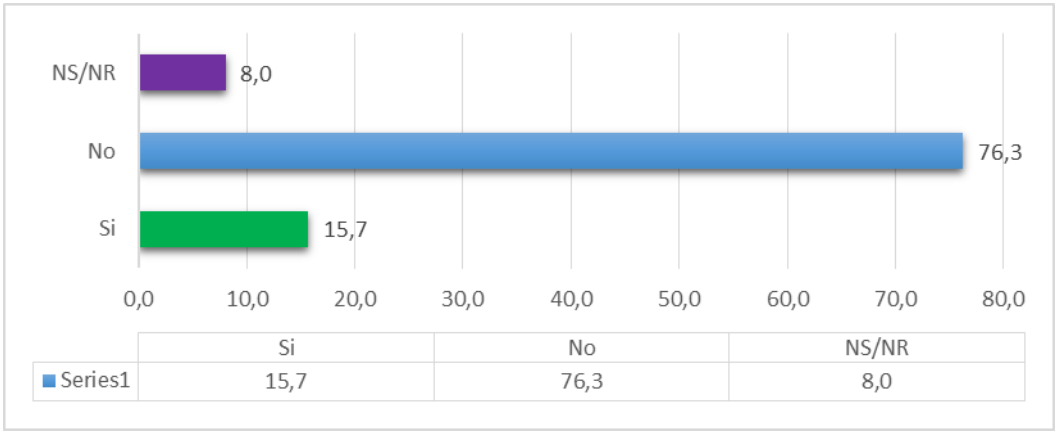
Gráfico 38 Porcentaje de la población que realiza trámites en las páginas web De la Gobernación (Prefectura)



Fuente: Elaboración propia en base a las encuestas Tic

La población que realiza trámites en las páginas de la gobernación (prefectura), evidencia que un 14,6% si realiza trámites y un 77,2% no lo hace y un 8,2% no sabe no responde.

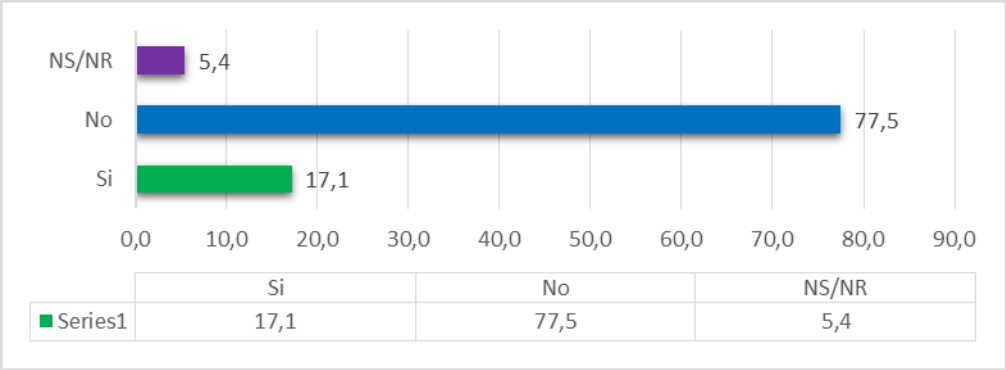
Gráfico 39 Porcentaje de la población que realiza trámites en las páginas web Del Poder Judicial



Fuente: Elaboración propia en base a las encuestas Tic.

El 15,7% de la población si realiza trámites en las páginas web del Poder Judicial, un 76,3% indica lo contrario y el 8% no sabe no responde.

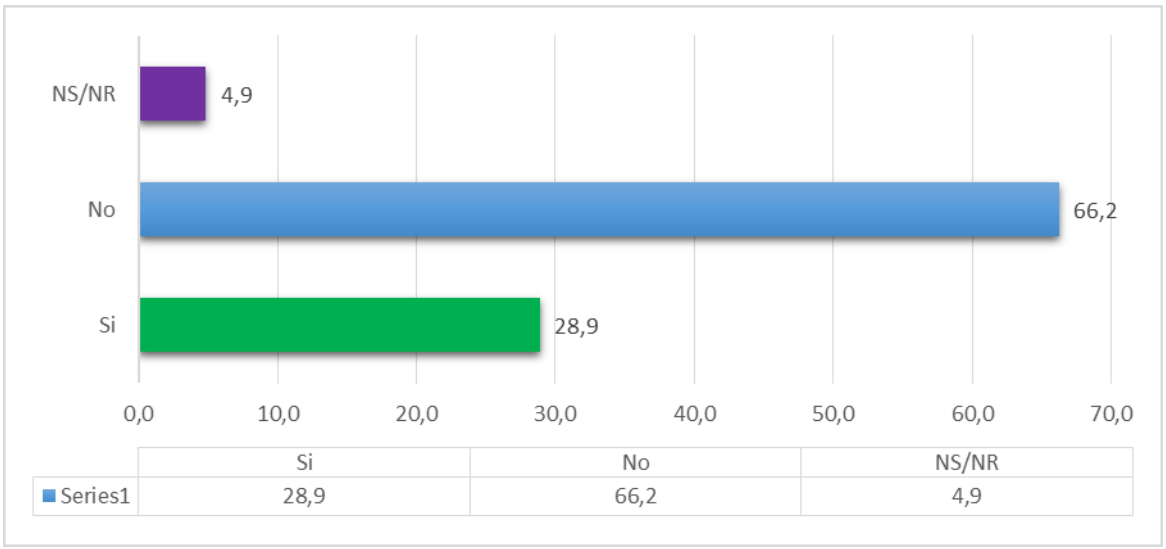
Gráfico 40 Porcentaje de la población que realiza trámites en las páginas web del Tribunal Supremo Electoral



Fuente: Elaboración propia en base a las encuestas Tic.

El porcentaje de la población que si realiza trámites en la página web del Tribunal Supremo Electoral es un 17,1%, un 77, 5% señala que no y 5,4% no sabe no responde.

Gráfico 41 Porcentaje de la población que realiza trámites en las páginas web De las Universidades



Fuente: Elaboración propia en base a las encuestas Tic.

La población que realiza tramites en las páginas web de las Universidades un 28,9% señala que si lo hace un 66,2% revela no hacerlo y un 4,9% no sabe no responde.

CAPÍTULO V - DISCUSIÓN

Esta investigación tuvo como propósito identificar la seguridad de la información para la protección de los datos personales en la firma digital implementados por Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB). Sobre todo, se pretendió examinar el comportamiento de la sociedad de la información en Bolivia, en factores asociados a la filtración de la información, servicios, ataques cibernéticos, daño a la imagen, actividad económica y desarrollo de trámites en la actualidad, donde la información es expuesta por medio de esta sociedad. A continuación, se discutirán los principales hallazgos de estudio.

De los resultados obtenidos en esta investigación, se puedo ratificar que la Agencia para el Desarrollo de la sociedad de la información en Bolivia (ADSIB), proporciona seguridad a la información y protección de los datos personales en la firma digital. Donde, se puede contemplar que la inadecuada seguridad de la información, repercute en la mala protección de los datos personales, también así para la implementación de una firma digital. Sin embargo, la sociedad de la información es un factor al cual debe orientarse la seguridad de la información

La seguridad de la información es la preservación de la confidencialidad, integridad y disponibilidad de la información, los cuales se establecen conforme al nivel requerido en cumplimiento de los objetivos de servicios o negocio de las entidades. Ahora bien, la ADSIB reafirma que contempla la seguridad de la información expresada en el cuadro N°14, que consulta la regularización de acceso a la información, tanto como personal trabajador y clientes usuarios, que en el cual detalla que “cuentan con medidas de protección para el acceso de la información tanto para el personal operador del servicio y usuarios finales, las cuales están en base a las POLÍTICAS DE CERTIFICACIÓN (CP) y DECLARACIÓN DE PRACTICAS DE CERTIFICACIÓN (CPS), Políticas de Seguridad y procedimientos internos”.

Mientras, en el cuadro N°16 se detalla el tipo de información administrada y más importante para la entidad, como ser su activo de información, que describe "Al hablar de Certificación Digital se entiende que todo el proceso de registro, hasta la emisión del certificado es crítico, es decir en todo ese periodo la información proporcionada por el usuario es protegida por las diferentes amenazas, vulnerabilidades e identificando un nivel de riesgo para cada una de ellas, toda esta información se encuentra en las políticas de certificación (CP), declaración de prácticas de certificación (CPS) y otros documentos relacionados a la gestión de la información que son internos." Esto es, garantizar la seguridad para las organizaciones que acreditan la identidad del titular de la firma digital, legitima la autoría de la firma digital que certifica, vincula un documento digital que certifica, vincula un documento digital o mensaje electrónico de datos, con la firma digital y la persona, así también, garantiza la integridad del documento digital o mensaje electrónico con firma digital.

Dentro de esta perspectiva, el servicio proporcionado por la ADSIB, es mediante la perspectiva de confidencialidad que contempla el evitar posibles fugas, divulgación no autorizada, mal uso o resguardo de la información. Por lo tanto, se establece que:

> *Los certificados digitales deben ser emitidos por una entidad certificadora autorizada, responder a formatos y estándares reconocidos internacionalmente y fijados por la ATT, contener como mínimo los datos que permitan identificar a su titular, a la entidad certificadora que lo emitió, su período de vigencia y contemplar la información necesaria para la verificación de la firma digital.* (Agencia para el Desarrollo de la Sociedad de la Información en Bolivia [ADSIB])

En consecuencia, es necesaria la clasificación de la misma, para poder identificar y clasificar la información en relación a valor para su uso. En efecto, se deben contemplar los requisitos legales, sensibilidad, criticidad para su uso y tratamiento, adecuados por la ADSIB.

La Constitucion Politica del Estado Plurinacional de Bolivia (2009), indica en relacion la administracion de los datos, donde, la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten el derecho fundamental a la intimidad y privacidad personal o familiar de toda persona individual o colectiva, la misma está amparada en la acción de protección de privacidad dentro de la Constitucion Politica del Estado. Para garantizar esto, todos los archivos o bancos de datos públicos o privados de las organizaciones, deben proporcionar la protección a los datos personales de las personas fisicas, tanto individuales como colectivas. En efecto, las organizaciones que traten con la información concerniente a una persona natural o jurídica que la identifica o la hace identificable, deben desarrollar políticas en relación a su tratamiento, transferencia o uso.

Los resultados de la entrevista realizada a la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia, evidencian el propósito de garantizar la acción de protección de privacidad, señalados en los lineamientos denominados como “Política de Protección de Datos Personales, descritas internamente en las Políticas de Certificación de la Entidad Certificadora ADSIB”, y la regulación por el ente moderador que es la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transporte (ATT) establece y condiciona que para el cumplimiento y presentación de servicios como Entidad Certificadora, debe realizar la protección de datos personales.

Si bien es cierto, los datos personales que se encuentran protegidos y administrados por la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB) en la firma digital y sus servicios, es corroborada por las políticas implementadas y sujetas en las condiciones instituidas por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y

Transportes (ATT) y obligaciones en protección de datos personales que eviten la divulgación no autorizada por las usuarias o usuarios, en el marco de la Constitución Política del Estado y la presente Ley N°164 Ley General de Telecomunicaciones. No obstante, la Agencia no cuenta con políticas de protección de datos personales dirigidas a la Sociedad de la Información, aquella sociedad que crece, se desarrolla alrededor de la información y el impulso tecnológico que permiten las tecnologías de la información y comunicación. Tema enfocado de la siguiente manera:

> *La Entidad Certificadora Pública considera que es relevante analizar y considerar la implementación de regulación integral sobre la protección de los datos personales que cursan a través de las TIC's, para otorgar seguridad y protección a la intimidad del usuario que navega en la red*. (Agencia para el Desarrollo de la Sociedad de la Información en Bolivia [ADSIB])

La afirmación anterior, contempla que la ADSIB considera necesario el implementar una regulación integral para la protección de los datos personales de la sociedad de la información en Bolivia.

Sin embargo, para el buen desarrollo de la sociedad de la información es muy importante contemplar su alcance, como se realiza en países desarrollados que vislumbran la trascendencia de la sociedad información, que adquiere y se establece en niveles nacionales como internacionales. Por lo tanto, estos países examinan la necesidad de establecer medidas que garanticen el nivel de protección de datos personales en Estados u organizaciones internacionales. Tal como, se manifiesta en el reglamento general de protección de datos personales, establecido por países europeos para el buen funcionamiento de sus datos personales en relación con otros Estados con los que tengan convenios o compromisos internacionales, es por eso, que decide lo siguiente:

> *Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado.* (El Parlamento Europeo y el Consejo de la Unión Europea, 2016, p. 61)

A este respecto, los países u organizaciones que tengan relaciones con estos Estados de primer mundo, o buscan acceder a trabajar con los mismos, deben garantizar la protección de los datos personales, conforme a lo establecido en el reglamento general de protección de datos personales implementado por países de la Unión Europea.

A continuación, se describen los factores de filtración de la información, servicios, ataques cibernéticos, daño a la imagen, actividad económica y desarrollo de trámites, que son asociados directamente con la seguridad de la información, donde envuelve la confidencialidad, integridad y disponibilidad de la información, asimismo, comprometidos con la protección de los datos personales, considerados en los resultados más sobresalientes de la sociedad de la información en Bolivia, de la encuesta de opinión nacional en tecnologías de la información y comunicación.

Todo Estado u organización posee activos de información, que concierne a aquellos datos, información, sistemas y elementos relacionados con la tecnología de la información, como documentos electrónicos entre otros. Y que contiene o manipula información de valor para la institución, como ser información estratégica o confidencial. No obstante, en el grafico N°9 manifiesta que la población de un 24.8% de la sociedad de la información, revelo que trabajo alguna vez para el Estado o una organización pública o privada, en los cuales 17.6% miembros de la misma exponen que copio, movió y duplico documentos de estas entidades. Sin embargo, en el grafico N°9 se contempla que en los últimos 12 meses sufrió un problema de virus en su computadora en el uso de su correo electrónico personal o corporativo. Aunque, se contempla el

poco uso de las redes sociales como medio para enviar o recibir correo o documentos adjuntos. Según los resultados, debe considerarse la formación de medidas de control de difusión de la información dirigidas a la sociedad de la información en Bolivia, por la facilidad de reproducciones de la información en documentos de diferentes soportes.

Del análisis de los resultados de este estudio se puede afirmar que la sociedad de la información boliviana requiere acceder a la información de datos estadísticos de las organizaciones con un 33.4% manifestado en el grafico N°15 y la misma busca asentir en la información general sobre las instituciones y sobre todo información concerniente a su organización interna. Al mismo tiempo, revela el grafico N°16 que la sociedad de la información busca indagar sobre trámites y requisitos usados por estas organizaciones. No obstante, los resultados evidencian que esta población 47.5% realiza la búsqueda y trata de acceder a archivos de las páginas Web de los órganos del Estado. En efecto, los servicios basados en internet, mediante el empleo de las nuevas tecnologías de la información y comunicación, que permite la comunicación de las organizaciones y la sociedad de la información en Bolivia, logrando obtener un intercambio de acceso y recogida de información. En consecuencia, la información puesta a disponibilidad por medio de las páginas Web de las organizaciones, son necesariamente cercioradas del tipo de información a disposición, evitando futuras vulnerabilidades y accesos no autorizados al tipo de información, afín de que, proporcione una buena distribución y acopio de la información.

Uno de los hallazgos principales de esta investigación, en el grafico N°21 revela que todas las personas que trabajan tuvieron un problema de virus en su computadora, donde un 35.8% desarrolla sus actividades laborales en una organización, sufriendo al mismo tiempo un problema de virus. Sin embargo, en el grafico N°19 detalla la acción realizada ante el inconveniente,

indicando que la población contacto con un técnico 42.4% ante tal eventualidad y un 29.8% uso un antivirus. Por consiguiente, Gómez Vieites (2007) revela. “Un virus informático trata de reproducirse rápidamente para extender su alcance, alcanzando en la actualidad una propagación exponencial gracias al desarrollo de internet y de las redes de ordenadores” (p.164). Puesto que, la carga dañina de un virus informático es conforme al nivel de alcance, donde la misma busca propagarse provocando una infección automática de los ordenadores. En efecto, produce una pérdida y robo de información.

Por otro lado, en este estudio se evidencia la imagen de las Entidades de Estado ante la sociedad de la información en Bolivia, donde en el gráfico N°22, la sociedad de la información plantea que confía poco 37.7%, más o menos 32.7% y no confía 21.7% en las redes sociales. Por consiguiente, los organismos de Estado, buscan desarrollar más una imagen por medio del Internet ante la sociedad de la información. Tal como se describe en lo siguiente:

> *Para 2017, la situación ha variado. Las cuentas en redes sociales se han incrementado, tanto que para octubre de ese año llegaban a 600 cuentas en Facebook, 216 en YouTube y 129 en Twitter (entre oficiales y no oficiales), de los distintos niveles de gobierno. Así, se nota que los gobiernos municipales, en este caso de La Paz y Santa Cruz, han invertido recursos para pautear en Facebook e incrementar su número de seguidores, es decir, que la importancia que le dan a las redes sociales hoy en día sin duda es mayor y cada vez requiere servicios más profesionales.* (Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación [AGETIC], 2018, p. 340)

Queremos con ello significar, la presencia de los organismos de Estado presentes en las redes sociales, donde las mismas buscan dar a conocer su imagen y actividades por medio del Internet. Sin embargo, en el gráfico N°23 explica la confianza de la información de las redes sociales difundidas por la página de Gobierno Nacional, destacan que confía poco con un 30.8%, más o menos 27.2% y no confía 18.1%. En efecto, lo mismo sucede al acceder a la página web del Gobierno Nacional donde 82.5% indica no hacerlo. Asimismo, la página web de la Gobernación

(Prefectura) revela que 90.7% no lo hace. De igual manera, en la página web del Poder Judicial que un 93.1% asegura no hacerlo. Así también, en la página web del Tribunal Supremo Electoral que con 88.1% asegura que no. Además, tampoco visita la página web de las Universidades con 74% expone no hacerlo. En conclusión, la imagen de los distintos organismos de Estado mediante sus páginas web percibida por la sociedad de la información boliviana, se puede evidenciar la falta de confianza hacia la misma.

Este estudio nos permite entender las diversas características de la sociedad de la información, donde la actividad económica de esta población se caracteriza especialmente por su aprovechamiento de las nuevas tecnologías, los resultados de esta investigación evidencian en el gráfico N°31 expresa que la sociedad de la información realiza pagos a través de internet, que en el cual los pagos de luz, tv cable y agua son un 35.4% favorece a la misma. Asimismo, un 22.8% indica realizarlo para créditos bancarios. No obstante, se evidencia que las 3 características de pago descritas son mediante el uso de tarjetas de crédito. “En este sentido, las TIC han pasado de ser un privilegio a ser una necesidad para la población y el desarrollo del Estado en general, convirtiéndose en servicios básicos que deberían ser de acceso universal” (Agencia de Gobierno Electronico y Tecnologias de la Informacion y Comunicacion [AGETIC], 2018, p. 431). Sin embargo, ante la popularidad de ésta, la sociedad de la información necesita sobrellevar posibles intentos de robos.

Los trámites efectuados son desarrollados con poca coordinación interinstitucional, e ignorando las necesidades y demandas de la sociedad de la información desconocen la complejidad técnica para digitalizar, ya que este proceso requiere el uso de herramientas tecnológicas y profesionales especializadas que muchas instituciones desconocen. Al mismo tiempo, las evidencias de esta investigación manifiestan que en el gráfico N°32 revela que las

personas con un 78.1% no recaban información o requisitos sobre trámites en el sector público. Así mismo, el gráfico N°33 ostenta que la sociedad de la información con un 82.8% no completa y envía formularios de trámites del sector público. Es decir, que la diligencia de la sociedad de la información en Bolivia con los tramites actuales no confía en ellos y asegura no hacerlo. De ahí que, una de las causas posibles se determina en la siguiente explicación:

> *En efecto, en la región los trámites son difíciles. Son lentos, vulnerables a la corrupción, y terminan excluyendo a la gente con menos recursos. Muchos de ellos todavía se gestionan en persona y en papel. Los ciudadanos pierden tiempo entre ventanilla y ventanilla y, en muchos casos, terminan pagando sobornos a los funcionarios. Las empresas pierden horas productivas y, con ellas, parte de su competitividad. El Estado se enreda en procedimientos complejos y manuales, y no logra conectar a las políticas públicas con los beneficiarios objetivo. En definitiva, con los trámites difíciles todos pierden.* (Banco Interamericano de Desarrollo [BID], 2018, p. 17)

Si bien es cierto, la sociedad de la información en Bolivia no realiza tramites a través de internet contemplando negativamente con un 86.3% revelado en el gráfico N°35. Al mismo tiempo, sucede en el gráfico N°36 que detalla si existe la realización de trámites en las páginas del Gobierno Nacional en el cual un 77.3% indica no hacerlo. Asimismo, en el gráfico N°37 que indica el porcentaje de la población que realiza trámites en la página web del Gobierno Municipal un 73.6% indica no hacerlo. Además, entre otros como los gráficos N°39 y N°40 revela la negativa de la sociedad de la información en los trámites de las páginas del Poder Judicial con 76.3% indicando no hacerlo y en las páginas del Tribunal Supremo Electoral se revela que con un 77.5% manifiesta no hacerlo. En conclusión, la coordinación interinstitucional con el apoyo de profesionales que facilitan el acceso a la información, más la integración de seguridad de la información que garantice la confidencialidad, integridad y disponibilidad de la información, son necesarias para el buen funcionamiento y explotación de las nuevas tecnologías de la información y comunicación.

CAPITULO VI - CONCLUSIÓN

La seguridad de la información y protección de datos personales en la firma digital de la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB), da como resultado una ratificada seguridad orientada confidencialidad, disponibilidad e integridad de la información y la protección de los datos personales enfocada en el servicio de Certificación Digital y Firma Digital, la cual está protegida contra diferentes amenazas, vulnerabilidades e identificando un nivel de riesgo para cada una de ellas. En efecto, estas capacidades están establecidas con políticas de seguridad y protección de datos personales. No obstante, la agencia no ha desarrollado políticas de seguridad de la información y protección de datos personales orientadas a la sociedad de la información en boliviana, donde, la Agencia es responsable para su buen desarrollo a nivel nacional.

Se determinó que las causas de filtración de la información por medio de la sociedad de la información boliviana. Esto es, el mismo grupo poblacional que aprovecha el uso de las nuevas tecnologías de la información y comunicación y desarrolla sus actividades laborales en organizaciones públicas como privadas y señala que la información que manipula es perteneciente a las organizaciones públicas y privadas y la manera que desplazada esta información es mediante la copia y duplicado de la misma. Al mismo tiempo, es consiente que en los último 12 meses sufre con problemas de virus en su computadora. Sin embargo, continua con el uso de su correo electrónico personal y corporativo, en el cual este medio es usado como tipo de comunicación rápida, barata y asíncrona, la misma también se ve afectada por distintos problemas de seguridad, mediante la falta de control y conciencia de la sociedad de la información en el uso de su correo electrónico sobrellevando sus actividades laborales con

problemas de virus y desplazando, copiando y duplicando información de las entidades públicas y privadas.

Siendo las cosas así, resulta clara la vulnerabilidad que proporciona la sociedad de la información en la revelación de la información de las organizaciones a terceros mediante el fácil desplazamiento y duplicado de la información sin la autorización concerniente, asimismo, la filtración de la información contenida en correos electrónicos. Sin embargo, llama la atención la regularidad de transferir información mediante la conexión de otros dispositivos a las computadoras.

La Sociedad de la Información boliviana considera la sensibilidad de los servicios de información ante la disposición del tipo de información proporcionada (información pública, restringida o clasificada), en los servicios de información de las organizaciones, es decir, medidas necesarias para evitar vulnerabilidades, accesos no autorizados y mala distribución y acopio de la información puesta a disposición por las organizaciones, debido a que, esta sociedad requiere acceder a información de datos estadísticos de las organizaciones. Asimismo, busca conseguir información general sobre las instituciones y sobre todo información concerniente a la organización interna. No obstante, también busca indagar sobre trámites y requisitos establecidos por las organizaciones. Al mismo tiempo, acceder a archivos de las páginas web de los organismos del Estado.

La identificación de la sensibilidad de la Sociedad de la Información en Bolivia ante ataques cibernéticos puede considerarse neutro entre lo bueno y malo. Estos ataques, son mayormente perpetrados mediante la infección y uso de virus informáticos. Un ejemplo de su comportamiento es similar a los virus biológicos con carácter infeccioso, capaz de tener vida independiente. Sin embargo, todas las personas que trabajan manifestaron que tuvieron problemas con virus en sus

computadoras. No obstante, ante tal eventualidad revelaron que esta población percibe la necesidad de contactar con un técnico o el uso un antivirus.

Se examinó la imagen de las entidades de Estado contempladas en la Sociedad de la Información en Bolivia, ante el incremento de su presencia en las distintas redes sociales. Mientras que, conforme a tal acción esta sociedad confía poco, más o menos y no confía en la información de estas entidades en las Redes Sociales. En consecuencia, no acceden ni usan las páginas web de diferentes organismos de Estado, por la falta de claridad existente en la misma.

Se describió a la sociedad de la información boliviana que se apoya en las tecnologías comprendiendo las facilidades que brindan en la creación, distribución y manipulación de la información. Sobre todo, las que juegan un papel esencial en las actividades sociales, culturales y económicas. En otras palabras, la actividad económica de esta población se caracteriza especialmente en el aprovechamiento de las nuevas tecnologías, puesto que, contempla la realización de pagos a través de internet, destinados a pagos de luz, tv cable y agua, acciones que son realizadas mediante el uso de tarjetas de crédito.

La diligencia de la sociedad de la información referente a los trámites desarrollados por las organizaciones burocráticas y de control jerárquico no permite alcanzar o responder hacia un desafió de la velocidad que exige la era moderna. Por lo tanto, para mantener a la empresa u organización en pie surgieron nuevos diseños que rechazan la rigidez e introducen formas planas, horizontales y flexibles, donde la información fluya libremente. En consecuencia, la sociedad no realiza trámites a través de internet, a causa de la burocratización que se les da a los procesos.

BIBLIOGRAFÍA

Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación [AGETIC]. (2018). *Estado de las Tecnologías de Información y Comunicación en el Estado Plurinacional de Bolivia.* La Paz.

Agencia de Gobierno Electrónico y Tecnologías de la Información y Comunicación [AGETIC]. (2016). *Propuesta para la clasificación de la información*. La Paz, Bolivia.

Agencia de Gobierno Electrónico y Tecnologías de la Información y Comunicación *[AGETIC]. (2018). Estado TIC. La Paz, Bolivia.*

Agencia para el desarrollo de la sociedad de la información en Bolivia [ADSIB]. (17 de Agosto de 2017). *Adsib.* Recuperado de www.firmadigital.bo/ayuda.html#practicas-politicas

Agencia para el Desarrollo de la Sociedad de la Información en Bolivia [ADSIB]. (s.f.). *Políticas de certificación de la entidad certificadora pública Agencia para el Desarrollo de la Sociedad de la Información en Bolivia [ADSIB]*. La Paz, Bolivia.

Arévalo Ascanio, J. G., Bayona trillos, R. A., & Rico Bautista, D. W. *(2015*). Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: análisis del riesgo de la información. *Tecnura.*

Banco Central de Bolivia [BCB]. (21 de Agosto de 2017). *Seguridad de la información. (A. d. información, Recopilador)* La Paz, Murillo, Bolivia. Recuperado de https://ctic.gob.bo/nube/s/qGYfkD7J7b8uuK6

Banco Interamericano de Desarrollo [BID]. (2018). *El fin del trámite eterno. Washington, D.C. : Sarah Schineller (A&S Information Specialists, LLC)*

Blanco de la lama, A. (1981). *La revelación como locutio dei en la obra de Santo Tomas.* Pamplona.

Bustamante Paco, S. (2014). *Casos prácticos de estrategias de marketing en bibliotecas, archivos y museos: modelos de planificación estratégica y proyecto de grado.* La Paz, Bolivia: Stigma.

Candid W. (5 de Agosto de 2016). *¿Cuánto cuestan los datos robados y servicios de ataque en el mercado clandestino?* [Mensaje en un blog]. Recuperado de https://www.symantec.com/connect/ru/blogs/cuanto-cuestan-los-datos-robados-y-servicios-de-ataque-en-el-mercado-clandestino?page=1

Castel, J. (6 de diciembre de 2017). El 'efecto Pari' obliga a la banca a mejorar controles. *La Razón.* Recuperado de http://www.la-razon.com/suplementos/financiero/efecto-Pari-obliga-mejorar controles_0_2831716876.html

Conde, E. V., & Arteaga, F. (2011). *Glosario de Términos de Ciencias de la Información.* La Paz, Bolivia.

Consejo Internacional de Archivos. (Septiembre de 1996). *Código de ética profesional.*

Consejo para las tecnologías de información y comunicación [CTIC]. (27 de Agosto de 2017). Recuperado de https://www.ctic.gob.bo/

Cornella, A. (2004). *Infoxicación: buscando un orden en la información.* Barcelona: Infonomia.

Cuba Q., S. (2011). *Manual de gestión documental y administración de archivos II.* La Paz, Bolivia.

Daros, W. R. (2006). *La libertad individual y el contrato social según J. J. Rousseau. Filosofía universitaria de Costa Rica.*

Delito cibernético. (25 de Agosto de 2017). *Departamento Federal de Investigaciones [FBI]*. Recuperado de: https://www.fbi.gov/investigate/cyber

Diez claves para entender el caso Quiborax en torno a Carlos Mesa. (11 de Julio de 2018). *Los tiempos*. Recuperado de http://www.lostiempos.com/actualidad/pais/20180711/diez-claves-entender-caso-quiborax-torno-carlos-mesa

El Parlamento Europeo y el Consejo de la Unión Europea. (27 de Abril de 2016). *Reglamento (UE) 2016/679 del parlamento europeo y del consejo de 27 de abril de 2016.* Reglamentos. Unión Europea.

En Portada. (2006). *La gestión de la seguridad en la empresa*. En portada.

Especial directivos. (2014). *Los principales riesgos de la empresa española en cuanto a seguridad de la información*. Especial ediciones.

Federación Internacional de Asociaciones e Instituciones Bibliotecarias [IFLA]. (2003). *Prevención de desastres y planes de emergencia.*

Federer, L. (2018). *Cuáles son las habilidades necesarias de un un bibliotecario de datos* [Mensaje en un blog]. Recuperado de https://universoabierto.org/2018/07/03/cuales-son-las-habilidades-necesarias-de-un-un-bibliotecario-de-datos/

Flores Barrios, L., Soto del Ángel, M., Camacho Díaz, O. D., & Barrera Reyes, M. A. (2011). Evaluación del impacto de los sistemas de gestión de seguridad de la información bajo la serie ISO/IEC 27001 en empresas de la ciudad de Tuxpan, Veracruz. *Revista de la alta tecnología y la sociedad*, *4*(1)44.

Fonnegra Osorio, C. P. (2014). *Benjamín Constant. Libertad, democracia y pluralismo. Estudios políticos*.

Gaceta oficial de Bolivia (2005). *Decreto Supremo N. 28168 para Garantizar el acceso a la información, como derecho fundamental de toda persona y la transparencia en la gestión del Poder Ejecutivo.* Recuperado de http://www.gacetaoficialdebolivia.gob.bo/index.php/normas/buscar

Gaceta oficial de Bolivia (2009). *Constitución Política del Estado Plurinacional de Bolivia* Recuperado de http://www.gacetaoficialdebolivia.gob.bo/index.php/normas/lista/9

Gaceta oficial de Bolivia (8 de Agosto de 2011). Decreto supremo N° 1793 *Reglamento para el desarrollo de tecnologías de información y comunicación.* Recuperado de http://www.gacetaoficialdebolivia.gob.bo/index.php/normas/buscar

Gaceta oficial de Bolivia (8 de Agosto de 2011). Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación *N. 164* Recuperado de https://att.gob.bo/sites/default/files/archivosvarios/Ley%20164%20%20Ley%20General%20de%20Telecomunicaciones%2C%20Tecnlolog%C3%ADas%20de%20Informaci%C3%B3n%20y%20Comunicaci%C3%B3n.pdf

García Rojas, W. A. (2008). *Implementación de firma digital en una plataforma de comercio electrónico.* (Tesis de pregrado) Pontifica Universidad Católica del Perú. Lima, Perú.

Gómez Vieites, A. (2007). *Enciclopedia de la seguridad informática*. México: Alfaomega.

Gómez Vieites, A. (Mayo de 2007). *Sistemas criptográficos simétricos*. México, México.

Hernández Sampieri, R., Fernández Collao, C., & Baptista Lucio, P. (2014). *Metodología de la investigación* (6 ed.). México: McGraw-Hill.

Herrera, N. (12 de Julio de 2012). *Teoría clásica de la administración.* Recuperado de Organización Norelys Herrera: https://sites.google.com/site/organizacionnorelys/teoria-clasica-de-la-administracion

Instituto Boliviano de Normalización y Calidad [IBNORCA]. (2010). *Norma Boliviana NB/ISO/IEC 27000 Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de la seguridad de la información – Visión general y vocabulario.* La Paz.

Internacional. (6 de Abril de 2018). La filtración de datos de Facebook podría haber afectado a 2,7 millones de europeos. *Internacional*. Obtenido de https://elpais.com/internacional/2018/04/06/actualidad/1523012161_044631.html

La filtración de datos de Facebook podría haber afectado a 2,7 millones de europeos. (6 de Abril de 2018). *El País.* Recuperado de https://elpais.com/internacional/2018/04/06/actualidad/1523012161_044631.html

La protección de datos exige nueva profesión (15 de Mayo de 2018). *El Deber*. Recuperado de https://www.eldeber.com.bo/dinero/La-proteccion-de-datos-exige-nueva-profesion-20180514-8597.html

Ladino A., M. I., Villa S., P. A., & López E., A. M. (2011). *Fundamentos de ISO/27001 y su aplicación en las empresas.* Sciencia et technical.

Lin Zambrana, M. H. (12 de Septiembre de 2016). *Clasificación de la Información*. La Paz, Bolivia.

López Rojas, M. D., Suarez Botero, D. M., & Meneses Durango, C. N. (2011). Firma digital: instrumento de transmisión de información a entidades financieras. *Revista Avances en Sistemas e Informática*, 8(1).

Maggiore, M. L. (2014). *Modelo de evaluación de madurez para la gestión de la seguridad de la información integrada en los procesos de negocio.*

Martínez Martínez, R. (2007). El derecho fundamental a la protección de datos: perspectivas. *IDP Revista de internet, derecho y política*. (5) Recuperado de http://www.redalyc.org/articulo.oa?id=78812861005

Miguel Pérez, J. C. (2015). *Protección de datos y seguridad de la información*. España: Ra-ma.

Ministerio de Transparencia Institucional y Lucha contra la Corrupción. (s.f.). *Proyecto de ley de transparencia y acceso a la información pública.*

Ministro de Salud reveló la enfermedad incurable de Cusi (19 de agosto de 2018). *Erbol.* Recuperado de https://erbol.com.bo/noticia/social/22122014/ministro_de_salud_revelo_la_enfermedad_incurable_de_cusi

Montiel, L., Hernández, F., Lizama, L., Lizama, L., & Simancs, E. (2017). *Firma digital móvil basada en criptografía Hash.* México: ECORFAN.

Najar Pacheco, J. C., & Suarez Suárez, N. E. (2015). La seguridad de la información: un activo valioso de la organización. Vínculos, 12(1).

Oporto Ordoñez, L. (2011). *Archivos militares de Bolivia historia y organización archivística.* La Paz: La Pesada.

Oporto Ordoñez, L. (2015). *Acceso a la información pública, archivos y bibliotecas en la constitución política del estado.* La Paz.

Oporto Ordóñez, L., & Rosso Ramirez, F. (2007). *Legislación archivística boliviana el ABC normativo del archivero boliviano.* La paz: Grafica druck.

Paredes Granados, G. (2006). Introducción a la criptografía. *Revista Digital Universitaria*,*7*(7), 13.

Paul, R. (26 de julio de 2018). Facebook sufre la mayor pérdida en la historia de la bolsa. *El País*. Recuperado de https://cnnespanol.cnn.com/2018/07/26/facebook-recupera-inversores-panico/

Qué Es Un Hash Y Cómo Funciona (10 de abril de 2014). [Mensaje en un blog] Recuperado de https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/

Real Academia Española. (21 de Septiembre de 2017). *Diccionario de la real academia española* Recuperado de http://dle.rae.es/?w=diccionario

Redacción de Capital Humano. (2012). *Una cultura fuerte es la mejor protección de la información confidencial.*

Reynoso Castillo, C. (2017). Privacidad y protección de datos en las relaciones laborales. *Alegatos*.

Rodríguez, G. A. (2010). *Las nuevas entidades de Información.* México: Universidad Nacional Autónoma de México.

RT Noticias Internacionales. (05 de Abril de 2018). *Facebook admite que se filtraron datos de 87 millones de usuarios*. Recuperado de https://actualidad.rt.com/video/267592-facebook-admite-filtraron-datos-87

Sánchez, Vanderkst, E. J. (2014). *El acceso a la información gubernamental: experiencias y expectativas*. México: Universidad Nacional Autónoma de México.

Suarez, L. E. (2013). *Mejoramiento de la gestión de tramite documentario utilizando la firma digital en el proyecto especial Alto Mayo - Moyobamba.*

Torres Gorena, F., Suarez Mamani, J., Telleria Escobar, L., & Mérida Aguilar, I. F. (2016). *Bolivialeaks*. La Paz: Ministerio de la presidencia.

Torres, I. P. (2016). *Propuesta de estándar de seguridad de la información.*

Una fuga de datos de Facebook abre una tormenta política mundial (20 de marzo de 2018). *El País*. Recuperado de https://elpais.com/internacional/2018/03/19/estados_unidos/1521500023_469300.html

Unión Internacional de Telecomunicaciones. (2007). *Guía de Ciberseguridad para los países en desarrollo.*

Universidad de Chile. (1 de Octubre de 2018). *Información y bibliotecas*. Obtenido de Índice h: http://www.uchile.cl/portal/informacion-y-bibliotecas/ayudas-y-tutoriales/100617/indice-h

Universo Abierto. (2018). *Blog de la biblioteca de Traducción y Documentación de la Universidad de Salamanca*. Obtenido de ¿Cuáles son las habilidades necesarias de un bibliotecario de datos?

Voutssas, M. J. & Barnard Amozorrutia, A. (2014). *Glosario de preservación archivística digital versión 4.0.* México: UNAM.

Zabala Trías, S. (2002) *Guía a la redacción en el estilo APA, 6ta edición.* UMET

CAPITULO VII - MARCO PROPOSITIVO

TÍTULO:

Implementación de un Acuerdo de Confidencialidad para la desvinculación del personal, para mejorar la seguridad de la información de los datos personales en la firma digital de los usuarios de la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB) para el período 2019.

INSTITUCIÓN EJECUTORA:

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

BENEFICIARIOS:

Funcionarios, y usuarios de la sociedad de la información de Bolivia.

UBICACIÓN:

Ciudad de La Paz, Calle Mercado esquina Yanacocha #...

TIEMPO ESTIMADO DE LA EJECUCIÓN:

6 meses

INICIO:

Enero 2019

FINALIZACIÓN:

Julio 2019

EQUIPO TÉCNICO RESPONSABLES:

Directora Ejecutiva, Maria Jannett Ibañez Flores.

Profesional en Recursos Humanos, Livia Terán Claros.

COSTO:

74070 Bs (SETENTA Y CUATRO MIL SETENTA BOLIVIANOS 00/100)

ANTECEDENTES DE LA PROPUESTA

En la investigación que se realizó mediante encuesta y entrevistas, se determinó la obligación y necesidad de contar con estrategias para garantizar la seguridad de la información en los recursos humanos.

Una de las estrategias es contar con acuerdos de confidencialidad que garanticen la seguridad de la información al desvincular al recurso humano de la entidad, así mismo, garantizará que la información personal de los usuarios no sea divulgada, logrando mayor seguridad de los datos personales de los mismos y mejorando el servicio de los usuarios de la sociedad de la información en Bolivia, lo que permitirá solucionar la vulnerabilidad de la información.

JUSTIFICACIÓN

Es necesario establecer mecanismos de relación, en materia de seguridad de la información, entre el recurso humano y la entidad o institución pública con el objetivo de preservar la información a la que tienen acceso durante y después de la vinculación laboral.

El acuerdo de confidencialidad brinda beneficios a ambas partes garantizando la seguridad de la información. Se conoce que la información es el pilar fundamental para el desarrollo de las empresas y la sociedad en general, por lo tanto, se necesita que los funcionarios tengan el criterio de garantizar la seguridad de la información, conforme a las necesidades y la realidad social.

Así mismo, se logrará crear conciencia de la importancia de un acuerdo de confidencialidad y su estricto cumplimiento, garantizando la confidencialidad de la información.

OBJETIVOS

OBJETIVO GENERAL

Mejorar la seguridad de la información de los datos personales en la firma digital, al desvincular a los recursos humanos que trabajan en la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB) garantizando la disponibilidad de la misma, manteniendo su confidencialidad, logrando prevenir fugas, divulgaciones no autorizadas y mal uso de la información.

OBJETIVOS ESPECÍFICOS

- Crear acuerdos de confidencialidad.
- Garantizar la confidencialidad de la información de los usuarios.
- Concientizar a los funcionarios de la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB) sobre la seguridad de la información de los datos personales en la firma digital.
- Informar sobre las responsabilidades adquiridas al firmar el acuerdo de confidencialidad.
- Evitar la filtración de la información de los usuarios de la sociedad de la información.

ANÁLISIS DE FACTIBILIDAD

La presente propuesta es factible porque la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB) , está prestando su apoyo en cuanto a la realización, preparación y capacitación, lo que permitirá tener una buena acogida con los funcionarios, quienes tienen la predisposición y aceptación, de ser capacitados en la firma del acuerdo de confidencialidad; realizado con autofinanciamiento, ya que es para proteger uno de sus activos de información, y por lo tanto la entidad debe destinar presupuesto, para garantizar la seguridad de la información de los datos personales en la firma digital.

MODELO OPERATIVO DE LA PROPUESTA

La presente propuesta tiene la finalidad de capacitar a los funcionarios Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB), sobre la seguridad de la información al desvincular a los recursos humanos de la entidad**.**

OBJETIVOS ESTRATÉGICOS	ACTIVIDADES	RECURSOS	RESPONSABLES	TIEMPO	RESULTADOS
Crear acuerdos de confidencialidad.	Elaborar borradores de acuerdos de confidencialidad	➢ Asesores legales ➢ Material de escritorio	RECURSOS HUMANOS	1 mes	Garantizar la confidencialidad de la información de los usuarios.
	Revisar y aprobar los acuerdos de confidencialidad	➢ Material de escritorio ➢ Equipo electrónico	RECURSOS HUMANOS	1 mes	
Concientizar a los funcionarios de la Agencia Para El Desarrollo De La Sociedad De La Información En Bolivia (Adsib) sobre la seguridad de la información de los datos personales en la firma digital.	Realizar talleres de concientización.	➢ Material de escritorio ➢ Equipos electrónicos	RECURSOS HUMANOS	1 mes	Funcionarios consientes de la importancia de los acuerdos de confidencialidad.

	Hacer conocer las obligaciones y responsabilidades de firma un acuerdo de confidencialidad.	➢ 1 archivista		1 mes	
Informar sobre las responsabilidades adquiridas al firmar el acuerdo de confidencialidad.	Realizar seminarios de información	➢ Asesor legal ➢ Material de escritorio ➢ Archivista	RECURSOS HUMANOS	1 mes	Funcionarios informados e la responsabilidad de los acuerdos de confidencialidad.
Evitar la filtración de la información de los usuarios de la sociedad de la información.	Hacer cumplir los acuerdos de confidencialidad.	➢ Material de escritorio ➢ Asesor legal ➢ Recursos económicos	➢ RECURSOS HUMANOS ➢ ÁREA LEGAL	1 mes	Seguridad de la información garantizada y confiable

PRESUPUESTO

Recursos Humanos

Personal	Cantidad	Costo / mes	Costo / año
Asesores legales	2	2500 Bs.	30000 Bs.
Archivista	2	2500 Bs.	30000 Bs.
Total	4	-	60000 Bs.

- **CURSOS DE CAPACITACIÓN**

Nombre	Cantidad	Duración / meses / días	Costo	Total
Taller	2	5 días	100 Bs.	1000 Bs.
Seminario	2	3 días	50 Bs.	300 Bs.
TOTAL	4	8 días	-	1300 Bs.

- **MATERIAL DE ESCRITORIO**

Insumos	Cantidad	Descripción	Costo / Unid	Total
Computadora I5	1	LG.	7000 Bs.	7000 Bs.
Impresora EPSON 380	1	EPSON	1150 Bs.	1150 Bs.
Hojas	4	-	30 Bs.	120 Bs.
Fotocopiadora	1	-	2500 Bs.	2500 Bs.
Material en general	-	-	2000 Bs.	2000 Bs.

TOTAL	-	-	-	12770 Bs.

- **PRESUPUESTO - RESUMEN**

Cuadro – Resumen de Gastos	**Total**
Recursos Humanos	60000 Bs.
Cursos de capacitación	1300 Bs.
Material de escritorio	12770 Bs.
TOTAL	74070 Bs.

Modelo De Contrato De Confidencialidad

CONTRATO DE CONFIDENCIALIDAD

A objeto de garantizar la confidencialidad entre la empresa y el empleador, se hace necesaria la firma de un acuerdo que garantice unos niveles de confianza entre las partes. El documento se firmará una vez aceptado y firmado el por ambas partes.

Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB) y en su nombre y representación, Maria Jannett Ibañez Flores Directora Ejecutiva, con cedula de identidad # …….

Por otro las [nombre] con poder suficiente para ello, en calidad de [cargo, administrador,]

I – Que las partes, anteriormente citadas, están interesadas en el desarrollo del presente contrato, para lo cual, aceptaron celebrar el presente Acuerdo de Confidencialidad con el fin de establecer el procedimiento que regirá la custodia y no transmisión a terceros de la información distribuida entre las partes, así como los derechos, responsabilidades y obligaciones inherentes en calidad de remitente, Propietario y «Destinatario» de la referida información.

II – Que las partes, en virtud de lo anteriormente expuesto, convinieron que el presente Acuerdo de Confidencialidad se rija por la normativa aplicable al efecto y, en especial por las siguientes cláusulas:

PRIMERA - Definiciones

A los efectos del presente Acuerdo, los siguientes términos serán interpretados de acuerdo con las definiciones anexas a los mismos. Entendiéndose por:

- «Información propia»: descubrimientos, conceptos, ideas, conocimientos, técnicas, diseños, dibujos, borradores, diagramas, textos, modelos, muestras, bases de datos de cualquier tipo, aplicaciones, programas, marcas, logotipos, así como cualquier información de tipo técnico, industrial, financiero, publicitario, de carácter personal o comercial de cualquiera de las partes, esté o no incluida en la solicitud de oferta presentada, independientemente de su formato de presentación o distribución, y aceptada por los «Destinatarios».

- «Dato personal»: es la información de carácter personal concerniente a una persona, dicha información es usada habitualmente en una sociedad de la información, gracias al uso de las nuevas tecnologías de la información y comunicación. Al mismo tiempo, los datos personales representan a una persona en distintos soportes o características, ya sea fecha de nacimiento, correo electrónico, número telefónico, hasta el historial médico.

- «Fuente»: tendrá la consideración de tal, cualquiera de las partes cuando, dentro de los términos del presente Acuerdo, sea ella la que suministre la Información Propia y/o cualquiera de los implicados (accionistas, directores, empleados) de la empresa o la organización.

- «Destinatarios»: tendrán la consideración de tales cualquiera de las partes cuando, dentro de los términos del presente Acuerdo, sean ellos quienes reciban la Información Propia de la otra parte.

SEGUNDA.- Información Propia.

Las partes acuerdan que cualquier información relativa a sus aspectos financieros, comerciales, técnicos, y/o industriales suministrada a la otra parte como consecuencia de la solicitud de Oferta para el desarrollo del presente proyecto objeto del contrato, o en su caso, de los acuerdos a los que se lleguen (con independencia de que tal transmisión sea oral, escrita, en soporte magnético o en cualquier otro mecanismo informático, gráfico, o de la naturaleza que sea) tendrá consideración de información confidencial y será tratada de acuerdo con lo establecido en el presente documento. Esa información, y sus copias y/o reproducciones tendrán la consideración de «Información propia» para los efectos del presente acuerdo.

TERCERA.- Exclusión del Presente Acuerdo.

No se entenderá por «Información propia», ni recibirá tal tratamiento aquella información que:

I – Sea de conocimiento público en el momento de su notificación al «Destinatario» o después de producida la notificación alcance tal condición de pública, sin que para ello el «Destinatario» violentara lo establecido en el presente acuerdo, es decir, no fuera el «Destinatario» la causa o «Fuente» última de la divulgación de dicha información.

II – Pueda ser probado por el «Destinatario», de acuerdo con sus archivos, debidamente comprobados por la «Fuente», que estaba en posesión de la misma por medios legítimos sin que

estuviese vigente en ese momento algún y anterior acuerdo de confidencialidad al suministro de dicha información por su legítimo creador.

III – Fuese divulgada masivamente sin limitación alguna por su legítimo creador.

IV – Fuese creada completa e independientemente por el «Destinatario», pudiendo este demostrar este extremo, de acuerdo con sus archivos, debidamente comprobados por la «Fuente».

CUARTA.- Custodia y no divulgación.

Las partes consideran confidencial la «Información propia» de la otra parte que le pudiera suministrar y acuerdan su guarda y custodia estricta, así como a su no divulgación o suministro, ni en todo ni en parte, a cualquier tercero sin el previo, expreso y escrito consentimiento de «Fuente». Tal consentimiento no será necesario cuando la obligación de suministrar o divulgar la «Información propia» de la «Fuente» por parte del «Destinatario» venga impuesta por Ley en vigor o Sentencia Judicial Firme.

Este Acuerdo no autoriza a ninguna de las partes a solicitar o exigir de la otra parte el suministro de información, y cualquier obtención de información de/o sobre la «Fuente» por parte del «Destinatario» será recibida por éste con el previo consentimiento de la misma.

QUINTA.- Soporte de la «Información propia».

Toda o parte de la «Información propia», papeles, libros, cuentas, grabaciones, listas de clientes y/o socios, programas de ordenador, procedimientos, documentos de todo tipo o tecnología en el que el suministro fuese hecho bajo la condición de «Información propia», con independencia del soporte que la contuviera, tendrá la clasificación de secreta, confidencial o restringida

SEXTA.- Responsabilidad en la Custodia de la «Información propia».

La «Información propia» podrá ser dada a conocer por el «Destinatario» o sus directivos y/o sus empleados, sin perjuicio de que el «Destinatario» tome cuantas medidas sean necesarias para el exacto y fiel cumplimento del presente Acuerdo, debiendo necesariamente informar a unos y otros del carácter secreto, confidencial, o restringido de la información que da a conocer, así como la existencia del presente Acuerdo.

Así mismo, el «Destinatario» deberá dar a sus directivos y/o sus empleados, las directrices e instrucciones que considere oportunas y convenientes a los efectos de mantener el secreto, confidencial, o restringido de la información propia de la «Fuente». El «Destinatario» deberá advertir a todos sus directivos, empleados, etc., que de acuerdo con lo dispuesto en este acuerdo tengan acceso a la «Información propia», de las consecuencias y responsabilidades en las que el «Destinatario» puede incurrir por la infracción por parte de dichas personas, de lo dispuesto en este Acuerdo.

Sin perjuicio de lo anterior, la «Fuente» podrá pedir y recabar del «Destinatario», como condición previa al suministro de la «Información propia», una lista de los directivos y empleados que tendrán acceso a dicha información, lista que podrá ser restringida o reducida por la «Fuente».

Esta lista será firmada por cada uno de los directivos y empleados que figuren en ella, manifestando expresamente que conocen la existencia del presente Acuerdo y que actuarán de conformidad con lo previsto en él. Cualquier modificación de la lista de directivos y/o empleados a la que se hizo referencia anteriormente será comunicada de forma inmediata a la «Fuente», por escrito conteniendo los extremos indicados con anterioridad en este párrafo.

Sin perjuicio de lo previsto en los párrafos anteriores, cada parte será responsable tanto de la conducta de sus directivos y/o empleados como de las consecuencias que de ella se pudieran derivar de conformidad con lo previsto en el presente Acuerdo.

SÉPTIMA.- Responsabilidad en la custodia de la «Información propia».

El «Destinatario» será responsable de la custodia de la «Información propia» y cuantas copias pudiera tener de la misma suministrada por la «Fuente», en orden a su tratamiento, como secreta, confidencial o restringida, en el momento presente y futuro, salvo indicación explicita de la «Fuente».

A objeto de garantizar esta custodia, se deberá devolver la «Información propia» y cuantas copias pudiera tener de la misma suministrada por la «Fuente», a la terminación de las relaciones comerciales, o antes, si fuera requerido por la «Fuente» y respondiendo a los daños y perjuicios correspondientes, en el caso de incumplimiento de lo aquí dispuesto. (En aquellos casos en los que no fuera necesaria la devolución de la «Información propia» deberá eliminarse este párrafo)

OCTAVA.- Incumplimiento.

El incumplimiento de las obligaciones de confidencialidad plasmadas en este documento, por cualquiera de las partes, sus empleados o directivos, facultará a la otra a reclamar por la vía legal lo que estime más procedente, a la indemnización de los daños y perjuicios ocasionados, incluido el lucro cesante.

NOVENA.- Duración del Acuerdo de Confidencialidad.

Ambas partes acuerdan mantener el presente Acuerdo de Confidencialidad, aún después de terminar sus relaciones comerciales.

DECIMA.- Legislación Aplicable

Constitución Política del Estado

Capítulo segundo: Principios, valores y Fines del estado

Art. 9 Inciso 2 Garantizar el bienestar, el desarrollo, la seguridad y la protección e igual dignidad de las personas, las naciones, los pueblos y las comunidades, y fomentar el respeto mutuo y el diálogo intercultural, y plurilingüe.

Garantías Jurisdiccionales y Acciones de Defensa, Capítulo Segundo Acciones de Defensa, Sección III Acción de Protección de Privacidad

Art. 130 I. Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad.

Art. 131 I. La Acción de Protección de Privacidad tendrá lugar de acuerdo con el procedimiento previsto para la acción de Amparo Constitucional.

Decreto supremo N° 1793 Reglamento para el Desarrollo de Tecnologías de Información y Comunicación

Da a conocer los aspectos más importantes a continuación:

Título I Disposiciones Generales

Art. 4.- (Principios) II. Tratamiento de datos personales: Los servicios de certificación digital en cuanto al tratamiento de datos personales, se regirán por los siguientes principios:

a) Finalidad: La utilización y tratamiento de los datos personales por parte de las entidades certificadoras autorizadas, deben obedecer a un propósito legítimo, el cual debe ser de conocimiento previo del titular;

b) Veracidad: La información sujeta a tratamiento debe ser veraz, completa, precisa, actualizada, verificable, inteligible, prohibiendo el tratamiento de datos incompletos o que induzcan a errores;

c) Transparencia: Se debe garantizar el derecho del titular a obtener de la entidad certificadora autorizada, en cualquier momento y sin impedimento, información relacionada de la existencia de los datos que le concierne.

d) Seguridad: Se deben implementar los controles técnicos y administrativos que se requieran para preservar la confidencialidad, integridad, disponibilidad, autenticidad, no repudio y confiabilidad de la información, brindando seguridad a los registros, evitando su falsificación, extravío, utilización y acceso no autorizado o fraudulento;

e) Confidencialidad: Todas las personas involucradas y que intervengan en el tratamiento de datos personales, están obligadas a garantizar la reserva de la información, incluso hasta después de finalizado su vínculo con alguna de las actividades que comprende el tratamiento, pudiendo únicamente realizar el suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las tareas autorizadas.

(En la protección de los datos, se debe identificar la finalidad de la misma, la veracidad de la información, si la misma está completa o cuenta con errores. También así, su transparencia, conforme al derecho del titular o datos con los que se relacionan. Tomando más relevancia al tema de seguridad, que exige que se deben implantar los controles tanto técnicos como administrativos, garantizando la confidencialidad, integridad y disponibilidad de la información y los datos)

Capítulo II Desarrollo de Contenidos y Aplicaciones

Art. 5.- (Desarrollo de Contenidos y Aplicaciones TIC) I. El Estado promoverá de manera prioritaria el desarrollo de contenidos y aplicaciones y servicios de las TIC en software libre, utilizando estándares abiertos y velando por la seguridad de la información en las siguientes áreas:

c) En la gestión gubernamental, a través de la implementación del gobierno electrónico promoviendo la transparencia y la capacitación de los recursos humanos para garantizar la eficiencia de los sistemas implantados.

Art. 6.- (Objetivos del Desarrollo de Contenidos Digitales). El desarrollo, diseño e innovación de contenidos digitales tendrán mínimamente los siguientes objetivos:

d) Promover la identidad cultural de los pueblos originarios, sus territorios ancestrales, usos y costumbres; para el bienestar, el desarrollo, la seguridad y la protección e igual dignidad de las personas, las naciones, los pueblos y las comunidades y fomentar el respeto mutuo y el diálogo intracultural, intercultural y plurilingüe;

m) Fortalecer la seguridad informática del Estado Plurinacional de Bolivia.

Art. 8 (Plan de Contingencia) Las entidades públicas promoverán la seguridad informática para la protección de datos en sus sistemas informáticos, a través de planes de contingencia desarrollados e implementados en cada entidad.

Título IV Certificado y Firma Digital y Entidades Certificadoras

Art. 44.- (Responsabilidad de las Entidades Certificadoras Autorizadas Ante Terceros) I. Las entidades certificadoras autorizadas serán responsables por la emisión de certificados digitales con errores y omisiones que causen perjuicio a sus signatarios.

Art. 46.- (Auditorías) I. Las entidades certificadoras podrán ser sometidas a inspecciones o auditorías técnicas por la ATT.

II. La ATT, podrá implementar el sistema de auditoría, que debe como mínimo evaluar la confiabilidad y calidad de los sistemas utilizados, el cumplimiento de los estándares nacionales e internacionales sobre certificación y firma digital, la integridad, confidencialidad y disponibilidad de los datos, como así también el cumplimiento de las políticas de certificación definidas por la

autoridad, su declaración de prácticas de certificación y los planes de seguridad y de contingencia aprobados.

Art. 54.- (Derechos del Titular del Certificado) El titular del certificado digital tiene los siguientes derechos:

b) A la confidencialidad de la información proporcionada a la entidad certificadora.

Capítulo II Tratamiento de los Datos Personales

Art. 56.- (Protección de Datos Personales) A fin de garantizar los datos personales y la seguridad informática de los mismos, se adoptan las siguientes previsiones:

a) La utilización de los datos personales respetará los derechos fundamentales y garantías establecidas en la Constitución Política del Estado;

b) El tratamiento técnico de datos personales en el sector público y privado en todas sus modalidades, incluyendo entre éstas las actividades de recolección, conservación, procesamiento, bloqueo, cancelación, transferencias, consultas e interconexiones, requerirá del conocimiento previo y el consentimiento expreso del titular, el que será brindado por escrito u otro medio equiparable de acuerdo a las circunstancias. Este consentimiento podrá ser revocado cuando exista causa justificada para ello, pero tal revocatoria no tendrá efecto retroactivo;

c) Las personas a las que se les solicite datos personales deberán ser previamente informadas de que sus datos serán objeto de tratamiento, de la finalidad de la recolección y registro de éstos; de los potenciales destinatarios de la información; de la identidad y domicilio del responsable del tratamiento o de su representante; y de la posibilidad de ejercitar los derechos de acceso, rectificación, actualización, cancelación, objeción, revocación y otros que fueren pertinentes. Los datos personales objeto de tratamiento no podrán ser utilizados para finalidades distintas de las expresadas al momento de su recolección y registro;

d) Los datos personales objeto de tratamiento sólo podrán ser utilizados, comunicados o transferidos a un tercero, previo consentimiento del titular u orden escrita de autoridad judicial competente;

e) El responsable del tratamiento de los datos personales, tanto del sector público como del privado, deberá adoptar las medidas de índole técnica y organizativa necesarias que garanticen la

seguridad de los datos personales y eviten su alteración, pérdida, tratamiento no autorizado, las que deberán ajustarse de conformidad con el estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

Empleado	Entidad
_____	_____
Firma	Firma
representante _____	representante_____
	DNI
	representante_____

Reunidos en [lugar], a [día] de [Mes] de [Año]

ANEXOS

Anexo: 1 Licencia de uso de la datos abiertos y encuesta nacional en tecnologías de la información y comunicación

LICENCIA DE USO	
Declaración de uso de Datos Abiertos	
La presente declaración promueve el uso y reutilización de los conjuntos de datos abiertos bajo las siguientes libertades y condiciones:	
I.- Usted es libre de:	a) Hacer, publicar y distribuir copias del conjunto de datos;
	b) Adaptar, remezclar y/o transformar el conjunto de datos;
	c) Extraer total o parcialmente contenido del conjunto de datos;
	d) Crear conjuntos de datos derivados del conjunto de datos o su contenido;
II.- Siempre y cuando cumpla con las siguientes condiciones:	a) Citar la fuente de origen de donde obtuvo el conjunto de datos,
	b) En el caso de copiar, distribuir, remezclar, modificar y crear a partir de un conjunto de datos y sus resultados, se mantengan la mismas libertades y condiciones de la presente Declaración.
Compatible con Creative Commons License (CC BY SA 4.0) y ObdL	

Anexo: 2 Entrevista hacia el comité de Seguridad de Agencia para el Desarrollo de la Sociedad de la Información en Bolivia ADSIB.

Universidad Mayor de San Andrés
Facultad de Humanidades y Ciencias de la Educación
Carrera de Bibliotecología y Ciencias de la Información

Nota: Esta entrevista es parte de la investigación en Seguridad de la Información en la Protección de los Datos Personales en la Firma Digital de la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB) 2017.

La presente entrevista se desarrollara con 10 preguntas que analizara la Seguridad de la Información de la ADSIB, en relación al Personal Administrativo y Clientes o Usuarios. También así, con la seguridad de la información a nivel de Acceso a la Información, Filtración de la Información y Seguridad de la Información en las Operaciones.

También así, se contemplara con 8 preguntas que analizara la protección de los Datos Personales proporcionado por la ADSIB en relación a la Firma Digital, Sociedad de la Información, Personal Administrativo y Clientes o Usuarios.

ENTREVISTA

Hora: ……fecha:……lugar:……

Cargo que Ocupa: ……

SEGURIDAD DE LA INFORMACION

1.- ¿Cuenta la ADSIB con políticas de acceso a la información?

2.- ¿Cree usted que es necesario la regulación de acceso a la información de la ADSIB, para el personal trabajador, también así para los clientes u usuarios?

3.- ¿Cree usted que se puede dejar de poner a disposición de los empleados toda la información suficiente para que puedan desarrollar su trabajo?

4.- ¿Considera usted de que si no se da toda la información de la ADSIB a los empleados estos podrían realizar su trabajo?

5.- ¿Usted idéntica algún el tipo de información que la ADSIB se debería proteger? Y si lo hace mencione las medias ADSIB realiza para protegerla.

6.- ¿La ADSIB cuenta con controles y clasificación de la información? Podría mencionar algunas

7.- ¿La ADSIB cuenta con medidas de seguridad de la información en las operaciones? Podría mencionar algunas

8.- ¿La ADSIB cuenta con alguna medida de protección de la información ante un incidente que atañe la seguridad de la información?

9.- ¿La ADSIB realizo alguna capacitación al personal responsable, administrativo, o también así a los clientes u usuarios en temas de seguridad en el último año?

10.- ¿La entidad ha implementado lineamientos contra modificaciones o pérdida accidental de información?

PROTECCION DE LOS DATOS PERSONALES

1.- ¿La entidad ha implementado lineamientos, normas y/o estándares para proteger la información personal y privada de los ciudadanos que utilicen sus servicios?

2.- ¿Qué importancia tienen los datos personales para la ADSIB en la sociedad de la información?

3.- ¿Qué medidas de protección realiza la ADSIB ante la recogida de datos personales de los clientes, usuarios y personal administrativo?

4.- ¿Cuáles son los datos personales especialmente protegidos por la ADSIB?

5.- ¿La ADSIB conoce o regula los datos obtenidos por terceros de la firma digital y la sociedad de la información?

6.- ¿La ADSIB mantiene controles de protección en la recogida de datos, uso de datos, actualización y su almacenamiento? Podría mencionar algunas

7.- ¿La ADSIB considera que se da protección a los datos personales de las personas en las recientes invenciones y métodos de negocio de la sociedad de la Información en Bolivia?

8.- ¿Conoce usted las normas, leyes nacionales o internacionales relativas a la protección de los datos personales en lo que respecta al tratamiento y uso de las mismas? Podría mencionar algunos

Anexo: 3 Conformación del comité de Seguridad de la Información de la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia

Comité de Calidad, Seguridad de la Información y de Emergencia de la ADSIB
Esta integrado por los siguientes miembros:
Directora o Director Ejecutivo de la ADSIB
Asesor Legal
Jefe de la Unidad de Innovación y Desarrollo
Jefe de la Unidad de Infraestructura de Servicios
Jefe de la Unidad Administrativa Financiera
Jefe de la Unidad de Gestión de Servicios
Profesional en Seguridad de la Información
Profesional en Calidad de los Servicios
Otros designados por la Dirección Ejecutiva

Anexo: 4 Ejemplo de Inventario de Activos

INVENTARIO DE ACTIVOS IDENTIFICADOS								VALORACIÓN DE ACTIVOS						Criticidad	VALORACION FINAL	GESTIÓN	
	Activo	Descripción	Tipo	Ubicación	Unidad Responsable	Responsable	Custodio	Disponibilidad		Integridad		Confidencialidad	Cuantitativo			Fecha de Ingreso	Fecha de Salida
1	Base de datos de proveedores	<descripción>	Datos o Información	Servidor Base de datos 192.168.2.190	SISTEMAS	Jaime	Pedro	MUY ALTO	5	MUY ALTO	5	MUY ALTO	5	5	MUY ALTO	08/30/16	
2	Código fuente de sistemas	<descripción>	Datos o Información	Servidor de versionamiento 192.168.2.192	SISTEMAS	Jaime	Maria	ALTO	4	ALTO	4	MUY ALTO	5	4	ALTO	08/30/16	
3	Sistema de facturación	<descripción>	Software – Aplicaciones informáticas					MUY ALTO	5	BAJO	2	MUY ALTO	5	4	ALTO	08/30/16	
4	Información almacenada en la nu	<descripción>	Datos o Información					ALTO	4	ALTO	4	ALTO	4	4	ALTO	08/30/16	
5	Base de datos de clientes	<descripción>	Datos o Información					ALTO	4	ALTO	4	BAJO	2	3	MEDIO	08/30/16	
6	Sistema de inventario	<descripción>	Software – Aplicaciones informáticas					ALTO	4	MEDIO	3	MEDIO	3	3	MEDIO	08/30/16	
7	Informes internos	<descripción>	Datos o Información					MEDIO	3	ALTO	4	MEDIO	3	3	MEDIO	08/30/16	
8	LAN	<descripción>	Redes de comunicaciones					ALTO	4	BAJO	2	ALTO	4	3	MEDIO	08/30/16	
9	Pagina web	<descripción>	Software – Aplicaciones informáticas					ALTO	4	MUY ALTO	5	MUY BAJO	1	3	MEDIO	08/30/16	
10	Servicio de internet	<descripción>	Servicios					ALTO	4	ALTO	4	MUY BAJO	1	3	MEDIO	08/30/16	
11	Servidor web	<descripción>	Servicios					ALTO	4	BAJO	2	MEDIO	3	3	MEDIO	08/30/16	
12	Computadoras	<descripción>	Hardware – Equipamiento informático					MEDIO	3	MUY BAJO	1	MEDIO	3	2	BAJO	08/30/16	
13	Energía eléctrica	<descripción>	Equipamiento auxiliar					MUY ALTO	5	MUY BAJO	1	MUY BAJO	1	2	BAJO	08/30/16	

Anexo: 5 Política de protección de datos personales de ADSIB

Política de Protección de Datos Personales
1. Introducción
1.1. Descripción general.
Descripción del servicio
Un certificado digital emitido por ADSIB le permite al cliente realizar firmas digitales avanzadas y autenticar su identidad con la validez legal, vincula un documento digital o mensaje electrónico de datos y garantiza la integridad del documento digital o mensaje electrónico con firma digital .La certificación que emite ADSIB, contempla tres destinatarios: cargos públicos, personas jurídicas y personas naturales.
A nivel conceptual, la Firma Digital consiste en un par de claves criptográficas, una pública y otra privada, aplicadas mediante una función matemática a documentos digitales. La clave privada siempre se encuentra en posesión del firmante y es la utilizada para realizar firmas. La pública se divulga y es la utilizada para verificar una firma de otro sujeto.
Todo lo descrito se encuentra validado por la Resolución Administrativa Regulatoria RAR - DJ-RA TL LP 32/2015 emitido por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT), y la ley N° 164, Ley General de Telecomunicaciones y Tecnologías de Información y Comunicaciones y el Decreto Supremo reglamentario N° 1793.
1.2. Identificación y nombre del documento.
Políticas de Protección de Datos La Entidad Certificadora Pública considera que es relevante analizar y considerar la implementación de regulación integral sobre la protección de los datos personales que cursan a través de las TIC's, para otorgar seguridad y protección a la intimidad del usuario que navega en la red.
Nombre El presente documento lleva como título “Contenido mínimo de las políticas de certificación para una entidad certificadora. Políticas de certificación. Apéndice 2. Política de Protección de Datos Personales”. Se constituye en su versión final, sin revisiones.
Versión fecha de elaboración El documento fue elaborado desde el 21 de noviembre hasta el 21 de diciembre del año 2014.
Fecha de actualización A ser acordado una vez se realicen las revisiones necesarias.
Sitio web de consulta. El sitio web de consulta es: www.firmadigital.bo.
2.-Conceptos fundamentales:

a) Archivo o Banco de Datos: indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento físico, electrónico, magnético o informático, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso
b) Autorización: consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales por una Entidad Certificadora Autorizada.
c) Cesión de datos: toda revelación de datos realizada a una persona distinta del titular de los datos.
d) Consentimiento del titular: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual el titular consienta el tratamiento de datos personales que le concierne.
e) Datos personales: toda información de cualquier tipo referida a personas individuales o colectivas determinadas o determinables.
f) Datos sensibles: datos personales que revelen filiación política o filosófica, credo religioso, ideología, afiliación sindical e informaciones referentes a origen racial y étnico, salud u orientación sexual.
g) Destinatario: persona individual o colectiva, pública o privada, que reciba cesión de datos, se trate o no de un tercero.
h) Disociación de datos: todo tratamiento de datos personales de manera que la información obtenida no pueda vincularse a persona determinada o determinable.
i) Encargado del tratamiento: persona individual o colectiva, pública o privada, que sola o en conjunto con otros trate datos personales por cuenta del responsable del archivo o banco de datos o del tratamiento.
j) Tercero: la persona individual o colectiva, pública o privada, distinta del titular del dato, del responsable del archivo o banco de datos o tratamiento, del encargado y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable o del encargado del tratamiento.
k) Responsable del tratamiento: persona individual o colectiva, pública o privada, propietaria del archivo o banco de datos o que decida sobre la finalidad, contenido y uso del tratamiento.
l) Titular de los datos: es la persona natural o jurídica a quien se refiere la información que reposa en un archivo o banco de datos.
m) Tratamiento de datos personales: Es cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.
n) Usuario de datos: toda persona, pública o privada, que realice a su arbitrio el tratamiento de datos, ya sea en un archivo o banco de datos propio o a través de conexión con los mismos.

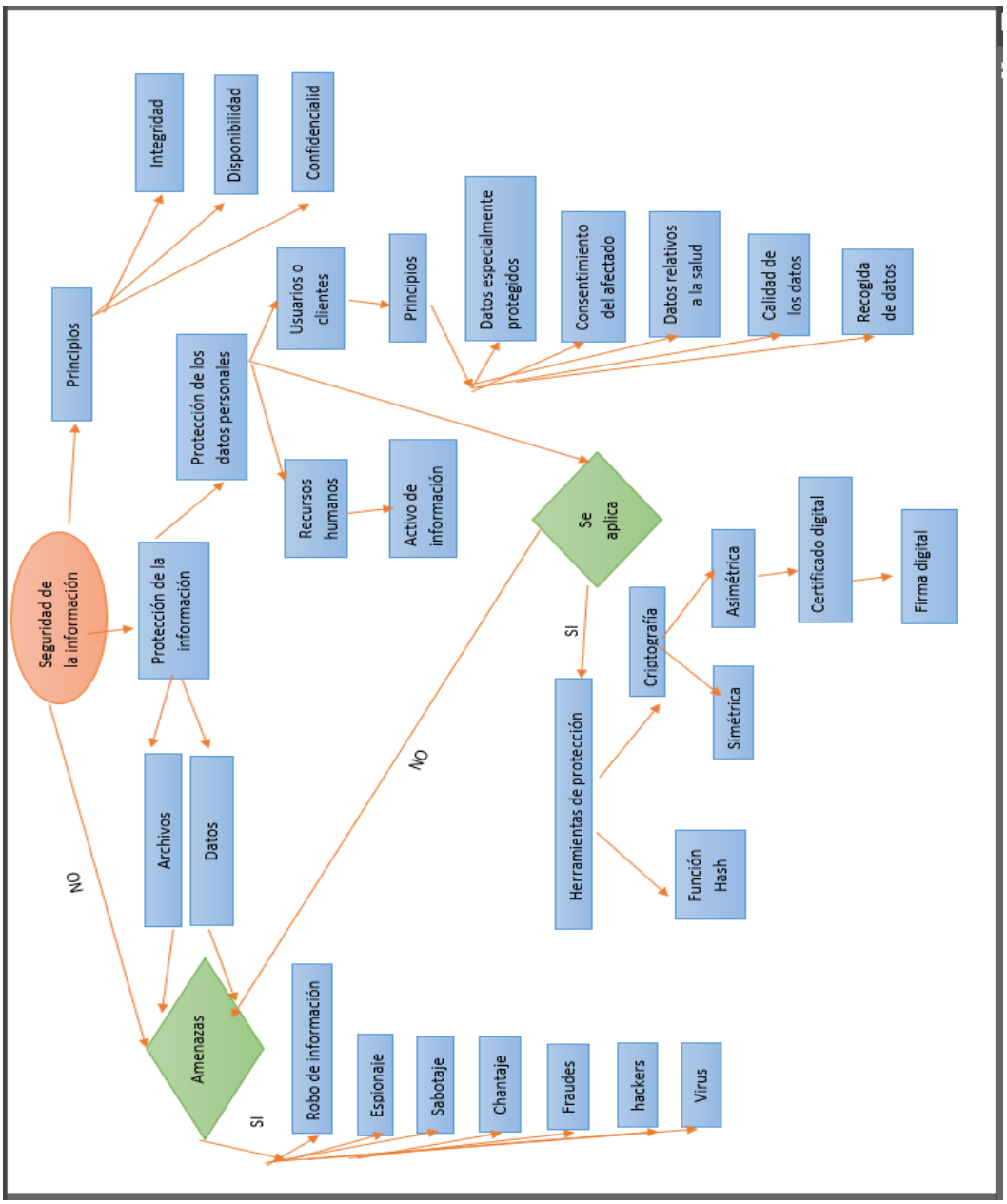
o) Fuentes accesibles al público: aquellos archivos o banco de datos cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación.
p) Firma Digital: Conjunto de datos adjunto o lógicamente asociado a un documento electrónico, que permita verificar su integridad, así como identificar en forma unívoca y vincular jurídicamente al autor con el documento.
q) Protección de datos personales: Toda información concerniente a una persona natural o jurídica que la identifica o la hace identificable.
r) Servicio de certificación digital: Consiste en emitir, revocar y administrar los certificados digitales utilizados para generar firmas digitales.
s) Servicio de registro: Consiste en comprobar y validar la identidad del solicitante de un certificado digital, y otras funciones relacionadas al proceso de expedición y manejo de los certificados digitales.
3.- Principios
Los servicios de certificación digital en cuanto al tratamiento de datos personales, se regirán por los siguientes principios:
Principio de Finalidad.- La utilización y tratamiento de los datos personales por parte de las entidades certificadoras autorizadas, deben obedecer a un propósito legítimo, el cual debe ser de conocimiento previo del titular;
Principio de Veracidad.- La información sujeta a tratamiento debe ser veraz, completa, precisa, actualizada, verificable, inteligible, prohibiéndose el tratamiento de datos incompletos o que induzcan a errores;
Principio de Transparencia.- Se debe garantizar el derecho del titular a obtener de la entidad certificadora autorizada, en cualquier momento y sin impedimento, información relacionada de la existencia de los datos que le conciernan;
Principio de Seguridad.- Se debe implementar los controles técnicos y administrativos que se requieran para preservar la confidencialidad, integridad, disponibilidad, autenticidad, no repudio y confiabilidad de la información, brindando seguridad a los registros, evitando su falsificación, extravío, utilización y acceso no autorizado o fraudulento;
Principio de Confidencialidad.- Todas las personas involucradas y que intervengan en el tratamiento de datos personales, están obligadas a garantizar la reserva de la información, incluso hasta después de finalizado su vínculo con alguna de las actividades que comprende el tratamiento, pudiendo únicamente realizar el suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las tareas autorizadas.
4.- Derechos de los Titulares de Datos
Los titulares de los datos, tendrán los siguientes derechos:
Derecho de información y contenido de la información.

Derecho de conocer los datos registrados.
Derecho de rectificación, actualización, inclusión o eliminación.
Datos sensibles: Ninguna persona puede ser obligada a proporcionar datos sensibles, como ser: ideología, religión, salud, origen racial o étnico y otros. Éstos sólo podrán ser objeto de tratamiento con el consentimiento expreso y escrito del titular y/o cuando medien razones de interés general autorizadas por ley, o cuando la Entidad Certificadora tenga mandato legal para hacerlo.
5.- Marco legal nacional para el tratamiento de los datos personales en materia de telecomunicaciones
La Ley N° 164, Ley General de Telecomunicaciones, Tecnologías de Información Y Comunicación, en su Art. 56 (Inviolabilidad y Secreto de las Telecomunicaciones) señala: "En el marco de lo establecido en la Constitución Política del Estado, los operadores de redes públicas y proveedores de servicios de telecomunicaciones y tecnologías de información y comunicación, deben garantizar la inviolabilidad y secreto de las comunicaciones, al igual que la protección de los datos personales y la intimidad de usuarias o usuarios, salvo los contemplados en guías telefónicas, facturas y otros establecidos por norma".
Por otro lado, el Art. 56 del Decreto Supremo N° 1793 Reglamento para el Desarrollo de Tecnologías de Información y Comunicación, a fin de garantizar los datos personales y la seguridad informática de los mismos, adopta las siguientes previsiones: a) La utilización de los datos personales respetará los derechos fundamentales y garantías establecidas en la Constitución Política del Estado;
b) El tratamiento técnico de datos personales en el sector público y privado en todas sus modalidades, incluyendo entre éstas las actividades de recolección, conservación, procesamiento, bloqueo, cancelación, transferencias, consultas e interconexiones, requerirá del conocimiento previo y el consentimiento expreso del titular, el que será brindado por escrito u otro medio equiparable de acuerdo a las circunstancias. Este consentimiento podrá ser revocado cuando exista causa justificada para ello, pero tal revocatoria no tendrá efecto retroactivo.
c) Las personas a las que se les solicite datos personales deberán ser previamente informadas de que
sus datos serán objeto de tratamiento, de la finalidad de la recolección y registro de éstos; de los potenciales destinatarios de la información; de la identidad y domicilio del responsable del tratamiento o de su representante; y de la posibilidad de ejercitar los derechos de acceso, rectificación, actualización, cancelación, objeción, revocación y otros que fueren pertinentes. Los datos personales objeto de tratamiento no podrán ser utilizados para finalidades distintas de las expresadas al momento de su recolección y registro;
d) Los datos personales objeto de tratamiento sólo podrán ser utilizados, comunicados o transferidos a un tercero, previo consentimiento del titular u orden escrita de autoridad judicial competente;

e) El responsable del tratamiento de los datos personales, tanto del sector público como del privado, deberá adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, tratamiento no autorizado, las que deberán ajustarse de conformidad con el estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural. El Decreto Supremo N° 1391, Reglamento General a la Ley N° 164, Sector de Telecomunicaciones, en el Art. 176 establece:
Artículo 176.- (Protección de los Datos Personales). I. El personal de operadores y proveedores de servicios de telecomunicaciones y tecnologías de información y comunicación, está obligado a guardar secreto de la existencia o contenido de las comunicaciones y a la protección de los datos personales y la intimidad de los usuarios.
II. Los operadores y proveedores de servicios están obligados a adoptar las medidas más idóneas para garantizar, preservar y mantener la confidencialidad y protección de los datos personales de los
usuarios del servicio, salvo en los siguientes casos: a) De existir una orden judicial específica; b) Con consentimiento previo, expreso y por escrito del usuario titular; c) En casos que la información sea necesaria para la emisión de guías telefónicas, facturas, detalle de llamadas al titular acreditado, o para la atención de reclamaciones, provisión de servicios de información y asistencia establecidos por el presente Reglamento, o para el cumplimiento de las obligaciones relacionadas con la interconexión de redes y servicios de apoyo.
III. El operador o proveedor de servicios deberá coadyuvar en la identificación de los presuntos responsables de vulneraciones a la inviolabilidad, secreto de las comunicaciones, protección de los datos personales y la intimidad de los usuarios, que su personal pudiera cometer en las instalaciones del operador o proveedor.
IV. La ATT aprobará los procedimientos y medidas utilizadas por los operadores y proveedores para salvaguardar la inviolabilidad y secreto de las comunicaciones y a la protección de los datos personales y la intimidad de los usuarios.
V. Queda prohibido que los operadores y proveedores de servicios permitan el acceso a registros o bases de datos de sus usuarios, ya sea de manera individual o a través de listas de usuarias, usuarios o números, con fines comerciales o de publicidad, salvo autorización previa, expresa y escrita de la usuaria o usuario que desee recibir dicha publicidad .
Asimismo de conformidad a lo establecido en el artículo 43 inciso i) del D.S 1793, la Entidad Certificadora mantendrá la confidencialidad de la información proporcionada por los titulares de certificados digitales limitando su empleo a las necesidades propias del servicio de certificación, salvo
Orden judicial o solicitud del titular del certificado digital, según sea el caso. Finalmente, el Art. 43 inciso b) del Decreto Supremo N° 1793, Reglamento para el desarrollo de Tecnologías de la Información y Comunicación, de fecha 13 de noviembre de 2013, señala: “Desarrollar y actualizar los procedimientos de servicios de certificación digital, en función a las técnicas y métodos de protección de la información y lineamientos establecidos por la ATT”.

6.- Marco jurídico aplicable
Asimismo, las disposiciones legales y reglamentarias que regulan la protección de datos, son: - Constitución Política del Estado - Ley N° 164, Ley General de Telecomunicaciones, Tecnologías de la Información y Comunicación, de fecha 08 de agosto de 2011. - Decreto Supremo N° 1793, Reglamento para el desarrollo de Tecnologías de la Información y Comunicación, de fecha 13 de noviembre de 2013. - Decreto Supremo N° 1391, Reglamento General a la Ley N° 164, Sector de Telecomunicaciones, de fecha 24 de octubre de 2012. - Decreto Supremo N° 28168, que garantiza el acceso a la información, como derecho fundamental de toda persona y la transparencia en la gestión del Poder Ejecutivo, de fecha 17 de mayo de 2005. - Estándares Técnicos emitidos por la ATT.

Anexo: 6 Ejemplo de flujograma orientado en la seguridad de la información y protección de datos personales.



Anexo: 7 Síntesis legal de seguridad de la información y protección de datos en Bolivia.

Constitución Política del Estado

Capitulo segundo: Principios, valores y Fines del Estado

Art. 9 Inciso 2 Garantizar el bienestar, el desarrollo, la seguridad y la protección e igual dignidad de las personas, las naciones, los pueblos y las comunidades, y fomentar el respeto mutuo y el diálogo intercultural, intercultural y plurilingüe. (Este artículo, presenta la responsabilidad por parte del Estado en garantizar la protección y dignidad de las personas garantizando su bienestar, podemos entender que el Estado realiza primicias en la protección de la dignidad de las personas, en todos los aspectos posibles.)

Capítulo tercero: derechos Civiles y Políticos

Art. 23 I Toda persona tiene derecho a la libertad y seguridad personal. La libertad personal sólo podrá ser restringida en los límites señalados por la ley, para asegurar el descubrimiento de la verdad histórica en la actuación de las instancias jurisdiccionales. (En este artículo se presenta que la constitución resalta el derecho de las personas tanto en temas de libertad, también en el tema de seguridad, asegurando la verdad dentro de la actuación.)

Garantías Jurisdiccionales y Acciones de Defensa, Capítulo Segundo Acciones de Defensa, Sección III Acción de Protección de Privacidad

Art. 130 I. Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad. (Este artículo, ve la importancia de preservar los datos personales, notando que es necesario poner a disposición en cualquier medio en el que se encuentre, recalcando la protección de la intimidad y privacidad de las personas)

Art. 131 I. La Acción de Protección de Privacidad tendrá lugar de acuerdo con el procedimiento previsto para la acción de Amparo Constitucional.

(la constitución, da en necesidad de la protección y privacidad dentro de una acción que tutela las garantías de los particulares establecidas en la constitución, leyes y tratados internacionales, condenando acciones de los agresores, bien sean ciudadanos, organizaciones públicas o privadas.)

Decreto supremo N. 1793 Reglamento para el Desarrollo de Tecnologías de Información y Comunicación

Da a conocer los aspectos más importantes a continuación:

Título I Disposiciones Generales

Art. 4.- (Principios) II. Tratamiento de datos personales: Los servicios de certificación digital en cuanto al tratamiento de datos personales, se regirán por los siguientes principios:

a) Finalidad: La utilización y tratamiento de los datos personales por parte de las entidades certificadoras autorizadas, deben obedecer a un propósito legítimo, el cual debe ser de conocimiento previo del titular;

b) Veracidad: La información sujeta a tratamiento debe ser veraz, completa, precisa, actualizada, verificable, inteligible, prohibiéndose el tratamiento de datos incompletos o que induzcan a errores;

c) Transparencia: Se debe garantizar el derecho del titular a obtener de la entidad certificadora autorizada, en cualquier momento y sin impedimento, información relacionada de la existencia de los datos que le conciernan;

d) Seguridad: Se debe implementar los controles técnicos y administrativos que se requieran para preservar la confidencialidad, integridad, disponibilidad, autenticidad, no repudio y confiabilidad de la información, brindando seguridad a los registros, evitando su falsificación, extravío, utilización y acceso no autorizado o fraudulento;

e) Confidencialidad: Todas las personas involucradas y que intervengan en el tratamiento de datos personales, están obligadas a garantizar la reserva de la información, incluso hasta después de finalizado su vínculo con alguna de las actividades que comprende el tratamiento, pudiendo únicamente realizar el suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las tareas autorizadas.

(En la protección de los datos, se debe identificar la finalidad de la misma, su veracidad de la información, si la misma está completa o cuenta con errores. También así, su transparencia, conforme al derecho del titular o datos con los que se relacionan. Tomando más relevancia al tema de seguridad, que exige que se debe implantar los controles tanto técnicos como administrativos, garantizando la confidencialidad, integridad y disponibilidad de la información y los datos)

Capítulo II Desarrollo de Contenidos y Aplicaciones

Art. 5.- (Desarrollo de Contenidos y Aplicaciones TIC) I. El Estado promoverá de manera prioritaria el desarrollo de contenidos y aplicaciones y servicios de las TIC en software libre, utilizando estándares abiertos y velando por la seguridad de la información en las siguientes áreas:

c) En la gestión gubernamental, a través de la implementación del gobierno electrónico promoviendo la transparencia y la capacitación de los recursos humanos para garantizar la eficiencia de los sistemas implantados.

Art. 6.- (Objetivos del Desarrollo de Contenidos Digitales). El desarrollo, diseño e innovación de contenidos digitales tendrán mínimamente los siguientes objetivos:

d) Promover la identidad cultural de los pueblos originarios, sus territorios ancestrales, usos y costumbres; para el bienestar, el desarrollo, la seguridad y la protección e igual dignidad de las personas, las naciones, los pueblos y las comunidades y fomentar el respeto mutuo y el diálogo intracultural, intercultural y plurilingüe;

m) Fortalecer la seguridad informática del Estado Plurinacional de Bolivia.

Art. 8 (Plan de Contingencia) Las entidades públicas promoverán la seguridad informática para la protección de datos en sus sistemas informáticos, a través de planes de contingencia desarrollados e implementados en cada entidad.

Título IV Certificado y Firma Digital y Entidades Certificadoras

Art. 44.- (Responsabilidad de las Entidades Certificadoras Autorizadas Ante Terceros) I. Las entidades certificadoras autorizadas serán responsables por la emisión de certificados digitales con errores y omisiones que causen perjuicio a sus signatarios.

Art. 46.- (Auditorias) I. Las entidades certificadoras podrán ser sometidas a inspecciones o auditorías técnicas por la ATT.

II. La ATT, podrá implementar el sistema de auditoría, que debe como mínimo evaluar la confiabilidad y calidad de los sistemas utilizados, el cumplimiento de los estándares nacionales e internacionales sobre certificación y firma digital, la integridad, confidencialidad y disponibilidad de los datos, como así también el cumplimiento de las políticas de certificación definidas por la autoridad, su declaración de prácticas de certificación y los planes de seguridad y de contingencia aprobados.

Art. 54.- (Derechos del Titular del Certificado) El titular del certificado digital tiene los siguientes derechos:

b) A la confidencialidad de la información proporcionada a la entidad certificadora.

Capítulo II Tratamiento de los Datos Personales

Art. 56.- (Protección de Datos Personales) A fin de garantizar los datos personales y la seguridad informática de los mismos, se adoptan las siguientes previsiones:

a) La utilización de los datos personales respetará los derechos fundamentales y garantías establecidas en la Constitución Política del Estado;

b) El tratamiento técnico de datos personales en el sector público y privado en todas sus modalidades, incluyendo entre éstas las actividades de recolección, conservación, procesamiento, bloqueo, cancelación, transferencias, consultas e interconexiones, requerirá del conocimiento previo y el consentimiento expreso del titular, el que será brindado por escrito u otro medio equiparable de acuerdo a las circunstancias. Este consentimiento podrá ser revocado cuando exista causa justificada para ello, pero tal revocatoria no tendrá efecto retroactivo;

c) Las personas a las que se les solicite datos personales deberán ser previamente informadas de que sus datos serán objeto de tratamiento, de la finalidad de la recolección y registro de éstos; de los potenciales destinatarios de la información; de la identidad y domicilio del responsable del tratamiento o de su representante; y de la posibilidad de ejercitar los derechos de acceso, rectificación, actualización, cancelación, objeción, revocación y otros que fueren pertinentes. Los

datos personales objeto de tratamiento no podrán ser utilizados para finalidades distintas de las expresadas al momento de su recolección y registro;

d) Los datos personales objeto de tratamiento sólo podrán ser utilizados, comunicados o transferidos a un tercero, previo consentimiento del titular u orden escrita de autoridad judicial competente;

e) El responsable del tratamiento de los datos personales, tanto del sector público como del privado, deberá adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, tratamiento no autorizado, las que deberán ajustarse de conformidad con el estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

Habeas Data

Las características empleadas por el Estado comprenden el derecho a la información, su actualización, corrección o modificación, confidencialidad y exclusión. De forma que, Oporto y Rosso, detallan tal efecto como lo siguiente:

> *Datos registrados por cualquier medio físico, electrónico, magnético, informático, que cursen en archivos o banco de datos públicos o privados (sic) que afecten su derecho su derecho fundamental a la intimidad y privacidad personal y familiar, a su imagen y honra y reputación reconocidos, (pero) no procederá a levantar el secreto en la materia de prensa. (Oporto Ordoñes & Rosso Ramirez, 2007, p. 66)*

La información individual registrada en cualquier medio, almacenada en archivo público o privado, debe proteger la intimidad y privacidad de las personas o su familia. Por lo tanto, es necesario contemplar la aplicación del Habeas Data de manera más específica. Es decir, comprende las siguientes características:

a) Derecho de acceso a la información o registro de datos personales obtenidos y almacenados en un banco de datos de la entidad pública o privada, para conocer qué es lo que se dice respecto a la persona que plantea el habeas data, de manera que pueda verificar si la información y los datos obtenidos y almacenados son los correctos y verídicos; si no afectan las áreas calificadas como sensibles para su honor, la honra y la buena imagen personal;

b) Derecho a la actualización de la información o los datos personales registrados en el banco de datos, añadiendo los datos omitidos o actualizando los datos atrasados; con la finalidad de evitar el uso o distribución de una información inadecuada, incorrecta o imprecisa que podría ocasionar graves daños y perjuicios a la persona;

c) Derecho de corrección o modificación de la información o los datos personales inexactos registrados en el banco de datos público o privado, tiene la finalidad de eliminar los datos falsos que contiene la información, los datos que no se ajustan de manera alguna a la verdad, cuyo uso podría ocasionar graves daños y perjuicios a la persona;

d) Derecho a la confidencialidad de cierta información legalmente obtenida, pero que no debería trascender a terceros porque su difusión podría causar daños y perjuicios a la persona;

e) Derecho de exclusión de la llamada "información sensible" relacionada al ámbito de la intimidad de la persona, es decir, aquellos datos mediante los cuales se pueden determinar aspectos considerados básicos dentro del desarrollo de la personalidad, tales como las ideas religiosas, políticas o gremiales, comportamiento sexual; información que potencialmente podría generar discriminación o que podría romper la privacidad del registrado.