MAESTRÍA EN AUDITORIA DE TECNOLOGÍA DE LA INFORMACIÓN

# PROPUESTA DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN DESDE EL ENFOQUE DE PROTECCIÓN DE DATOS PERSONALES PARA LOS ENTES GUBERNAMENTALES DEL ECUADOR QUE TIENEN IMPLEMENTADO LA ESTRATEGIA DE GOBIERNO EN LÍNEA

**Propuesta de artículo presentado como requisito para la obtención del título:**

## Magíster en Auditoría de Tecnologías de la Información


**Por el estudiante:**

**Angel Ignacio YÁNEZ NAVARRETE**

**Bajo la dirección de:**

**César Martín GONZALES ARBAIZA**



**Universidad Espíritu Santo**

**Maestría en Auditoría de Tecnología de la Información**

**Samborondón - Ecuador**

**Agosto del 2018**

# *Propuesta de controles de seguridad de la información desde el enfoque de protección de datos personales para los entes gubernamentales del Ecuador que tienen implementado la estrategia de gobierno en línea*

Proposal of information security controls from the personal data protection approach for the governmental entities of Ecuador that have implemented the online government strategy

Resumen

En el sector público del Ecuador, el gobierno en línea ha facilitado la tramitología entre la ciudadanía y las entidades del estado, sin embargo, esta interacción puede dejar expuesta la información personal de los ciudadanos a riesgos que atentan contra su privacidad. Para esta investigación se efectuó el entendimiento de los requerimientos de protección de datos personales, se revisó la situación actual de otros países de la región y del Ecuador en materia de protección de datos personales contrastando estos resultados con los problemas comunes de las instituciones públicas del Ecuador sobre el mismo tema, además se elaboró una lista de verificación de cumplimiento de protección de datos personales que fue validada por un grupo de expertos. Este trabajo propone los controles mínimos de seguridad de la información que, las instituciones públicas del Ecuador que tienen implementado el gobierno en línea y las organizaciones privadas (de todos los sectores), deberían poner en práctica para proteger los datos personales de los ciudadanos, que son administrados y procesados en su infraestructura tecnológica. Finalmente, el cuadro de controles propuesto, debería ser considerado para su implementación en el sector privado.

Palabras clave: Gobierno en línea, Controles de Seguridad, Seguridad de la Información, Protección de Datos Personales, Derechos ARCO.

Abstract

In the public sector of Ecuador, the online government has facilitated the paperwork between citizens and state entities, however, this interaction can expose the personal information of citizens to risks that violate their privacy. For this research, an understanding of the requirements for the protection of personal data was made, the current situation of other countries in the region and of Ecuador in the area of protection of personal data was reviewed, contrasting these results with the common problems of the public institutions of Ecuador. On the same subject, a compliance checklist for personal data protection was developed and validated by a group of experts. This work proposes the minimum security controls of the information that the public institutions of Ecuador that have implemented the online government and private organizations (of all sectors), should put into practice to protect the personal data of citizens, which they are managed and processed in their technological infrastructure. Finally, the proposed control chart should be considered for implementation in the private sector.

Key words: Online Government, Security Controls, Information Security, Protection of Personal Data, ARCO Rights.

## INTRODUCCIÓN

En la actualidad, las actividades de negocio de las empresas se desarrollan alrededor de las tecnologías de la información y de la comunicación. Debido a esto, es necesario que la infraestructura tecnológica y los sistemas estén dotados de políticas y medidas de seguridad que aseguren el crecimiento y continuidad del negocio, Bertolín (2008).

Según el documento "Rol de las TIC en la gestión pública y en la planificación para un desarrollo sostenible en América Latina y el Caribe", de los autores Alejandra Naser y Gastón Concha; publicado por la Comisión Económica para América Latina y el Caribe (CEPAL) (2014), el gobierno en línea no se aparta de la administración pública, debido a que en mayor o menor nivel y aunque con restricciones, se aplica en servicios estatales, municipios y demás organizaciones gubernamentales, cuyos cambios importantes se reflejan en la organización, nuevos proyectos y políticas ligadas a estrategias de TIC.

Es precisamente en este esquema que los tres pilares fundamentales de la seguridad de la información como son la confidencialidad, integridad y disponibilidad están expuestos a riesgos.

Frente a estas situaciones, las organizaciones deberán proponer políticas y controles apropiados que promuevan una gestión segura de los procesos del negocio, primando la protección de la información, Álvarez & Fernández (2012).

Precisamente para constituir, poner en práctica y sostener la mejora contínua en un sistema de gestión de seguridad de la información, el Ecuador cuenta con la norma técnica NTE INEN-ISO/IEC 27001, cuyo objeto y campo de aplicación lo define el Servicio Ecuatoriano de Normalización (INEN) (2017), de la siguiente manera:

> *"Esta norma nacional especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información en el contexto de la organización. Esta norma nacional también incluye los requisitos para la apreciación y el tratamiento de los riesgos de seguridad de la información adaptados a las necesidades de la organización. Los requisitos establecidos en esta norma nacional son genéricos y se pretende que sean aplicables a todas las organizaciones, independientemente del tipo, tamaño o naturaleza". (pág. 6)*

El objetivo principal del presente trabajo, es el de proponer controles mínimos de seguridad de la información para que las instituciones públicas del Ecuador que tienen implementado el gobierno en línea puedan proteger los datos personales de sus ciudadanos a quienes prestan sus servicios. En el desarrollo de este trabajo daremos a conocer la situación actual en el Ecuador y algunos países de la región acerca de las leyes y normativas relacionadas sobre los requerimientos de protección de datos personales. En adición expondremos los problemas frecuentes y limitaciones de las instituciones públicas del Ecuador para asegurar la protección de dichos datos y finalmente proponer los controles mínimos útiles para enfrentar dichos problemas y minimizar sus limitaciones.

## MARCO TEÓRICO

### Gobierno en línea

Según la definición de la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC) (2010) del Uruguay, uno de los principales conceptos de gobierno en línea es lograr la mejora en el acceso a la información, trámites y los servicios prestados a la ciudadanía, incrementar la efectividad y competencia de la gestión pública y aumentar sustancialmente la transparencia y la interacción ciudadana mediante la implantación y uso de las tecnologías en las entidades públicas.

La Secretaría Técnica Plan toda una Vida (2018), del Ecuador, nos muestra que el gobierno ecuatoriano mediante Decreto Ejecutivo 149 publicado en el Registro Oficial el 18 de diciembre de 2013, dispone la

implementación del Gobierno Electrónico en la Gestión Pública, basado, entre otros considerandos, en:

> *"Que, de acuerdo a los artículos 52 y 53 de la Constitución de la República, las personas tienen derecho a disponer de bienes y servicios de óptima calidad, a elegirlos con libertad, así como obtener una información precisa y no engañosa sobre su contenido y características, además, es deber de las empresas, instituciones y organismos que prestan servicios públicos, incorporar sistemas de medición de satisfacción de las personas usuarias y consumidoras así como poner en práctica sistemas de atención y reparación". (pág. 1)*

**Información**

Heredero, López-Hermoso, Romo, & Medina (2004), describe que la información es de gran importancia en el desarrollo, trabajo y existencia de las organizaciones públicas o privadas. Además, recomienda tomar en cuenta que, la información no podrá ser valorada como un simple soporte a las funciones y actividades de carácter operativo de las empresas, por el contrario, esta será considerada como un activo principal y de relevante importancia.

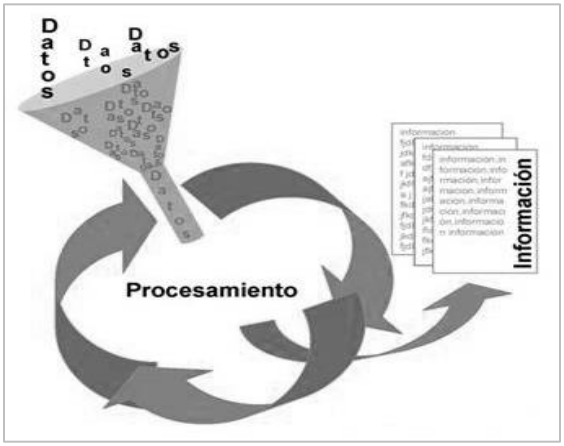


*Figura 1 Proceso sistemático para la gestión de la seguridad de la información*
*Fuente: El portal de ISO 27001 en Español (2012)*

Este mismo autor propone que, a la información, se le implementen metodologías y técnicas tales como: planificación, organización, dirección y control.

**Datos Personales**

Según la Oficina de Planeamiento y Presupuesto (OPP) (2016), del Uruguay, un dato personal es toda clase de información que permita nuestra identificación de manera directa o puede hacernos identificables, y puede ser un nombre, dirección, teléfono, cédula de identidad, RUT, huella digital, ID de socio, ID de estudiante, fotografía o hasta el ADN.

Otro concepto lo define la Universidad Autónoma de Ciudad Juárez (2018), haciendo referencia al Artículo 5º fracción XI de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chihuahua, y Artículo 11º fracción VIII de la Ley de Protección de Datos Personales del Estado de Chihuahua, donde datos personales es todo tipo de información referente a individuos físicos identificados o identificables.

En el mismo tema, el Instituto Tabasqueño de Transparencia y Acceso a la Información Pública (ITAIP) (2013), de México, define que dato personal es la información relativa a una persona que pueda ser empleada para su identificación, ya sea de forma directa o indirecta. Se puede representar en forma de números, letras, imágenes, sonidos, hologramas, entre otros.

Universidad de Guadalajara (2018), en su portal web, muestra la "Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales" elaborada en junio del año 2015 por el Instituto Nacional de transparencia, acceso a la información y protección de datos personales (INAI), de México, que ofrece tres (3) ejemplos de clasificación de los datos personales según su naturaleza:

a) Nivel estándar: Identificación y contacto.

b) Nivel sensible: Ubicación física, patrimonio, autenticación, jurídicos, salud, creencias y opiniones políticas.

c) Nivel especial: Información adicional al número de tarjeta bancaria y titulares de alto riesgo.

**Importancia de los datos personales**

La Superintendencia de Industria y Comercio (SIC) (2018), de Colombia, indica que los datos personales contienen la información indispensable para que se realice la interacción de una persona con otras o con una o más organizaciones y/o instituciones que permite que sea absolutamente particularizada de la sociedad, logrando que se generan flujos de información que favorecen al desarrollo económico y a la mejora de bienes y servicios. Es así que por ejemplo, cuando se realiza una solicitud de crédito a cualquier entidad financiera se llenan formularios con información personal, o al realizar la factura cuando se efectúa una compra se requieren datos tales como el número de documento de identidad, correo electrónico, dirección y teléfono de contacto, entre otros.

Este flujo de información personal tiene muchísimo valor para las organizaciones comerciales y puede generar actividades que el usuario o cliente desconoce; es así que El Comercio (2018), diario de la ciudad de Quito, en su sección Opinión define lo siguiente:

> *"La información personal es poder y vale oro. Su procesamiento y uso puede ser variado y sofisticado en caminos que van desde la publicidad y el espionaje hasta la comisión de delitos. Si una empresa conoce nuestros datos personales, puede leer nuestros gustos, determinar hábitos de consumo y acercarnos publicidad. Y esa publicidad se paga muy bien. El negocio es sencillo: entregamos información a cambio de un servicio. Pero el servicio no es gratis porque se paga con nuestros datos personales." (pág. 1)*

En el mismo orden, la Superintendencia de Comunicación (SUPERCOM) (2015), del Ecuador; cita al Superintendente de la Información y Comunicación, Carlos Ochoa, quien en el Seminario Internacional de Protección de datos personales organizado en la ciudad de Quito por la Función de Transparencia y Control Social (FTCS) junto con el Programa Eursocial expresó que la relevancia de los datos personales radica en que:

> *"Son datos que evidencian quiénes somos personal y profesionalmente, qué consumimos, cuáles son nuestras preferencias. Son, en suma, datos que reflejan nuestra vida. Y estos en manos de personas inescrupulosas se convierten en un peligro no solo para nuestra seguridad sino también para la de nuestras familias". (pág. 1)*

La base de datos de acceso online de gestión e información del Programa Eurosocial conocida como Sistema de Información de Eurosocial (SIA) (2015), en su publicación "Manual de protección de datos personales para el sector público salvadoreño" indica que desde una perspectiva pública como privada, los datos personales se transformaron en un producto de alta valía que podrían ser coleccionados y procesados mediente el uso de la tecnología, cuyo propósito es emplearlos para conseguir diferentes objetivos, muchas veces ilegales.

SIA agrega que debido a estas situaciones, se propuso por primera vez la urgencia de normar y regular jurídicamente la protección de datos personales con el fin de salvaguardar varios derechos fundamentales que estaban siendo objeto de amenaza por la naciente sociedad de la información, especialmente el derecho a la intimidad y la privacidad.

Las leyes expedidas surgieron tambien, además de regular y normar el derecho a la intimidad y la privacidad, para encontrar un equilibrio entre la protección de datos personales y el uso de las TIC en las actividades que realicen las organizaciones públicas o privadas.

Para el Observatorio Iberoamericano de protección de datos (OIPRODAT) (2015), la definición de si los países poseen un nivel óptimo de protección se determina de acuerdo al progreso sobre protección de datos personales en el continente europeo, concretamente a la Directiva 95/46 del Parlamento Europeo y del Consejo, de 24 de octubre de 1995.

En el Ecuador, el 12 de Julio de 2016 la entonces presidenta de la Asamblea Nacional, remitió el proyecto de Ley Orgánica de

Protección de los Derechos de la Intimidad y Privacidad sobre los Datos Personales a la Asamblea, este proyecto, que aún no ha sido aprobado; evidencia que se aplicará a toda clase de base de datos: "ficheros, archivos, en forma física o digital, en instancias públicas o privadas", Intercambio Internacional por la Libertad de Expresión (IFEX, International Freedom of Expression Exchange) (2016).

**El Reglamento General de Protección de Datos (RGPD)**

El Reglamento General de Protección de Datos (RGPD) tiene como objetivo regular el procesamiento de datos personales de los, ciudadanos de la Unión Europea que residen en el Espacio Económico Europeo. (EEA), es decir, Estados miembros de la UE e Islandia, Liechtenstein y Noruega. El GDPR está diseñado para tener un alcance más amplio e incluye otros cambios importantes que tienen en cuenta el panorama actual de ciberseguridad, Trend Micro, (2018).

**Leyes regulatorias para la protección de datos personales**

Luego de la elaboración y discusión, durante 4 años, el Reglamento General de Protección de Datos de la UE (RGPD) finalmente tuvo su aprobación por el Parlamento de la UE el 14 de abril de 2016 , y tal como lo indica European Commission (2018) en su portal web, desde el 25 de mayo de 2018, fecha de vigencia del reglamento; se aplicarán un grupo de reglas de protección de datos para todas las compañías que tiene su centro de operación comercial en la UE, sin depender de su ubicación. European Commission (2018), agrega que, estas reglas tienen como fin que las personas tengan un mayor control sobre sus datos personales y tambien que las compañías gocen de beneficios en condiciones de igualdad.

En la elaboración de leyes para la protección de datos personales, Europa ha sido la mayor influencia en la región latinoamericana, siendo este continente un permanente referente para los países que la conforman, según lo expone la Asociación Española para el Fomento de la Seguridad de la Información (ISMS Forum Spain) (2016) en su artículo técnico "Datos personales en latinoamérica: ¿Dónde estamos?", escrito por Héctor Guzmán Rodríguez.

**ISO 27001**

La Organización Internacional de Normalización (ISO) (2013), define que este estándar fue creado para suministrar los requerimientos con los que se pueda determinar, implantar, conservar y perfeccionar de forma continua un sistema de administración de seguridad de la información. Es una acción estratégica, de toda organización, la adopción de un sistema de gestión de la seguridad de la información.
La ISO, agrega que dicho sistema de gestión de la seguridad de la información salvaguarda la confidencialidad, la integridad y la disponibilidad de la información con la implantación de un procedimiento de gestión de riesgos, otorgando seguridad a los interesados en que se adeministren los riesgos de manera adecuada.

## METODOLOGÍA.

Se utilizó un enfoque cualitativo, que tal como describe Lecanda & Garrido (2003), es "la investigación que produce datos descriptivos considerando: las propias palabras de las personas, habladas o escritas, y la conducta observable". El enfoque de esta metodología "estudia la realidad en su contexto natural, tal y como sucede, intentando sacar sentido de, o interpretar los fenómenos de acuerdo con los significados que tienen para las personas implicadas", Gómez, Flores, & Jiménez (1996).

Lecanda & Garrido (2003) aplica el método de la investigación-acción participativa porque se convierte en un investigador activo, tomando el rol principal al momento de detectar problemas y necesidades, en el levantamiento de información y finalmente en planteamiento de la solución.

Colmenares (2012), nos explica que para el conocimiento claro de la finalidad de estudio, el

punto de partida es el diagnóstico inicial, la pregunta a distintos grupo de interés para conocer su opinión, juicio, puntos de vista, acerca de un tema o dificultad propensa al cambio, lo que nos permite sugerir recomendaciones para este estudio.

El siguiente gráfico muestra los componentes que forman parte de la metodología de investigación del presente trabajo.

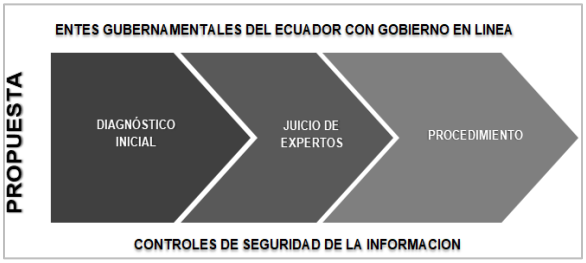


*Figura 2 Metodología Empleada*
*Fuente: Elaboración propia*

**Diagnóstico Inicial**

El diagnóstico inicial está basado de acuerdo a la experiencia profesional que el autor y los ingenieros en sistemas (que aportaron con su juicio de expertos) poseen dentro de las instituciones públicas donde laboran, de la investigación misma en materia de protección de datos personales, la lectura de información bibliográfica de leyes internacionales sobre la protección de datos personales y sobre la situación actual del Ecuador en el tema de la protección de datos personales; es precisamente que tomando como base este ultimo punto se plantea la interrogante de ¿Qué tipo de controles se deben implementar en los entes públicos del Ecuador, que tengan implementado la estrategia de gobierno en línea, para la protección de datos personales?.

**Juicio de expertos**

El juicio de expertos se realizó con base en una lista de verificación de veinticuatro (24) preguntas que permiten valorar cómo se gestiona la protección de datos personales en las instituciones públicas del Ecuador que tengan implementado gobierno en línea.

La elaboración de esta lista de verificación o cuestionario fue realizada considerando la revisión de bibliografía sobre la situación actual de otros países en el tema de protección de datos personales y la forma de evaluar su cumplimiento. Cada pregunta se analizó para relacionarla directamente con el objetivo principal de la investigación y para que, al ser aplicadas, sean de fácil compresión por parte de los entrevistados (expertos). Las preguntas se agruparon en diez (10) criterios de evaluación tomando en cuenta la información indicada en la introducción y marco teórico acerca de la problemática, la necesida de control y las prácticas aplicadas en otros países. *(ver Anexos-Tabla 1 - Instrumento).*

El juicio de expertos fue realizado con la participación de 5 ingenieros en sistemas que presten sus servicios en instituciones públicas del ecuador para que emitan su valoración sobre las preguntas, los mismos que se detallan a continuación:

1. MAE, MGTI. Victor Hugo Rea Sánchez. Director de la carrera de Ingeniería en Sistemas. UNEMI. 14 años de servicio en la institución.
2. M.sc. Rubén Antonio Pacheco Villamar. Especialista de Tecnología, Información y Comunicación 3. Superintendencia de Compañías, Valores y Seguros del Ecuador. 9 años de servicio en la institución.
3. Mg. Eddy Javier Aguilar Cedeño. Especialista de Tecnología, Información y Comunicación 2. Superintendencia de Compañías, Valores y Seguros del Ecuador. 8 años de servicio en la institución.
4. Ing. Katiushka del Rocío Solórzano Rey. Especialista de Tecnología, Información y Comunicación 2. Superintendencia de Compañías, Valores y Seguros del Ecuador. 18 años de servicio en la institución.

5. Ing. Jenny Alexandra Rezabala Pazmiño. Especialista de Tecnología, Información y Comunicación 2. Superintendencia de Compañías, Valores y Seguros del Ecuador. 4 años de servicio en la institución.

**Procedimiento**

Considerando el "Diagnóstico Inicial", contrastándolo con el "Juicio de Expertos", los controles de la norma ISO 27001:2013 y la norma técnica NTE INEN-ISO/IEC 27001, como producto final se propone un listado de controles mínimos de seguridad de la información para la protección de datos personales en los entes gubernamentales del Ecuador que tienen implementado el gobierno en línea. *(ver Anexos-Tabla 4).*

## ANÁLISIS DE RESULTADOS

### Situación de otros países sobre la protección de datos personales

Según lo afirma la Agencia Española de protección de datos (AGPD) (2018), los países que poseen normas concretas para la protección de datos y con autoridades que se encargan por velar por su aplicación, están distribuidos geográficamente de forma heterogénea. El continente Europeo ha llegado a niveles muy altos para la protección de datos y en casi todos los países de Europa pueden hallarse ciertos de estos factores y, con frecuencia, ambos. Otras de las regiones donde la protección de datos o más especificamente la privacidad ha logrado un elevado grado de progreso es América del Norte. En Iberoamérica, el Pacífico y en ciertas países de África, se han originado, en los últimos años, adelantos importantes en legislación e institucionalización sobre la protección de datos.

Esta misma agencia indica que el resultado más importante para que un país sea certificado como adecuado es el de poder transferir datos desde los estados que son miembros de la Unión Europea sin tener que efectuar trámite alguno o autorización exclusiva, los países son los siguientes: Andorra, Argentina, Canadá (Sector privado), Suiza, Islas Feroe, Guernsey, Israel, Isla de Man, Jersey, Nueva Zelanda y Uruguay.

Zamudio (2012) explica que, en lo concerniente al tema regulatorio del derecho a la protección de datos personales, América Latina avanza a ritmo propio. Este ritmo está determinado, a más de otras circunstancias, a que los legisladores, en la mayoría de estos países, poseen un grado de conocimiento medio-regular sobre la temática; tambien los problemas constitucionales en muchos de ellos; y dado que la protección de datos personales no es tema prioritario, en materia política, para sus autoridades.

La Organización de los Estados Americanos (OEA) (2018), muestra, en su portal web; información para consulta de las diferentes normativas que sustentan el derecho de protección de datos en varios de sus paises miembros. Incuye: textos constitucionales, leyes especiales y normativa administrativa, todo categorizado por país y alfabeticamente ordenado. Tambien en el mismo sitio se encuentran adjuntos desarrollos normativos que se han expedido recientemente en distintospaises del continente. Con dicha información se ha elaborado la siguiente tabla: *(ver Anexos-Tabla 2)*

La Asociación Española para el Fomento de la Seguridad de la Información (ISMS Forum Spain) (2016), muestra una tabla en la figura 3, que identifica a los más importantes países latinoamericanos que cuentan con reglamentación de diverso origen o que, en relación a la manera en que han reglamentado la protección de los datos personales, han sostenido una labor de habeas data.

| PROTECCIÓN DE DATOS | 'HABEAS DATA' |
|---|---|
| Argentina | |
| Colombia | |
| Perú | |
| Uruguay | |
| República Dominicana | |
| Chile | Bolivia |
| Costa Rica | Brasil |
| México | Ecuador |
| Nicaragua | Guatemala |
| | Honduras |
| | Panamá |

*Figura 3 Países latinoamericanos con reglamentación de protección de datos personales*
*Fuente: Asociación Española para el Fomento de la Seguridad de la Información (ISMS Forum Spain) (2016)*

En el mismo artículo nos da a conocer que el primer país de latinoamerica en ser distinguido por la Comisión Europea que ofrece un apropiado nivel de protección de datos personales que pueden ser transferidos desde Europa hasta su territorio, es Argentina, avalado por la (Decisión 2003/490/EC). Recién en el año 2012, Uruguay fue reconocido por la Comisión Europea, como país que mantiene un apropiado nivel de protección o su equivalente respecto al procesamiento automatizado de datos personales, mediante la (Decisión 2012/484/UE) concerniente a la protección adecuada de datos personales.

Destaca a Colombia por la Ley Estatutaria 1581, de 17 de octubre de 2012, de la misma manera hace referencia a México, cuya ley es famosa debido a su descripcion y a su campo de ejecución: la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPD), en la actualidad en este país se realiza el trámite para la aprobación de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados que ayudará a cubrir los vacios dejados por la primera ley; y finalmente a Costa Rica que sobresale debido a la manera de regular la protección de datos personales y cuyo Reglamento de la Ley 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales define el concepto del "superusuario", que no es otra cosa que "un perfil de ingreso que cuenta con acceso para consultar la base de datos [inscrita], de forma inmediata, actualizada y sin restricción alguna".

**Situación del Ecuador sobre la protección de datos personales**

Según la Asamblea Nacional (2016), del Ecuador, la propuesta de la Ley Orgánica de Protección de los Derechos de la Intimidad y Privacidad sobre los Datos Personales es en respuesta a los problemas originados por el trato que se da a los datos personales, en una epoca en que su transformación y almacenaje, mediante el uso de las tecnologías evoluciona de manera continua y surge con base en la premisa de que toda persona posee un principio de autonomía, el cual permite establecer una ley regulatoria para administrar y gestionar los datos personales.

Sin embargo a pesar de que en otros paises, este tipo de leyes, ha representado un avance en la materia de protección de datos personales, la Fundación Andina para la Observación y Estudio de Medios (Fundamedios) (2016), expresa que:

> *"Un proyecto de Ley que podría restringir o bloquear contenido en internet y prohibir el acceso a datos personales de ciudadanos públicos, imposibilitando la fiscalización ciudadana podría ser aprobada por el legislativo. Se trata del proyecto de "Ley Orgánica de Protección de los Derechos a la Intimidad y Privacidad de los Datos Personales". (pág. 1)*

La Red Iberoamericana de Protección de Datos (2009), muestra que en el Ecuador, previo a esta ley que ha generado polémica entre diversos actores, existe una constitución y varias legislaciones sectoriales que tratan el tema de la protección de datos personales, las que mostramos a continuación: *(ver Anexos-Tabla 3).*

**Problemas comunes de las instituciones públicas del Ecuador en materia de protección de datos personales**

Ontiveros (2005), en su artículo "Reforma de las Instituciones Públicas en México", define como institución pública al marco de reglamentaciones establecidad de manera formal o informal dentro de una organización, que contiene un conjunto de valores, acuerdos, tradiciones y símbolos, reconocidos por sus integrantes.

Las instituciones públicas del Ecuador, a pesar de contar con reglamentaciones de tipo administrativo, legal, financiero y tecnológicas, no están excentos amenazas y vulnerabilidades en el tema de protección de datos personales, siendo los problemas más comunes:

1) Gobierno de TI
   a) Existen, pero no se cumplen los procedimientos formales para la administración de privilegios de usuario.
   b) No existen o son insuficientes las cláusulas de previsiones cuando se realizan contratos con terceros.
   c) No se evalúan los procedimientos establecidos para monitoreo y/o auditoría.
   d) Incompletos reportes de fallas o son desactualizados.
   e) No existe un procedimiento formal para documentar y supervisar un Sistema de Gestión de Seguridad de Datos Personales (SGSDP).
   f) Existe, pero no se cumple la asignación de responsabilidades respecto a la seguridad de la información (Oficial de Seguridad).
   g) Existen, pero no se cumplen los procedimientos para la instalación y actualización de los sistemas de información desarrollados internamente.
   h) Existen, pero no se cumplen las políticas de uso de correo electrónico.
   i) No se evalúan las bitácoras con registros de actividad en los sistemas de administración u operación.
   j) No existe un proceso previo para categorización de datos personales.
   k) No existen procesos para el tratamiento de datos personales.
   l) No existen o son insuficientes las cláusulas sobre la protección de datos en contratos con empleados.
   m) Existen, pero no se cumplen los procesos en caso de un incidente o vulneración de seguridad.
   n) Existen, pero no se cumplen las políticas para el uso de activos fuera de las entidades.
   o) Existen, pero no se cumplen las políticas o procedimientos sobre seguridad de la información o de protección de datos.
   p) No se evalúan las actividades de monitoreo ante vulneraciones de la seguridad de los datos.
   q) Existen, pero no se cumplen los procedimientos para reportar debilidades en la seguridad.
   r) No existen Planes de Contingencia y de Gestión de Riesgos.
2) Humano
   a) Proceso de reclutamiento inadecuado.
   b) Existen, pero no se cumple la inducción al usuario final sobre políticas de TI.
   c) No existe personal sensibilizado y/o entrenado en Seguridad.
   d) No existe un responsable de seguridad de la información o de protección de datos.
   e) Mal uso de hardware y software.
   f) Incumplimiento de las políticas de TI.
   g) Existen, pero no se cumple el control sobre el trabajo de externos.
3) Infraestructura (Edificio)
   a) Insuficientes controles de acceso.
4) Redes
   a) Contraseñas no cifradas.
   b) Servicios de red habilitados innecesariamente y/o mal uso de ciertos protocolos.
   c) No existe o es escaso el monitoreo de los componentes de las redes, protocolos, servicios y aplicaciones.
   d) Descarga y uso de software no controlado.

e) Insuficientes respaldos información o respaldos con versiones muy antiguas.
f) Existen, pero no se cumplen los registros para la administración de los recursos.
g) Líneas de comunicación sin protección.
h) Cableado de interconexión dañado o antiguo.
i) Arquitectura de red insegura.

5) Hardware**:**
a) Configuraciones inadecuadas en los equipos.
b) Almacenamiento no cifrado .
c) Errores en la destrucción de soportes electrónicos.

6) Software:
a) No existe o faltan pruebas y certificación al software y su configuración antes de su puesta en producción.
b) Insuficientes actualizaciones y parches de seguridad en software.
c) Desuso o reutilización de dispositivos de almacenamiento sin un debido procedimiento para el borrado de información.
d) Incompletos registros de auditoría.
e) Fallos al asignar privilegios de acceso.
f) Interfaces de los sistemas para usuarios internos y externos, complicadas o con mensajes confusos.

CISCO (2008), recomienda que para mitigar la pérdida de datos, las organizaciones deben implantar la seguridad en su entorno cultural empresarial y medir frecuentemente los riesgos de cada interrelacion con las redes, el hardware, el software, datos y, obviamente, otros usuarios.

Como resultado de la necesidad de minimizar los problemas comunes detectados en las instituciones públicas del Ecuador en materia de protección de datos personales, dada la relación con los controles definidos por la norma ISO/IEC 27001/2013 y las preguntas de la lista de verificación indicadas en este paper, se recomienda tomar en cuenta los controles que se indican a continuación para la efectiva protección de datos personales en los entes gubernamentales del ecuador que tienen implementado el gobierno en línea:

1. Políticas de seguridad para datos personales
   1.1. Establecer Políticas para la gestión de datos personales.
   1.2. Revisar y evaluar las políticas.
2. Cumplimiento Legal
   2.1. Identificar y documentar la legislación/regulación aplicable.
   2.2. Prevenir el mal uso de activos.
   2.3. Revisar el cumplimiento técnico.
   2.4. Definir controles de auditoría de sistemas.
3. Estructura organizacional de la seguridad para datos personales
   3.1. Administrar y coordinar la seguridad de la información.
   3.2. Designar deberes en seguridad y protección de datos personales.
4. Clasificación y acceso a los activos
   4.1. Mantener inventario y clasificación de datos personales.
   4.2. Identificar los procesos de datos personales.
5. Seguridad del personal
   5.1. Identificar responsabilidades de seguridad en cada puesto de trabajo.
   5.2. Disponer la firma de un Acuerdo de confidencialidad.
   5.3. Establecer los Términos y condiciones de empleo.
   5.4. Establecer programas de entrenamiento y educación.
   5.5. Establecer proceso disciplinario.
6. Seguridad física y amiental
   6.1. Establecer controles de entrada física.
   6.2. Controlar el trabajo en áreas restringidas.
   6.3. Asegurar los activos fuera de las instalaciones.
   6.4. Aplicar mecanismos de borrado seguro de información.
7. Gestión de comunicaciones y operaciones
   7.1. Establecer controles de cambios operacionales.
   7.2. Segregar y aislar tareas.
   7.3. Separar el área de desarrollo de sistemas de datos personales.

7.4. Establecer estándares de configuración segura y actualizar los sistemas.
7.5. Establecer controles para la protección contra software malicioso.
7.6. Respaldar la información.
7.7. Establecer controles de red.
7.8. Gestionar los soportes informáticos extraíbles.
7.9. Proporcionar mecanismos de seguridad en la gestión del gobierno electrónico.
7.10. Proporcionar seguridad en la Mensajería electrónica.
7.11. Establecer proceso para autorización de divulgación de información de manera pública.
7.12. Establecer técnicas de disociación y separación.

8. Control de acceso
8.1. Establecer reglas de control de acceso
8.2. Gestionar la administración de usuarios y contraseñas.
8.3. Gestionar privilegios de usuario.
8.4. Establecer reglas de uso de servicios de red.
8.5. Asegurar autenticación de usuario para conexiones externas.
8.6. Segregar redes
8.7. Establecer mecanismos de identificación automática de terminales.
8.8. Establecer proceso de inicio de sesión.
8.9. Restringir el acceso a los datos personales.
8.10. Aislar sistemas sensibles.
8.11. Establecer procedimientos de seguridad para el uso de dispositivos móviles internos.
8.12. Establecer procedimientos de seguridad para el uso de dispositivos móviles externos.

9. Desarrollo y mantenimiento de sistemas
9.1. Validar datos de entrada.
9.2. Autenticar mensajes.
9.3. Validar de datos de salida.
9.4. Establecer reglas de Cifrado.
9.5. Establecer procedimientos para Firmas electrónicas.
9.6. Controlar software y sistemas.
9.7. Proteger datos de prueba del sistema.
9.8. Controlar el acceso a software de configuración.

10. Vulneraciones de seguridad de los datos personales
10.1. Establecer procedimientos para el manejo de incidentes.
10.2. Establecer procedimientos de notificación de vulneraciones de seguridad a titulares.

El detalle de estos cincuenta y tres (53) controles se muestra en la sección Anexos – Tabla 4.

**CONCLUSIONES**

De la investigación y el análisis realizado se puede determinar que, en el Ecuador, las instituciones públicas que tienen implementado gobierno en línea no cuentan con una regulación que estipule los controles tecnológicos ni un marco referencial que facilite el establecimiento de medidas de seguridad de información para la protección de los datos personales.

La principal limitación para el presente trabajo de investigación es la ausencia de información sobre protección de datos personales en el Ecuador y de una ley específica sobre dicho tema. Esta limitación también se convierte en una fortaleza porque permite ser pionero en la propuesta de controles para la protección de datos personales.

Dado el riesgo al cual están expuestos los datos personales se ha logrado implementar medidas de control en otros países incluido gran parte de países latinoamericanos, como Argentina, Uruguay, Colombia, Perú y México, y es muy probable que en el Ecuador deba ocurrir en un futuro cercano.

Los controles de protección de datos personales tienen estrecha relación con los controles de seguridad de la información lo que hace imprescindible que las instituciones públicas del Ecuador, que cuenten con gobierno en línea, deben tener implementado los controles de la

norma técnica ecuatoriana NTE INEN-ISO/IEC 27001.

Se ha tomado como referencia esta norma, en virtud que el gobierno del Ecuador mediante la Secretaria Nacional de Administración Pública, con el fin de controlar el crecimiento de las TIC, asegurar la integridad, confidencialidad y disponibilidad de la información que reposa en las instituciones públicas; propuso la ejecución del Esquema Gubernamental de Seguridad de la Información (EGSI) que se basa en la norma NTE INEN ISO/IEC 27001:2011.

Por lo tanto el presente trabajo servirá como punto de partida, para que las instituciones públicas ecuatorianas con gobierno en línea o aquellas que pretendan implementarlo, puedan administrar de manera óptima la seguridad de los datos personales de los ciudadanos al contar con una propuesta de controles basados en la Norma ISO/IEC 27001/2013.

De la misma manera este trabajo servirá como base para investigaciones futuras sobre la protección de datos personales en todas las instituciones públicas del Ecuador, además de las organizaciones privadas de todos los sectores.

Finalmente el cuadro de controles propuesto debería ser considerado para su implementación en el sector privado.

**Referencias Bibliográficas**

Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC). (14 de Junio de 2010). *https://www.agesic.gub.uy*. Recuperado el 03 de Marzo de 2018, de https://www.agesic.gub.uy: https://www.agesic.gub.uy/innovaportal/v/163/1/agesic/gobierno_electronico_.html

Agencia Española de Protección de Datos (AGPD). (2018). *www.agpd.es*. Recuperado el 13 de Marzo de 2018, de www.agpd.es: http://www.agpd.es/portalwebAGPD/internacional/Proteccion_datos_mundo/index-ides-idphp.php

Álvarez, A. A., & Fernández, L. A. (2012). *Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes 2.ª edición.* Madrid: AENOR. ASOCIACION ESPAÑOLA DE NORMALIZACION Y CERTIFICACION.

Asamblea Nacional. (12 de Julio de 2016). *www.asambleanacional.gob.ec.* Recuperado el 14 de Marzo de 2018, de www.asambleanacional.gob.ec: http://www.asambleanacional.gob.ec/sites/default/files/private/asambleanacional/filesasambleanacionalnameuid-29/Leyes%202013-2017/250%20protec-intimidad-grivadeneira-12-07-2016/PP-protec-intimidad-grivadeneira-12-07-2016.pdf

Asociación Española para el Fomento de la Seguridad de la Información (ISMS Forum Spain). (Abril de 2016). *www.ismsforum.es.* Recuperado el 13 de Marzo de 2018, de www.ismsforum.es: http://www.ismsforum.es/ficheros/descargas/segurilatam001blq1456907052.pdf

Bertolín, J. A. (2008). *Seguridad de la información. Redes, informática y sistemas de información.* Madrid, España: Paraninfo.

CISCO. (s.f. de s.f. de 2008). *www.cisco.com.* Recuperado el 11 de Marzo de 2018, de www.cisco.com: https://www.cisco.com/web/offer/em/pdfs_innovators/LATAM/data_mist_sp.pdf

Colmenares, A. M. (30 de Junio de 2012). Investigación-acción participativa: una metodología integradora del conocimiento y la acción. *Voces y Silencios: Revista Latinoamericana de Educación, 3*(1), 115.

Comisión Económica para América Latina y el Caribe (CEPAL). (Enero de 2014). *https://www.cepal.org.* Recuperado el 11 de Marzo de 2018, de https://www.cepal.org: https://repositorio.cepal.org/bitstream/handle/11362/35951/1/S1420470_es.pdf

El Comercio. (2018). *www.elcomercio.com*. Recuperado el 19 de Marzo de 2018, de www.elcomercio.com: http://www.elcomercio.com/opinion/oro-petroleo-datos-personales.html

European Commission. (2018). *www.ec.europa.eu*. Recuperado el 15 de Marzo de 2018, de www.ec.europa.eu: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

Fundación Andina para la Observación y Estudio de Medios (Fundamedios). (30 de Septiembre de 2016). *www.fundamedios.org*. Recuperado el 15 de Marzo de 2018, de www.fundamedios.org: http://www.fundamedios.org/alertas/fundamedios-alerta-sobre-graves-restricciones-la-libertad-de-expresion-en-internet-con-el-proyecto-de-ley-de-datos-personales/

Gómez, G. R., Flores, J. G., & Jiménez, E. G. (1996). *www.utp.edu.co.* Recuperado el 17 de Marzo de 2018, de www.utp.edu.co: http://media.utp.edu.co/centro-gestion-ambiental/archivos/metodologia-de-la-investigacion-cualitativa/investigacioncualitativa.doc.

Heredero, C. d., López-Hermoso, J. J., Romo, S. M., & Medina, S. (2004). *Informática y comunicaciones en la Empresa.* Madrid, Av. de Valdenigrales, s/n 28223 Pozuelo de Alarcón.: ESIC EDITORIAL.

Instituto Tabasqueño de Transparencia y Acceso a la Información Pública (ITAIP). (2013). *www.itaip.org.mx.* Recuperado el 22 de Marzo de 2018, de www.itaip.org.mx: http://www.itaip.org.mx/reusdap/manuales/manual_datos_personales_itaip.pdf

Intercambio Internacional por la Libertad de Expresión (IFEX, International Freedom of Expression Exchange) . (21 de Octubre de 2016). *www.ifex.org*. Recuperado el 18 de Marzo de 2018, de www.ifex.org: https://www.ifex.org/ecuador/2016/10/21/datos_proteccion/es/

Lecanda, R. Q., & Garrido, C. C. (2003). Introducción a la metodología de

investigación cualitativa. *Revista de Psicodidáctica*(14), 39.

Observatorio Iberoamericano de protección de datos (OIPRODAT). (25 de Noviembre de 2015). *ww.oiprodat.com*. Recuperado el 13 de Marzo de 2018, de ww.oiprodat.com: http://oiprodat.com/2015/11/25/no-uniformidad-legislativa-paises-con-legislacion-en-proteccion-de-datos-y-sin-legislacion-especifica/

Oficina de Planeamiento y Presupuesto (OPP). (12 de Septiembre de 2016). *www.opp.gub.uy*. Recuperado el 20 de Marzo de 2018, de www.opp.gub.uy: https://www.opp.gub.uy/images/documentos/1LOSDATOSPERSONALESYSUPROTECCION.pdf

Ontiveros, M. D. (2005). *www.unam.mx.* Recuperado el 19 de Abril de 2018, de www.unam.mx: https://archivos.juridicas.unam.mx/www/bjv/libros/4/1594/15.pdf

Organización de los Estados Americanos (OEA). (2018). *www.oas.org*. Recuperado el 16 de Marzo de 2018, de http://www.oas.org: http://www.oas.org/es/sla/ddi/proteccion_datos_personales_dn.asp

Organización Internacional de Normalización (ISO). (2013). *www.iso.org*. Recuperado el 20 de 03 de 2018, de www.iso.org: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

Red Iberoamericana de Protección de Datos. (2009). *www.redipd.es*. Recuperado el 12 de Marzo de 2018, de www.redipd.es: http://www.redipd.es/legislacion/ecuador-iden-idphp.php

Secretaría Técnica Plan toda una Vida. (20 de Enero de 2018). *https://www.todaunavida.gob.ec/.* Recuperado el 09 de Marzo de 2018, de https://www.todaunavida.gob.ec/: https://www.todaunavida.gob.ec/wp-content/uploads/downloads/2015/04/D.E.-No.-149-Implementaci%C3%B3n-del-Gobierno-Electr%C3%B3nico-en-la-Administraci%C3%B3n-P%C3%BAblica-Central-Insitucional.pdf

Servicio Ecuatoriano de Normalización (INEN). (25 de Enero de 2017). *www.normalizacion.gob.ec.* (INEN, Ed.) Recuperado el 16 de Octubre de 2018, de www.normalizacion.gob.ec: http://181.112.149.204/buzon/normas/nte_inen_iso_iec_27001.pdf

Sistema de Información de Eurosocial (SIA). (Junio de 2015). *www.sia.eurosocial-ii.eu.* Recuperado el 12 de Marzo de 2018, de www.sia.eurosocial-ii.eu: http://sia.eurosocial-ii.eu/files/docs/1434619841-Sintesis%20Proteccion%20de%20datos%20para%20funcionarios%20publicos_Lecturafacil.pdf

Superintendencia de Comunicación (SUPERCOM). (29 de Septiembre de 2015). *www.supercom.gob.ec*. Recuperado el 15 de Marzo de 2018, de www.supercom.gob.ec: http://www.supercom.gob.ec/kw/willachiy-uku/willaykuna/550-proteccion-de-datos-personales-equilibrio-entre-intimidad-y-libertad-de-informacion

Superintendencia de Industria y Comercio (SIC). (2018). *www.sic.gov.co*. Recuperado el 22 de Marzo de 2018, de www.sic.gov.co: http://www.sic.gov.co/sobre-la-proteccion-de-datos-personales

Trend Micro. (2018). *www.trendmicro.com*. Recuperado el 10 de Marzo de 2018, de www.trendmicro.com: https://www.trendmicro.com/vinfo/us/security/definition/eu-general-data-protection-regulation-gdpr

Universidad Autónoma de Ciudad Juárez. (2018). *www.uacj.mx.* Recuperado el 21 de Marzo de 2018, de www.uacj.mx: http://www.uacj.mx/Transparencia/Documents/Carrusel%20Documentos/Conceptos%20b%C3%A1sicos%20de%20Protecci%C3%B3n%20de%20Datos%20Personales%20vf.pdf

Universidad de Guadalajara. (s.f. de s.f. de 2018). *www.udg.mx.* Recuperado el 13 de Marzo de 2018, de www.udg.mx: http://transparencia.udg.mx/sites/default/files/Gu%C3%ADa%20para%20la%20implementaci%C3%B3n%20de%20un%20SGSDP.pdf

Zamudio, M. d. (Diciembre de 2012). *www.habeasdatacolombia.uniandes.edu.co.* Recuperado el 13 de Marzo de 2018, de www.habeasdatacolombia.uniandes.edu.co: https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/ok3_Ma.-de-Lourdes-Zamudio_FINAL.pdf

## ANEXOS

**Tabla 1 - Instrumento**

*Lista de verificación de cumplimiento de protección de datos personales*

| Criterios de evaluación | Descripción | Pregunta(s) asociadas |
|---|---|---|
| 1. Obtención justa de los datos personales | Obtener los datos personales de manera abierta, directa y transparente, así como también darle un uso responsable | 1. ¿Los ciudadanos están al tanto del uso que se da a los datos personales recopilados sobre ellos la Institución? |
| | | 2. ¿Los ciudadanos conocen de cualquier divulgación de sus datos personales a terceros? |
| | | 3. ¿Los ciudadanos han dado su aprobación expresa para cualquier uso de sus datos personales, que no es obvio para ellos? |
| 2. Definición clara del propósito de la recolección de los datos personales | Definir de manera clara el propósito o propósitos por los cuales mantenemos los datos personales | 4. ¿La Institución ha determinado el compromiso de mantener una lista de todos los grupos de datos personales y el fin determinado con cada uno? |
| 3. Uso y divulgación | Definir reglas para el uso y divulgación de la información | 5. ¿La Institución posee prácticas, reglas, políticas o procedimientos definidos sobre el uso y la divulgación de datos personales que son de conocimiento de todos los ciudadanos? |
| 4. Seguridad | Definir reglas de seguridad para los datos personales con sus respectivo responsables | 6. ¿La Institución cuenta con un detalle de prácticas, reglas, políticas o procedimientos de seguridad vigentes para cada grupo de datos personales? |
| | | 7. ¿La Institución cuenta con un responsable del desarrollo y la revisión de estas prácticas, reglas, políticas o procedimientos? |
| | | 8. ¿Son estas prácticas, reglas, políticas o procedimientos apropiados para la confidencialidad de los datos personales que se almacenan dentro de la Institución? |
| | | 9. ¿La institución mantiene sus computadores, servidores, equipos de red, de comunicaciones y bases de datos protegidas con contraseña y encriptadas, de ser el caso? |
| | | 10. ¿La institución mantiene los computadores, servidores, equipos de red, de comunicaciones y archivos bloqueados de forma segura lejos de personas no autorizadas? |
| 5. Recopilación adecuada, relevante y no excesiva de los datos personales | Definir una política para la recopilación de datos personales relevantes y no excesivos. | 11. ¿La institución posee prácticas, reglas, políticas o procedimientos para el caso en que los ciudadanos pidieran justificación sobre toda los datos personales que existe sobre ellos? |
| 6. Precisión y actualización de | Obtener datos personales exactos y actualizados | 12. ¿La institución posee prácticas, reglas, políticas o procedimientos para verificar |

| | | |
|---|---|---|
| los datos personales | | la exactitud de datos personales? |
| 7. Tiempo de retención de los datos personales | Determinar política para la retención y eliminación de los datos personales | 13. ¿La Institución posee una declaración clara sobre cuánto tiempo se deben almacenar los datos personales? |
| | | 14. ¿La Institución libera con regularidad las bases de datos de información innecesaria, como datos relacionados con proveedores anteriores o ciudadanos? |
| | | 15. ¿La Institución cuenta con una política de eliminación de datos personales tan pronto como se haya completado el propósito para el que se obtuvieron? |
| 8. Derecho al acceso de los datos personales | Definir procedimiento y responsable para el acceso a los datos personales. | 16. ¿La Institución cuenta con un funcionario designado como responsable de atender las solicitudes de acceso a los datos personales? |
| | | 17. ¿La Institución cuenta con procedimientos claros para procesar dichas solicitudes? |
| | | 18. ¿Dichos procedimientos garantizan el cumplimiento de los requisitos de la Ley? |
| 9. Entrenamiento y educación sobre protección de datos personales | Establecer planes de capacitación sobre protección de datos personales | 19. ¿Se conocen, en la Institución, los niveles de entendimiento de la protección de datos personales? |
| | | 20. ¿Conocen los ciudadanos las responsabilidades de protección de datos personales, incluida la necesidad de confidencialidad? |
| | | 21. ¿La protección de datos personales está incluida como parte del programa de capacitación para los ciudadanos de la Institución? |
| 10. Coordinación y cumplimiento de la protección de datos personales | Definir personal con roles para coordinación y cumplimiento de protección de datos personales | 22. ¿La Institución ha designado al coordinador de protección de datos personales y la persona de cumplimiento? |
| | | 23. ¿Todos los ciudadanos están al tanto de su rol? |
| | | 24. ¿La Institución cuenta con mecanismos establecidos para la revisión formal por parte del coordinador de actividades de protección de datos personales? |

*Fuente: Elaboración propia*

**Tabla 2**

*Desarrollo normativo sobre protección de datos personales en algunos países de América del Sur*

| País | Desarrollo Normativo por País |
|---|---|
| Argentina | **Constitución de la Nación Argentina** (Ver artículos 43 y 86), Ley de Protección de Datos Personales, Reglamento General de Acceso a la Información Pública, Régimen de libre acceso a la información pública ambiental. |
| Colombia | **Constitución Política de Colombia** (Ver artículo 15), Ley Estatutaria 1581 de 2012, Ley Estatutaria 1266 de 2008. Habeas Data, Código Contencioso Administrativo, Ley 58 de 1982, Ley 57 de 1985, Ley 80 de 1993, Ley 136 de 1994, Ley 962 de 2005, Compilación de leyes varias, Decreto 886 de 2014, Decreto 1377 de 2013, Decreto 4886 de 2011, Decreto 1151 de 2008, Ley 1266 Habeas Data, Proyecto de Ley Estatutaria 156 de 2011 SENADO. |
| Perú | **Constitución Política del Perú** (Ver artículos 2, 11, 161 y 162), Ley de Transparencia y Acceso a la Información Pública, Ley de Protección de datos personales, Ley Nº 27309, de 17 de julio de 2000, Código Procesal Constitucional, Decreto Supremo Nº 003-2013-JUS, de 21 de marzo de 2013, Decreto Supremo Nº 072-2003-PCM, de 7 de agosto de 2003, Resolución Ministerial 111-2009 MTC/03, de 6 de febrero de 2009, Proyecto de Ley Nº 1269/2011 para la Gestión de Intereses en la Administración Pública, Proyecto de Ley Nº 1260/2011. |
| Uruguay | **Constitución de la República Oriental del Uruguay** (Ver artículo 10), Ley 18.381. Derecho de Acceso a la Información Pública, Ley Nº 18.220. Sistema Nacional de Archivos, Ley Nº 18.331. Protección de datos personales y acción de "Habeas Data". Ley N° 17.823, de 7 de septiembre de 2004. Código de la Niñez y la Adolescencia. (Arts. 218, 219, 221 y 222), Ley 19.030 Aprueba el Convenio N° 108 del Consejo de Europa, Decreto N° 664/008, de 22 de diciembre de 2008. |
| Chile | **Constitución Política de la República de Chile** de 1980 (Ver artículo 19), Ley de Transparencia de la Función Pública y de Acceso a la Información de la Administración del Estado, Ley de Protección de datos de carácter personal, Proyecto de Ley que Modifica la ley N° 19.628, sobre Protección de la Vida Privada y Protección de Datos de Carácter Personal. |

*Fuente: Elaboración propia*

**Tabla 3**

*Artículos y legislaciones sectoriales, en el Ecuador, sobre la protección de datos personales*

<table>
<tr><th>Constitución</th><th>Ley</th></tr>
<tr><td rowspan="2">Artículo 11.<br>Número 9: “Determina que el más alto deber del Estado consiste en respetar y hacer respetar los derechos garantizados en la Constitución.”</td><td>Ley Nº 162, de 31 de marzo de 2010, del Sistema Nacional de Registro de Datos Públicos.</td></tr>
<tr><td rowspan="4">Ley Nº 13, de 18 de octubre de 2005, de Burós de Información Crediticia (arts. 5 a 10).</td></tr>
<tr><td rowspan="3">Artículo 66.<br>Número 19: “El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección”.<br>“Número 20: “El derecho a la intimidad personal y familiar.”<br>Número 21: ”El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual”</td></tr>
<tr><td>Ley Nº67, de 17 de abril de 2002 de Comercio Electrónico, Firmas y Mensajes de Datos (Artículo 9).</td></tr>
<tr><td>Ley Orgánica de Transparencia y Acceso a la Información Pública, de 18 de mayo de 2004.</td></tr>
<tr><td rowspan="3">Artículo 92.<br>"Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes”</td><td>Ley Nº 184, de 10 de agosto de 1992 Especial de Telecomunicaciones (Arts. 1, 14 y 39).</td></tr>
<tr><td>Ley Nº 13, de 18 de octubre de 2005. Burós de Información Crediticia (Arts. 5 a 10).</td></tr>
<tr><td>Ley Orgánica de Transparencia y Acceso a la Información (LOTAIP), de 18 de mayo de 2004.</td></tr>
</table>

*Fuente: Elaboración propia*

**Tabla 4**

*Cuadro de controles mínimos propuestos para la protección de datos personales categorizados por cada dominio*

| N° | Control Propuesto | Descripción | Referencia control ISO 27001:2013 | Pregunta para Cumplimiento de Protección de Datos Personales |
|---|---|---|---|---|
| **Dominio 1: Políticas de seguridad para datos personales** | | | | |
| 1 | 1.1. Establecer políticas para la gestión de datos personales | Establecer políticas revisadas y aprobadas por la Máxima autoridad de la Institución. | 5.1.1. Conjunto de políticas para la seguridad de la información | 5,11,15 |
| 2 | 1.2. Revisar y evaluar las políticas | Revisar y evaluar las políticas para la protección de datos personales con el objetivo de medir su efectividad y cumplimiento de forma periódica. | 5.1.2 Revisión de las políticas para la seguridad de la información<br>18.2.1 Revisión independiente de la seguridad de la información<br>18.2.2 Cumplimiento de las políticas y normas de seguridad.<br>18.2.3 Comprobación del cumplimiento. | 7 |
| **Dominio 2: Cumplimiento legal** | | | | |
| 3 | 2.1. Identificar y documentar la legislación o regulación aplicable | Identificar y documentar los deberes y obligaciones de toda la Institución para cumplir con los requerimientos legales y contractuales acerca de la protección de datos personales. | 18.1.1 Identificación de la legislación aplicable<br>18.1.2 Derechos de propiedad intelectual (DPI)<br>18.1.3 Protección de los registros de la organización<br>18.1.4 Protección de datos y privacidad de la información personal | 12 |

| | | | | |
|---|---|---|---|---|
| 4 | 2.2. Prevenir el mal uso de activos | Establecer mecanismos contra el uso de activos para propósitos no autorizados. | 8.1.2 Propiedad de los activos 8.1.3 Uso aceptable de los activos | 9,10 |
| **N°** | **Control Propuesto** | **Descripción** | **Referencia control ISO 27001:2013** | **Pregunta para Cumplimiento de Protección de Datos Personales** |
| 5 | 2.3. Revisar el cumplimiento técnico | Revisar los activos y sus controles de seguridad. | 8.1.3 Uso aceptable de los activos | 9,10 |
| 6 | 2.4. Definir controles de auditoría de sistemas | Establecer un proceso para la revisión y evaluación del funcionamiento de los controles de protección de datos personales. | 12.7.1 Controles de auditoría de los sistemas de información | 24 |
| **Dominio 3: Estructura organizacional de la seguridad para datos personales** | | | | |
| 7 | 3.1. Administrar y coordinar la seguridad de la información | Definir objetivos claros tomando en cuenta las iniciativas generadas dentro del equipo de trabajo. Establecer una comunicación efectiva entre las diferentes áreas de la institución para la implementación de controles de seguridad. | 6.1.1 Asignación de responsabilidades para la seguridad. de la información | 6,7,13 |
| 8 | 3.2. Designar deberes en seguridad y protección de datos personales | Designar deberes y obligaciones dirigidas a los individuos que intervengan en el uso y protección de datos personales. | 6.1.2 Segregación de tareas | 7,16 |
| **Dominio 4: Clasificación y acceso a los activos** | | | | |
| 9 | 4.1. Mantener inventario y clasificación de datos personales | Mantener un registro de los datos personales recolectados y tratados por la Institución en cualquier soporte físico o electrónico. | 8.2.1 Directrices de clasificación 8.2.2 Etiquetado y manipulado de la información | 4 |

| N° | Control Propuesto | Descripción | Referencia control ISO 27001:2013 | Pregunta para Cumplimiento de Protección de Datos Personales |
|---|---|---|---|---|
| 10 | 4.2. Identificar los procesos de datos personales | Identificar el ciclo de vida de los datos personales en cada uno de sus procesos, desde la obtención, almacenamiento, procesamiento, cancelación o cualquiera que sea su tratamiento. | 8.1.1. Inventario de activos<br>8.2.1 Directrices de clasificación<br>8.2.2 Etiquetado y manipulado de la información<br>8.2.3 Manipulación de activos<br>8.3.1 Gestión de soportes extraíbles<br>8.3.2 Eliminación de soportes<br>8.3.3 Soportes físicos en tránsito. | 13 |
| **Dominio 5: Seguridad del personal** | | | | |
| 11 | 5.1. Identificar responsabilidades de seguridad en cada puesto de trabajo | Establecer y dar a conocer a cada, función, rol o puesto las responsabilidades que corresponden respecto a la seguridad y protección de datos personales, informando en su caso de las sanciones de incumplimiento de la política de seguridad. | 7.2.1 Responsabilidades de gestión | 19,20,22 |
| 12 | 5.2. Disponer la firma de un Acuerdo de confidencialidad | Firmar un acuerdo de confidencialidad o no revelación de información por los nuevos empleados. | 7.1.2 Términos y condiciones de contratación | 1,2,3 |
| 13 | 5.3. Establecer los Términos y condiciones de empleo | Informar ampliamente dentro de los términos de contratación a los nuevos empleados sobre la seguridad de la información y protección de datos personales, y presentar un aviso de privacidad al personal interno del cual recabaremos datos personales de distintos tipos. | 7.1.2 Términos y condiciones de contratación | 1,2,3,21 |

| | | | | |
|---|---|---|---|---|
| **N°** | **Control Propuesto** | **Descripción** | **Referencia control ISO 27001:2013** | **Pregunta para Cumplimiento de Protección de Datos Personales** |
| 14 | 5.4. Establecer programas de entrenamiento y educación | Concientizar y entrenar apropiadamente a los nuevos empleados, contrataciones externas y usuarios en general, respecto a la seguridad de la información y protección de datos personales. | 7.2.2 Concienciación, educación y capacitación en seguridad de la información | 21 |
| 15 | 5.5. Establecer proceso disciplinario | Establecer un proceso disciplinario en la Institución para aquellos que no cumplan la política o procedimientos. | 7.2.3 Proceso disciplinario | 24 |
| **Dominio 6: Seguridad física y ambiental** | | | | |
| 16 | 6.1. Establecer controles de entrada física | Implementar mecanismos que sólo permitan el acceso a personal autorizado. | 11.1.2 Controles físicos de entrada | 9,10 |
| 17 | 6.2. Controlar el trabajo en áreas restringidas | Determinar que los activos de información sólo deben ser accesibles por personal que los requiera por sus labores en la Institución o bien por un tercero autorizado. | 11.1.3 Seguridad de oficinas, despachos y recursos | 9,10 |
| 18 | 6.3. Asegurar los activos fuera de las instalaciones | Establecer mecanismos autorizados por la Máxima Autoridad, para controlar la salida fuera de las instalaciones de cualquier activo que contenga datos personales. | 8.3.3 Soportes físicos en tránsito<br>11.2.5 Salida de activos fuera de las dependencias de la empresa<br>11.2.6 Seguridad de los equipos y activos fuera de las instalaciones | 5,6,7,8 |
| **N°** | **Control Propuesto** | **Descripción** | **Referencia control ISO 27001:2013** | **Pregunta para Cumplimiento de Protección de Datos Personales** |
| 19 | 6.4. Aplicar mecanismos de borrado seguro de | Aplicar técnicas de borrado seguro o de destrucción adecuado cuando se elimine un activo como equipo de | 8.3.2 Eliminación de soportes | 15 |

| | | | | |
|---|---|---|---|---|
| | información | procesamiento, soporte físico o electrónico.<br>Cualquier eliminación de activos debe registrarse con fines de auditoría. | 11.2.7<br>Reutilización o retirada segura de dispositivos de almacenamiento | |
| **Dominio 7: Gestión de comunicaciones y operaciones** | | | | |
| 20 | 7.1. Establecer controles de cambios operacionales | Establecer un procedimiento para documentar y evaluar cualquier cambio que pueda afectar las operaciones relacionadas con datos personales. | 12.1.1<br>Documentación de procedimientos de operación<br>12.1.2<br>Gestión de cambios | 16 |
| 21 | 7.2. Segregar y aislar tareas | Se deberá segregar y aislar los puestos y responsabilidades del personal que realice tratamiento de datos personales, con el fin de reducir las oportunidades de un uso indebido de los activos. | 6.1.1<br>Asignación de responsabilidades para la seguridad de la información<br>6.1.2<br>Segregación de tareas<br>16.1.1<br>Responsabilidades y procedimientos | 19,22,23 |
| 22 | 7.3. Separar el área de desarrollo de sistemas de datos personales | Aislar las instalaciones de desarrollo y /o pruebas de las áreas operacionales. | 12.1.4<br>Separación de entornos de desarrollo, prueba y producción<br>13.1.3<br>Segregación de redes<br>14.2.6<br>Seguridad en entornos de desarrollo | 6 |
| **N°** | **Control Propuesto** | **Descripción** | **Referencia control ISO 27001:2013** | **Pregunta para Cumplimiento de Protección de Datos Personales** |
| 23 | 7.4. Establecer estándares de configuración segura y actualizar los sistemas | Identificar las necesidades de nuevos sistemas, actualizaciones o nuevas versiones. Se deben realizar pruebas antes de implementar cualquiera de ellos.<br>Verificar que los sistemas que soportan el tratamiento de datos personales cuentan con configuraciones seguras en el hardware, sistema operativo, base de datos y aplicaciones. | 14.2.1<br>Política de desarrollo seguro de software.<br>14.2.2<br>Procedimientos de control de cambios en los sistemas.<br>14.2.3 | 6 |

| | | | | |
|---|---|---|---|---|
| | | | Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo<br>14.2.8<br>Pruebas de funcionalidad durante el desarrollo de los sistemas<br>14.2.9<br>Pruebas de aceptación | |
| 24 | 7.5. Establecer controles para la protección contra software malicioso | Establecer diferentes controles respecto al software malicioso:<br>Prohibir el uso de software ilegal y/o no autorizado.<br>Difundir (campañas, boletines) sencillos para advertir del software malicioso.<br>Mantener en los dispositivos de procesamiento de información como computadoras, las respectivas herramientas actualizadas que las protejan contra software malicioso.<br>Monitorear el tráfico y las actividades de red para descubrir cualquier comportamiento anómalo, tales como virus, descargas de contenido inapropiado, fugas de información, etc. | 12.2.1<br>Controles contra el código malicioso<br>12.6.2<br>Restricciones en la instalación de software<br>13.1.1<br>Controles de red.<br>13.1.2<br>Mecanismos de seguridad asociados a servicios en red | 6 |
| **N°** | **Control Propuesto** | **Descripción** | **Referencia control ISO 27001:2013** | **Pregunta para Cumplimiento de Protección de Datos Personales** |
| 25 | 7.6. Respaldar la información | Establecer respaldos de datos personales, manteniendo un adecuado control sobre la periodicidad de generación de respaldos y el respectivo almacenaje de los soportes físicos/electrónicos, especialmente para el ejercicio de derechos ARCO.<br>Identificar el proceso a realizar en caso de que sea necesario restaurar un respaldo, asimismo, se deben probar los respaldos periódicamente para asegurar su correcto funcionamiento | 12.3.1<br>Copias de seguridad de la información | 6 |
| 26 | 7.7. Establecer controles de red | Separar los segmentos de red y administración de recursos de red.<br>Definir procedimientos y responsabilidades para el manejo de conexiones remotas.<br>Implementar controles especiales para salvaguardar la confidencialidad e integridad de las comunicaciones sobre | 13.1.3<br>Segregación de redes.<br>14.1.2<br>Seguridad de las comunicaciones en servicios accesibles por | 6,7 |

| | | | | |
|---|---|---|---|---|
| | | redes públicas (por ejemplo, redes privadas virtuales, métodos de cifrado, etc.) | redes públicas<br>14.1.3<br>Protección de las transacciones por redes telemáticas | |
| 27 | 7.8. Gestionar los soportes informáticos extraíbles | Establecer políticas y procedimientos para el uso de soportes informáticos extraíbles como memorias USB, discos, cintas magnéticas, etc. | 8.3.1<br>Gestión de soportes extraíbles.<br>8.3.2<br>Eliminación de soportes.<br>8.3.3<br>Soportes físicos en tránsito. | 6,7 |
| **N°** | **Control Propuesto** | **Descripción** | **Referencia control ISO 27001:2013** | **Pregunta para Cumplimiento de Protección de Datos Personales** |
| 28 | 7.9. Proporcionar mecanismos de seguridad en la gestión del gobierno electrónico | Disponer de mecanismos contra toda actividad fraudulenta, disputas contractuales o revelación/modificación de información.<br>Establecer en entornos web mecanismos de autorización y autenticación para las transacciones.<br>Revisar las cláusulas de intercambio de datos personales y seguridad en los acuerdos establecidos entre las partes involucradas. | 9.2.4<br>Gestión de información confidencial de autenticación de usuarios<br>9.2.5<br>Revisión de los derechos de acceso de los usuarios<br>9.3.1<br>Uso de información confidencial para la autenticación | 6,9,10 |
| 29 | 7.10. Proporcionar seguridad en la Mensajería electrónica | Hacer uso adecuado del correo electrónico, mensajería instantánea y redes sociales, utilizando técnicas o mecanismos que permitan bloquear la recepción de archivos potencialmente peligrosos, mensajes no deseados, no solicitados o de remitente desconocido. | 13.1.2<br>Mecanismos de seguridad asociados a servicios en red<br>13.2.3<br>Mensajería electrónica | 6,7,8,9,10 |
| 30 | 7.11. Establecer proceso para autorización de divulgación de información de | Establecer un proceso de autorización formal para hacer pública información, por cualquier medio de difusión. | 13.2.1<br>Políticas y procedimientos de intercambio de | 1,2,6,8 |

| | | | | |
|---|---|---|---|---|
| | manera pública | | información<br>13.2.2<br>Acuerdos de intercambio | |
| 31 | 7.12. Establecer técnicas de disociación y separación | Establecer técnicas o mecanismos para aislar los datos de manera que por sí mismos no aporten información valiosa.<br>Separar los activos de información grandes en activos de información más pequeños. | 8.2.1<br>Directrices de clasificación.<br>8.2.2<br>Etiquetado y manipulado de la información. | 6,8 |
| **N°** | **Control Propuesto** | **Descripción** | **Referencia control ISO 27001:2013** | **Pregunta para Cumplimiento de Protección de Datos Personales** |
| **Dominio 8: Control de Acceso** | | | | |
| 32 | 8.1. Establecer reglas de control de acceso | Establecer reglas y privilegios para cada usuario o grupo de usuarios conforme a sus responsabilidades. | 9.1.1<br>Política de control de accesos<br>9.1.2<br>Control de acceso a las redes y servicios asociados | 6 |
| 33 | 8.2. Gestionar la administración de usuarios y contraseñas | Asignar a cada usuario un identificador único en el sistema al cuál se vincularán sus privilegios y acceso.<br>Cada usuario deberá ser responsable de guardar en secreto la(s) contraseña(s) y/o mecanismos correspondientes para su acceso, deben existir guías o recomendaciones para la creación y mantenimiento de contraseñas seguras.<br>Establecer procedimientos para la administración de usuarios (altas, bajas y modificaciones) en los sistemas de información.<br>Definir controles respecto a las contraseñas entregadas a los funcionarios, ciudadanos, proveedores, prestadores de servicios o cualquier usuario del sistema de datos personales. | 9.2.1<br>Gestión de altas/bajas en el registro de usuarios<br>9.2.2<br>Gestión de los derechos de acceso asignados a usuarios<br>9.3.1<br>Uso de información confidencial para la autenticación<br>9.4.3<br>Gestión de contraseñas de usuario<br>10.1.1<br>Política de uso de los controles criptográficos<br>10.1.2<br>Gestión de claves | 6,7,8,9,10,20 |
| 34 | 8.3. Gestionar privilegios de usuario | Conceder privilegios a cada usuario o grupo de usuarios, en ambiente multiusuario, en función de sus roles y | 9.2.2<br>Gestión de los derechos | 6,9,10,20 |

| | | | | |
|---|---|---|---|---|
| | | responsabilidades para el cumplimiento de sus tareas. | de acceso asignados a usuarios<br>9.2.3<br>Gestión de los derechos de acceso con privilegios especiales | |
| **N°** | **Control Propuesto** | **Descripción** | **Referencia control ISO 27001:2013** | **Pregunta para Cumplimiento de Protección de Datos Personales** |
| 35 | 8.4. Establecer reglas de uso de servicios de red | Establecer reglas respecto al acceso autorizado a las redes y servicios disponibles así como los procedimientos de uso y conexión. | 9.1.2<br>Control de acceso a las redes y servicios asociados.<br>13.1.1<br>Controles de red<br>13.1.2<br>Mecanismos de seguridad asociados a servicios en red | 6 |
| 36 | 8.5. Asegurar autenticación de usuario para conexiones externas | Establecer mecanismos para asegurar las conexiones que se hagan a través de redes externas a la institución, por ejemplo, cifrado, protocolos de autenticación por desafío mutuo, etc. | 9.1.2<br>Control de acceso a las redes y servicios asociados.<br>14.1.2<br>Seguridad de las comunicaciones en servicios accesibles por redes<br>públicas<br>14.1.3<br>Protección de las transacciones por redes telemáticas | 6 |
| 37 | 8.6. Segregar redes | Segregar a los usuarios de red mediante mecanismos como VPN o firewalls. | 9.1.2<br>Control de acceso a las redes y servicios asociados.<br>13.1.1<br>Controles de red.<br>13.1.2<br>Mecanismos de | 6 |

| | | | | |
|---|---|---|---|---|
| | | | seguridad asociados a servicios en red<br>13.1.3<br>Segregación de redes | |
| 38 | 8.7. Establecer mecanismos de identificación automática de terminales | Establecer un mecanismo de red interna para autenticar cualquier tipo de conexión. | 9.1.2<br>Control de acceso a las redes y servicios asociados.<br>10.1.1<br>Política de uso de los controles criptográficos.<br>10.1.2<br>Gestión de claves<br>13.1.1<br>Controles de red | 6,9,10 |
| **N°** | **Control Propuesto** | **Descripción** | **Referencia control ISO 27001:2013** | **Pregunta para Cumplimiento de Protección de Datos Personales** |
| 39 | 8.8. Establecer proceso de inicio de sesión | Definir que únicamente se debe tener acceso a los sistemas de datos personales a través de un inicio de sesión seguro. | 9.1.2<br>Control de acceso a las redes y servicios asociados.<br>9.4.2<br>Procedimientos seguros de inicio de sesión | 9,10 |
| 40 | 8.9. Restringir el acceso a los datos personales | Definir el acceso a los datos personales a través del personal o aplicaciones en consistencia con la política de seguridad de los datos personales. | 9.4.1<br>Restricción del acceso a la información | 6,7,8,9,10 |
| 41 | 8.10. Aislar sistemas sensibles | Evaluar los sistemas y activos que por su naturaleza deban desarrollarse en ambientes aislados. | 8.1.1<br>Inventario de activos<br>8.1.2<br>Propiedad de los activos<br>12.1.4<br>Separación de entornos de desarrollo, prueba y producción<br>13.1.3<br>Segregación de redes<br>14.2.6<br>Seguridad en entornos de desarrollo | 6,7,8,9,10 |

| | | | | |
|---|---|---|---|---|
| 42 | 8.11. Establecer procedimientos de seguridad para el uso de dispositivos móviles internos | Considerar el trabajo externo a través de dispositivos móviles asignados a los usuarios por la institución, incluyendo capacitación sobre la responsabilidad y medidas de seguridad relacionadas a su uso y las consecuencias de su pérdida.<br>Limitar y ajustar el uso de dispositivos móviles a las condiciones de seguridad y protección de datos de la institución, previamente autorizadas por la Máxima Autoridad. | 8.1.3<br>Uso aceptable de los activos.<br>8.3.1<br>Gestión<br>de soportes extraíbles | 6,7,8, 21 |
| **N°** | **Control Propuesto** | **Descripción** | **Referencia control ISO 27001:2013** | **Pregunta para Cumplimiento de Protección de Datos Personales** |
| 43 | 8.12. Establecer procedimientos de seguridad para el uso de dispositivos móviles externos | Definir mecanismos para la incorporación de dispositivos personales ingresados por los usuarios al entorno de la institución, así como para el tratamiento de datos a través de dichos dispositivos. Limitar y ajustar el uso de dispositivos móviles a las condiciones de seguridad y protección de datos de la institución, previamente autorizadas por la Máxima Autoridad. | 6.2.1<br>Política de uso de dispositivos para movilidad.<br>6.2.1<br>Política de uso de dispositivos para movilidad.<br>8.1.3<br>Uso aceptable de los activos.<br>8.3.1<br>Gestión de soportes extraíbles.<br>8.3.3<br>Soportes físicos en tránsito.<br>11.2.5<br>Salida de activos fuera de las dependencias de la empresa.<br>11.2.6<br>Seguridad de los equipos y activos fuera de las instalaciones. | 6,7,8 |
| **Dominio 9: Desarrollo y mantenimiento de sistemas** | | | | |
| 44 | 9.1. Validar datos de entrada | Validar que los datos proporcionados a un sistema, sean ingresados de forma correcta, para que no se produzcan conflictos de tratamiento posteriores. | 14.1.1<br>Análisis y especificación de los requisitos de | 12 |

| | | | | |
|---|---|---|---|---|
| | | Asegurar, en el caso de aplicaciones, que los métodos de entrada sean seguros y no produzcan vulnerabilidades. | seguridad<br>14.2.1<br>Política de desarrollo seguro de software<br>14.2.5<br>Uso de principios de ingeniería en protección de sistemas<br>14.2.6<br>Seguridad en entornos de desarrollo<br>14.2.8<br>Pruebas de funcionalidad durante el desarrollo de los sistemas<br>14.2.9<br>Pruebas de aceptación<br>14.3.1<br>Protección de los datos utilizados en pruebas | |
| **N°** | **Control Propuesto** | **Descripción** | **Referencia control ISO 27001:2013** | **Pregunta para Cumplimiento de Protección de Datos Personales** |
| 45 | 9.2. Autenticar mensajes | Establecer mecanismos de autenticación de mensajes, en los sistemas de información, para asegurar que un mensaje proviene de una fuente autorizada o que no está corrompido. | 12.4.1<br>Registro y gestión de eventos de actividad<br>12.4.3<br>Registros de actividad del administrador y operador del sistema | 12 |
| 46 | 9.3. Validar de datos de salida | Asegurar que los datos entregados, en las aplicaciones, sean los esperados y que se proporcionen en las circunstancias adecuadas. | 14.2.8<br>Pruebas de funcionalidad durante el desarrollo de los sistemas<br>14.2.9<br>Pruebas de aceptación<br>14.3.1<br>Protección de los datos utilizados en pruebas | 12 |
| 47 | 9.4. Establecer reglas de Cifrado | Establecer reglas que definan el uso de cifrado en comunicaciones y/o almacenamiento, así como de los | 10.1.1<br>Política de uso de los | 6,7,8,9,10 |

| | | | | |
|---|---|---|---|---|
| | | controles y tipos de cifrado a implementar.<br>Identificar la sensibilidad de los datos y el nivel de protección necesario para aplicar el cifrado correspondiente, en almacenamiento y/o transferencia de información. | controles criptográficos | |
| **N°** | **Control Propuesto** | **Descripción** | **Referencia control ISO 27001:2013** | **Pregunta para Cumplimiento de Protección de Datos Personales** |
| 48 | 9.5. Establecer procedimientos para Firmas electrónicas | Utilizar firmas electrónicas o digitales para ayudar a la autenticidad e integridad de documentos electrónicos. | 10.1.1<br>Política de uso de los controles criptográficos | 6,7,8,9,10 |
| 49 | 9.6. Controlar software y sistemas | Establecer controles y procesos para integrar software al ambiente operacional, con el objetivo de minimizar el riesgo de corrupción de datos.<br>Probar cualquier cambio o actualización de sistemas críticos antes de su implementación en la institución.<br>Aplicar los cambios a una copia concreta del software original evaluando su funcionamiento. | 12.1.4<br>Separación de entornos de desarrollo, prueba y producción<br>14.1.1<br>Análisis y especificación de los requisitos de seguridad<br>14.2.1<br>Política de desarrollo seguro de software<br>14.2.2<br>Procedimientos de control de cambios en los sistemas<br>14.2.3<br>Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo<br>14.2.6<br>Seguridad en entornos de desarrollo<br>14.2.8<br>Pruebas de funcionalidad durante el desarrollo de los sistemas<br>14.2.9<br>Pruebas de aceptación | 6 |
| 50 | 9.7. Proteger datos de | Vigilar y gestionar los datos que se utilicen en las pruebas, | 14.3.1 | 6 |

| | | | | |
|---|---|---|---|---|
| | prueba del sistema | evitando el uso de bases de datos con datos personales, si se necesitan usar datos personales, se deben desligar de su titular antes de usarlos. | Protección de los datos utilizados en pruebas | |
| 51 | 9.8. Controlar el acceso a software de configuración | Restringir el acceso a los usuarios no especializados a las carpetas que almacenan la configuración de las aplicaciones o sistemas (librerías), con el fin de prevenir corrupción en los archivos o software. | 9.1.1 Política de control de accesos<br>9.1.2 Control de acceso a las redes y servicios asociados<br>9.4.4 Uso de herramientas de administración de sistemas<br>9.4.5 Control de acceso al código fuente de los programas<br>12.4.2 Protección de los registros de información<br>12.4.3 Registros de actividad del administrador y operador del sistema<br>13.1.1 Controles de red<br>13.1.2 Mecanismos de seguridad asociados a servicios en red | 6,7,8,9,10 |
| **N°** | **Control Propuesto** | **Descripción** | **Referencia control ISO 27001:2013** | **Pregunta para Cumplimiento de Protección de Datos Personales** |
| **Dominio 10: Vulneraciones de seguridad de los datos personales** | | | | |
| 52 | 10.1 Establecer procedimientos para el manejo de incidentes | Establecer procedimientos para el manejo de incidentes, esperando una respuesta pronta y efectiva, llevando a cabo un registro para diferenciarlos y efectuar posteriores revisiones y comparaciones | 16.1.1 Responsabilidades y procedimientos<br>16.1.4 Valoración de eventos de seguridad de la información y toma de | 6,7,8 |

| | | | | |
|---|---|---|---|---|
| | | | decisiones<br>16.1.6 Aprendizaje de los incidentes | |
| 53 | 10.2 Establecer procedimientos de notificación de vulneraciones de seguridad a titulares | Establecer procedimientos relacionados a la notificación de vulneraciones a los titulares cuando éstas afecten sus derechos patrimoniales o morales. | 16.1.2 Notificación de los eventos de seguridad de la información<br>16.1.3 Notificación de puntos débiles de la seguridad<br>16.1.5 Respuesta a los incidentes de seguridad | 6,8 |

*Fuente: Elaboración propia*