OFICINA DE POSGRADOS

Tema:

DISEÑO DE HERRAMIENTAS METODOLÓGICAS PARA IMPLEMENTAR LA SEGURIDAD DE DATOS PERSONALES EN LA EMPRESA FENIX CORP

Proyecto de investigación y desarrollo previo a la obtención del título de Magister en Ciberseguridad

Línea de Investigación:

Seguridad de la Información

Autora:

Ing. Angela Karina Bustillos Mallitasig

Director:

Jaime Gabriel Llumiquinga Veintimilla, Mg.

Ambato – Ecuador

Octubre 2022

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE AMBATO

HOJA DE APROBACIÓN

Tema:

DISEÑO DE HERRAMIENTAS METODOLÓGICAS PARA IMPLEMENTAR LA SEGURIDAD DE DATOS PERSONALES EN LA EMPRESA FENIXCORP

Línea de Investigación:

Seguridad de la Información

Autora:

Angela Karina Bustillos Mallitasig

Gabriel Llumiquinga Veintimilla, Mg. f._____

CALIFICADOR

Verónica Maribel Pailiacho Mena, Mg. f._____

CALIFICADOR

Liliana del Rocío Mena Hernández, Mg. f._____

CALIFICADOR

Padre Juan Carlos Acosta, PhD. f._____

COORDINADOR DE LA OFICINA DE POSGRADOS

Hugo Rogelio Altamirano Villarroel, Dr. f._____

SECRETARIO GENERAL PUCESA

Pontificia Universidad Católica del Ecuador
DIRECCIÓN CENTRO DE POSGRADOS
Sede Ambato

Pontificia Universidad Católica del Ecuador
SECRETARÍA GENERAL
PROCURADURÍA

Ambato – Ecuador

Octubre 2022

Pontificia Universidad Católica del Ecuador
BIBLIOTECA

DECLARACIÓN DE AUTENCIDAD Y RESPONSABILIDAD

Yo: **ANGELA KARINA BUSTILLOS MALLITASIG**, con CC. **050252662-7**, autora del trabajo de graduación intitulado: **"DISEÑO DE HERRAMIENTAS METODOLÓGICAS PARA IMPLEMENTAR LA SEGURIDAD DE DATOS PERSONALES EN LA EMPRESA FENIX CORP",** previa a la obtención del título profesional de **MAGISTER EN CIBERSEGURIDAD**, en la **OFICINA DE POSGRADOS.**

1.- Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través de sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de Universidad.

Ambato, octubre 2022



ANGELA KARINA BUSTILLOS MALLITASIG

CC. 050252662-7

DEDICATORIA

Este trabajo de titulación está dedicado a toda mi familia que son mi fortaleza para cada día alcanzar mis sueños y apoyar en los suyos.

A mis padres “Angel y Mercedes”, por creer en mí siempre por ser el pilar fundamental en mi vida, brindándome su apoyo incondicional para concluir satisfactoriamente uno más de mis propósitos.

A mi hermano Alejo quien me dio ánimos de continuar y no rendirme jamás, sin su apoyo él logro de mi carrera profesional no hubiese sido posible.

Y finalmente, a mi abuelita sé que desde el cielo es la mamita más feliz del mundo siempre me demostró ese orgullo inigualable que sentía por mí y cada uno de sus nietos y aquí estoy nuevamente alcanzando una meta más.

Angela Karina Bustillos

AGRADECIMIENTO

Al concluir esta etapa de mi vida, quiero agradecer a DIOS y a mis padres por haberme permitido estar en ese mundo, por ser mi fortaleza en los momentos de debilidad y por brindarnos una vida llena de aprendizaje.

A mi Tutor Mg. Gabriel LLumiquinga quien con su experiencia ha sido la guía idónea en este proceso, quien me ha brindado el tiempo necesario, paciencia y comprensión para culminar con éxito lo anhelado.

Así, también, un agradecimiento rotundo por estar siempre ahí a mis amigos, compañeros de estudios, mis docentes y a toda mi familia quienes de una u otra manera me apoyaron para culminar mi meta.

Angela Karina Bustillos

RESUMEN

En la actualidad la información es el activo más importante dentro de las organizaciones, en el que requieren de un análisis para protegerla de cualquier riesgo a la que está expuesta. Siendo así los activos que se protege con mayor precaución son los datos personales donde abarca la información para identificar a una persona física de forma directa o indirecta, especialmente por un número de identificación, datos de localización, uno o más factores referidos específicamente a su identidad física, fisiológica, genética, mental, económica, cultural o social. El objetivo del presente proyecto es diseñar herramientas metodológicas para la seguridad de datos personales, de tal manera la metodología utilizada es el ciclo de mejora continua P.D.C.A. (Planear, Hacer, Chequear y Actuar), que está constituida por 4 fases, donde se logre un nivel de madurez aceptable para minimizar los riesgos frente al tratamiento de la información personal. A su vez para garantizar la privacidad de los datos personales se toma medidas y controles de seguridad basadas en normas ISO 27001, 27002 y 27701. los mismos que se trabaja con resultados de análisis de riesgos, evaluación de impacto en los que se considera las particularidades del tratamiento, partes involucradas, el tipo y volumen de datos personales, para lograr reducir los riesgos y proteger sus datos personales.

Palabras claves: riesgo, datos personales, evaluación impacto.

ABSTRACT

Nowadays, information is the most important asset within organizations because it requires an analysis to protect it from any exposed risk. Thus, the assets that we must protect with greater caution is personal data which includes information to identify a natural person directly or indirectly especially by an identification number, location data, one or more factors specifically referring to their physical, physiological, genetic, mental, economic, cultural, or social identity. The objective of this research is to design methodological tools for the security of personal data through the use is the Continuous Improvement Cycle P.D.C.A. (Plan, Do, Check and Act) which has 4 phases, where an acceptable level of maturity is achieved to minimize the risks in the treatment of personal information. In this sense, to guarantee the privacy of personal data, security measures and controls are taken based on ISO 27001, 27002 and 27701 standards, which work with the risk analysis results and the impact evaluation where the particularities of treatment are considered between the parties involved, as well as the type and volume of personal data, in order to reduce risks and protect the personal data.

Keywords: risk, personal data, impact assessment.

INDICE

PRELIMINARES
DECLARACIÓN DE AUTENCIDAD Y RESPONSABILIDAD iii
DEDICATORIA.....iv
AGRADECIMIENTO.....v
RESUMEN vi
ABSTRACT vii
INDICE viii
INTRODUCCION 1
CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA..... 5
1.1. PRIVACIDAD 6
1.2. DATOS PERSONALES..... 8
1.3. PROTECCIÓN DE DATOS PERSONALES 11
1.4. ISO/IEC 27701:2019 13
1.5. LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES 17
CAPITULO II. DISEÑO METODOLÓGICO 20
2.1. CARACTERIZACIÓN DE LA INSTITUCIÓN 20
2.2. METODOLOGÍA DE INVESTIGACIÓN..... 21
2.3. TIPOS DE INVESTIGACIÓN..... 22
METODOLOGÍA DE DESARROLLO 24
CAPÍTULO III. ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN..... 45
3.2. CASOS DE USO Y ENFOQUE DEL INFORME..... 45
3.3. ESTABLECER KPI DE MEDIDAS DE SEGURIDAD..... 85
CONCLUSIONES..... 95
RECOMENDACIONES 96
BIBLIOGRAFÍA 97
ANEXOS 100

INTRODUCCION

La importancia de los crecientes cambios tecnológicos y las amenazas a las que están expuestos los datos personales conducen a la necesidad de una seguridad de la información que ayude a proteger los datos personales mediante la aplicación de estándares de seguridad que permitan analizar los riesgos y vulnerabilidades a los que están expuestos.

La seguridad de la información es un tema que, cada día, adquiere mayor relevancia a nivel mundial. Las amenazas, tanto externas como internas, se incrementan y diversifican sus patrones y frecuencias de ataques, esto genera, un aumento en el porcentaje de fuga de información. (Espinosa, 2017)

Para una mejor confidencialidad, han dado lugar a normas más estrictas destinadas a supervisar el tratamiento de la información personal con el fin de garantizar la confidencialidad y el derecho de toda persona a decidir sobre sus datos personales. Son considerados datos personales: cedula de identidad, teléfono, edad, dirección personal o laboral, educación, cargo, entre otros.

La protección de datos personales es una actividad fundamental para garantizar el respeto de los derechos humanos en cada jurisdicción donde opera la empresa. En este sentido, existe un firme compromiso de dar un tratamiento legal a los datos personales y aplicar las medidas necesarias para demostrar un manejo responsable de los mismos.

Hay cierta información importante que, se mantiene confidencial. Si un extraño pregunta el nombre, lo más probable es que se lo comparta. Ahora, si una persona desconocida solicita la cuenta bancaria, lo más probable es que no lo haga. La privacidad de datos funciona de la misma manera. Si los datos son importantes, se considera datos privados.

Cualquier persona que tenga acceso a la información se apropia de la identidad; por lo tanto, se considera mantener la privacidad de los datos personales básicos

y categorías especiales de datos para proteger la identidad. El robo de identidad es el uso liberado de la información para obtener beneficios financieros entre otros.

La confidencialidad, integridad y disponibilidad de los datos personales están protegidas por medidas de seguridad técnicas, administrativas u organizativas razonables y apropiadas contra el procesamiento no autorizado o ilegal, incluido el acceso, la pérdida, la destrucción, el daño o la divulgación, incluso si es ilegal o inesperado.

Los responsables y encargados de datos toman e implementan medidas, técnicas organizativas apropiadas y efectivas para asegurar y demostrar que el tratamiento se realiza de acuerdo con los principios de datos personales. Estas medidas son revisadas y actualizadas periódicamente. Los responsables o encargados y sus representantes (cuando corresponda) cooperen con las autoridades de protección de datos personales para llevar a cabo sus tareas según sea necesario.

El término “Datos Personales” abarca la información que identifica de manera razonable para identificar a una persona física de forma directa o indirecta, especialmente por referencia a un número de identificación, datos de localización, un identificador en línea o a uno o más factores referidos específicamente a su identidad física, fisiológica, genética, mental, económica, cultural o social. Incluye información expresada en forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica, electrónica, visual o de cualquier otro tipo.

El término “Tratamiento de Datos” se usa en un sentido amplio y abarca toda operación o conjunto de operaciones realizado con Datos Personales, se incluye, de manera enunciativa más no limitativa, la recopilación, acceso, organización, adaptación, indexación, aprovechamiento, registro, almacenamiento, alteración, recuperación, divulgación o transferencia.

El Comercio en su edición digital del 30 de julio de 2021 publica: La protección de datos, tras la pandemia, no solo deja de ser importante sino es un asunto prioritario. Ahora todo es a través del mundo digital: teletrabajo, teleeducación, el comercio

electrónico entre otros, todas las interrelaciones sociales usan la tecnología; en este contexto y con las experiencias recientes de entidades públicas afectadas por filtraciones de información o ciberataques es vital afianzar esa estrategia en el menor tiempo posible. (*La protección de datos de las empresas y de los usuarios - El Comercio*, 2021)

Así también la Ley Orgánica de Protección de Datos Personales, publicada en el Quinto Suplemento del Registro Oficial No.459 de fecha 26 de mayo de 2021; aprobada en Ecuador, obliga a las empresas y organizaciones a cambiar los procesos y prácticas internas que conciban los datos personales como un elemento importante dentro de sus actividades y áreas de trabajo, mediante la implementación de políticas y procesos internos, se estructura adecuadamente la documentación y contratos, se capacita al personal, con el uso de herramientas que permitan un control adecuado de la trazabilidad de los datos.

Para minimizar los riesgos y para evitar daños se trabaja con el estándar ISO 27701:2019 Privacidad de la Información que se refiere a técnicas de seguridad, esta normativa es la extensión de ISO/IEC 27001:2013 e ISO/IEC 27002:2013 para la gestión de privacidad de la información. La ISO/IEC 27701:2019, detalla los requisitos y brinda orientación necesaria para el establecimiento, mediante la implementación, mantenimiento y mejora de un Sistema de Gestión de Privacidad de la Información (SGPI).

Con todo lo expuesto el problema planteado como pregunta es: ¿Cómo mejorar la seguridad de los datos personales en la empresa Fenix Corp? para garantizar la privacidad de los datos personales, se toma medidas y controles de seguridad los mismos que se trabaja con resultados del análisis de riesgos y una evaluación de impacto en los que se considera las particularidades del tratamiento, partes involucradas, el tipo y volumen de datos personales.

Con el fin de garantizar y mejorar la seguridad del tratamiento de datos personales, el responsable o el encargado del tratamiento de datos personales, según el sector

de actividad, se realiza un proceso la verificación, evaluación continua, la eficiencia y eficacia de las medidas técnicas organizativas.

Según lo expuesto la idea a defender es: Con el diseño de herramientas metodológicas se facilita la implementación de la seguridad de datos personales en la empresa Fenix Corp.

El principal objetivo del proyecto es diseñar herramientas metodológicas que permitan mejorar la seguridad de los datos personales en Fenix Corp; con la aplicabilidad de los siguientes objetivos específicos.

1. Documentar los artículos científicos enfocados en la seguridad de datos personales existentes en el estado del arte actual.
2. Diagnosticar la situación actual de la seguridad de datos personales en la empresa Fenix Corp.
3. Aplicar las herramientas diseñadas para la seguridad de datos personales.
4. Compilar los datos obtenidos en las herramientas metodológicas de seguridad de datos personales.

Para cumplir con lo expuesto, se diseña herramientas metodológicas para implementar la seguridad de datos personales, de esa forma organizaciones y personas físicas mejoraran la seguridad de sus datos.

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

En este capítulo, se analizan los conceptos relacionados a la protección de los datos personales, los principales fundamentos, sus componentes, los términos y los diferentes mecanismos de prevención, corrección en seguridad de los datos y metodologías de seguridad.

La protección de datos personales, como un derecho fundamental autónomo del derecho a la vida privada, ha tenido un desarrollo asimétrico en los diferentes sistemas de derechos humanos. A pesar de la rápida evolución de la tecnología, la globalización de la economía y la digitalización de las relaciones humanas, aún no hay un nivel común de protección de datos en el mundo. (Maqueo Ramírez, 2017).

El Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) han traído una nueva regulación en materia de protección de datos que pretende dar respuesta a los constantes avances tecnológicos y las nuevas formas de éstos de transgredir la protección de datos.(Roca, 2020)

En el artículo titulado “El derecho a la protección de datos personales, tecnologías digitales y pandemia por COVID-19 en Colombia”; (Gómez Córdoba, 2020) menciona que la pandemia de COVID-19 ha generado impactos sociales y políticos adicionales más allá de los estrictamente relacionados con la salud, en el contexto de estados de emergencia declarados, limitar temporalmente algunos derechos y libertades civiles con el fin de preservar la vida y la salud de sus ciudadanos.

En las investigaciones analizadas, se identifica que la transformación digital y el uso de herramientas tecnológicas exponen los datos personales para diferentes fines, que ocasiona daños en la integridad de las personas; de manera que los diferentes países desarrollan leyes de protección de datos que garanticen el derecho fundamental a la “privacidad” de las personas.

1.1. Privacidad

La privacidad es entendida como un requisito previo fundamental para la verificación efectiva de los procesos de participación ciudadana en los diferentes países. Por lo tanto, se considera como un límite a la defensa de todas personas, el exceso de datos es utilizados por terceros para divulgación de dicha información que causa perjuicio a las personas.

En palabras de Claypoole y Payton, en su libro Privacy in the Age of Big Data el término de privacidad, tan complejo como personal, es similar a círculos concéntricos. Estos autores consideran que toda persona está en el centro y, alrededor de ella, existen muy cercanamente otros círculos compuestos por una serie de variables, como sus secretos, pensamientos, rituales y demás asuntos propios que “no comparte con nadie”.(Payton & Claypoole, 2015)

Otro autor, como Víctor Drummond, resume el concepto de privacidad de una manera por demás simple, como “la cómoda distancia que una persona mantiene, espontáneamente, entre su más profunda individualidad y el exterior” tomado de (Meraz Espinoza, 2018a)

El término privacidad aplica en todo tipo de actividad, de las personas como entes particulares y a nivel colectivo, como en las tareas que se desempeñan en una corporación. Legalmente, tanto en un caso como en el otro, se tiene como objetivo el preservar los derechos de las personas que, en un actuar individual o colectivo, se vulneren. (Meraz Espinoza, 2018b, p. 3)

Sin embargo, el tema de la privacidad es subjetivo porque es principalmente un tema que involucra percepción, valores, ética y otros temas personales.

La cuestión de la privacidad y la protección de datos personales se ha convertido en una referencia imprescindible en el ámbito empresarial. En vista del abundante procesamiento de todo tipo de información, recae una gran responsabilidad de salvaguardar todo tipo de documentos. La tecnología es necesaria para el buen

funcionamiento de las empresas, además, tiene un lado sensible que es contraproducente para la eficiencia de la organización y sus procesos diarios.

La privacidad, la información y los datos personales, desde el punto de vista de su sistema operativo, requieren medios que sean tanto manejables como seguros en los que los datos no estén expuestos. Desde una perspectiva legal, el uso y almacenamiento de la información requiere seguridad jurídica que permita a los propietarios de la información tener confianza en su retención.

Triada CIA

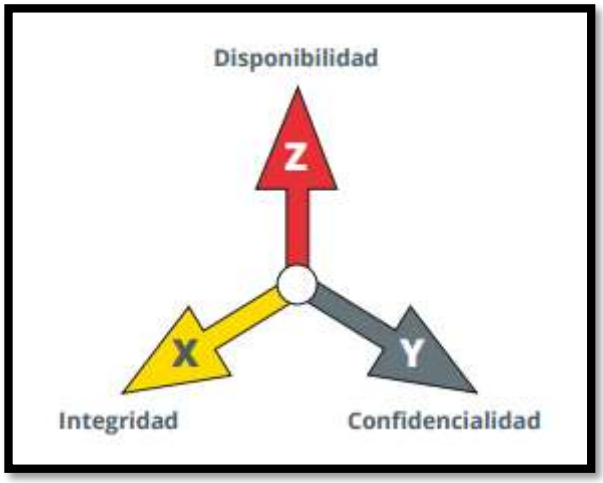
Según (Instituto Nacional de Ciberseguridad, 2020) en su colección protege tu empresa con el tema protección de la información describe las dimensiones de la seguridad de la información.

La seguridad de la información de divide en tres dimensiones, que son los pilares fundamentales para aplicar medidas de protección de los datos.

- La disponibilidad de la información hace referencia a que la información esté accesible cuando se necesite. Algunos ejemplos de falta de disponibilidad de la información son: cuando no es imposible acceder al correo electrónico corporativo debido a un error de configuración, o bien, cuando se sufre un ataque de denegación de servicio, en el que el sistema «cae» se impide accesos legítimos. Ambos tienen implicaciones serias para la seguridad de la información.(Instituto Nacional de Ciberseguridad, 2020, p. 6)
- La integridad de la información hace referencia a que la información sea correcta y esté libre de modificaciones y errores. La información es alterada intencionadamente o ser incorrecta y se toma decisiones en ella. Ejemplos de ataques contra la integridad de la información son la alteración malintencionada en los ficheros del sistema informático mediante la explotación de una vulnerabilidad, o la modificación de un informe de ventas por un empleado malintencionado o por error humano.(Instituto Nacional de Ciberseguridad, 2020, p. 6)

- La confidencialidad implica que la información es accesible únicamente por el personal autorizado. Es lo que se conoce como need-to-know. Con este término, se hace referencia a que la información solo se pone en conocimiento de las personas, entidades o sistemas autorizados para su acceso. Ejemplos de falta de confidencialidad, son el robo de información confidencial por parte de un atacante a través de Internet, la divulgación no autorizada a través de las redes sociales de información confidencial o el acceso por parte de un empleado a información crítica de la compañía ubicada en carpetas sin permisos asignados, a la que no debería tener acceso.(Instituto Nacional de Ciberseguridad, 2020, p. 6)

Figura 1. Dimensiones de la Seguridad de la Información



Fuente: Instituto Nacional de Ciberseguridad (INCIBE)

En base a la triada CIA de la Figura 1, se entiende que la seguridad de la información en sus diferentes tipos no es un activo para comprar ni un fin en sí mismo, y no solo basta en una determinada inversión para asegurar los datos de una institución, de la misma manera dicha información es gestionada hacia una meta concreta; con criterios generales y mejoras continuas al momento de tomar decisiones.

1.2. Datos Personales

Dado el avance tecnológico de los últimos años, el intercambio de información se ha realizado en volúmenes muy grandes, es decir, de manera masiva. Esta

situación ha permitido que, se tenga poco control sobre dicho intercambio, que incluye datos sensibles de las personas que dan a conocer algunas actividades que involucran las siguientes categorías: economía, gustos e intereses, preferencias y tendencias.

Por lo expuesto en el párrafo anterior, se establece que las personas tienen un registro digital, y por consiguiente con los datos personales se define a las personas, entender sus gustos, preferencias, su nivel socioeconómico, intereses, comportamientos, entre algunos otros aspectos, el mal uso de la información genera un alto riesgo.

Existen varias categorías de datos, por ejemplo, de identificación (nombre, domicilio, teléfono, correo electrónico, firma, cedula de identidad, Lugar y fecha de nacimiento, edad, nacionalidad, estado civil, entre otros); laborales (puesto, domicilio, correo electrónico y teléfono del trabajo); patrimoniales (información fiscal, historial crediticio, cuentas bancarias, ingresos y egresos); académicos (trayectoria educativa, título, número de cédula, certificados); datos sensibles como ideológicos (creencias religiosas, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y/o asociaciones religiosas; de salud (estado de salud, historial clínico, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico); características personales (tipo de sangre, ADN, huella digital, etc.); características físicas (color de piel, iris y cabello, señas particulares), la información mencionada es del titular y por consecuencia le pertenecen y deciden sobre ellos.

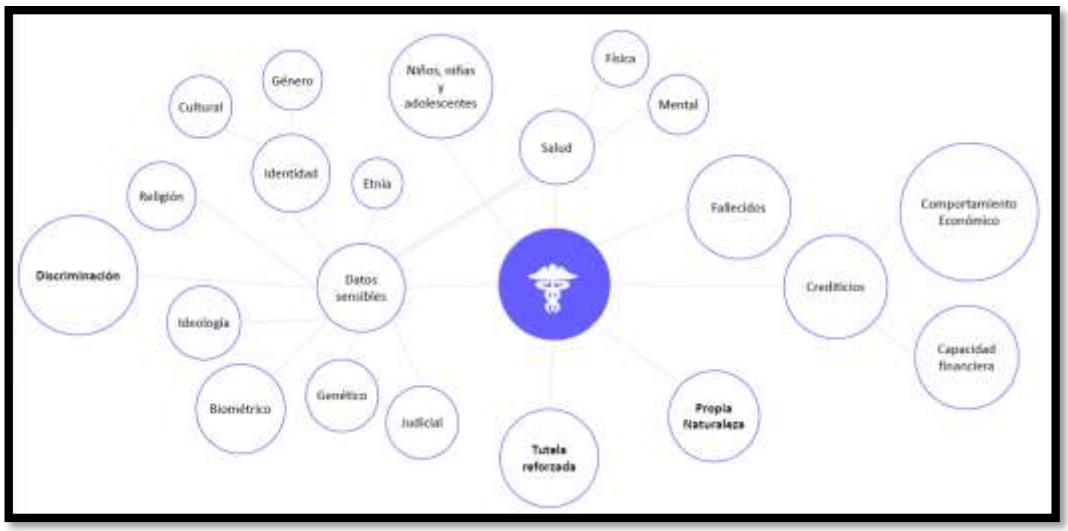
- **Datos Sensibles**

Los datos sensibles, se dividen desde lo material y formal; desde el punto material un dato sensible es aquel que revela o pone en manifiesto datos que hacen referencia a las cualidades de la persona relacionados con su dignidad, aspectos que afectan a la personalidad, su forma de ser entre otros; desde lo formal los datos requieren forzadas garantías de uso que alcancen su recogida y tratamiento, en estas fases los datos son expuestos según la voluntad de la persona.

Desde el punto de vista de (Ortiz, 1998), en su libro La violación de la intimidad en la protección de datos personales comenta que los datos sensibles se agrupan así, a las informaciones referidas a la libertad ideológica o creencias religiosas en un primer grupo y en segundo grupo involucra datos de origen racial, comportamiento sexual y salud.

Por lo tanto, datos sensibles son datos que identifican y hacen referencia a la ideología, origen étnico, situación patrimonial, financiera, opiniones políticas, color de cabello, filosofías, religión entre otros aspectos absolutamente personales e intrínsecos de cada individuo, en base a ello se considera que un dato sensible es aquello que, en caso de divulgarse de manera indebida, perturbarían la intimidad del ser humano.

Figura 2. Categoría Especiales de Datos



Fuente: https://telefonicatech.com/es

- **Diferencias entre datos personales y datos sensibles**

Un dato personal es cualquier información relacionada con una persona física identificada o identificable como nombre, edad, dirección, cédula, etc. Mientras que un dato sensible, se refiere a categorías especiales de datos personales que incluyen aquella información como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación

sindical, opiniones políticas, preferencia sexual; que afectan la esfera más íntima de la persona, o cuyo mal uso es causa de discriminación o provocar un riesgo grave.

De acuerdo con el informe final para segundo debate del Proyecto de Ley, se establecen categorías especiales de datos personales que incluyen: datos sensibles; datos de niñas, niños y adolescentes; datos de salud; y datos de personas con discapacidad y de sus sustitutos. Los datos catalogados dentro de categorías especiales se requieren de tratamientos específicos que les brinden y garanticen la efectiva vigencia de los derechos de sus titulares.

El uso masivo de las tecnologías y los avances científicos, que se evidencian hoy denotan, que se establecerían un sistema regulado sobre los datos personales, algo que en la actualidad es una tendencia mundial, donde paulatinamente varios países van implementado normativas de protección de datos en respuesta a derechos constitucionalmente reconocidos y a los marcos normativos vigentes.

1.3. Protección de Datos Personales

La protección de Datos de carácter personal se define como el amparo debido a los cuidados contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento automatizado, para de esa forma, confeccionar una información que, identificable con él, afecte a su entorno personal, social o profesional, en los límites de su intimidad. (Nuñez, 2007)

- **Principios básicos de la protección de datos**

La Organización para la Cooperación y el Desarrollo Económico (OECD) se define ciertos principios básicos que complementados con otros estándares y medidas facilitan la protección de la privacidad y de las libertades individuales.

Principio de limitación en la recolección de los datos

Existe límites para la recogida de datos personales y cualquiera de estos datos se obtiene con medios legales y justos y siempre que sea apropiado, con el conocimiento o consentimiento del sujeto implicado.

Principio de calidad de los datos

Los datos personales son relevantes para el propósito de su uso y, en la medida de lo necesario para dicho propósito, exactos, completos y actuales.

Principio de especificación del propósito

El propósito de la recogida de datos se especifica a más tardar en el momento en, que se produce dicha recogida, y su uso se ve limitado al cumplimiento de los objetivos u otros que no sean incompatibles con el propósito original, se especifica en cada momento el cambio de objetivo.

Principio de limitación de uso

No se divulga, se pone a disposición o usa los datos personales para propósitos que no cumplan lo expuesto en el principio anterior, excepto si se tiene el consentimiento del sujeto implicado o por imposición legal o de las autoridades (por ejemplo, se dispone de los datos recopilados con fines de toma de decisiones administrativas que están disponibles para investigación, estadísticas y planificación social).

Principio de salvaguardia de la seguridad

Se emplea salvaguardas razonables de seguridad para proteger los datos personales contra riesgos, tales como pérdida, acceso no autorizado, destrucción, uso, modificación o divulgación de los mismos. Los aspectos de seguridad y privacidad no son idénticos. Las limitaciones de uso y divulgación de los datos debieran ser reforzadas medidas de seguridad: físicas (por ejemplo, bloqueo de puertas, uso de tarjetas de identificación); organizacionales (por ejemplo, niveles de autoridad para acceder a los datos); en particular, en los sistemas informáticos.

Principio de transparencia

Existe una política general sobre transparencia en cuanto a evolución, prácticas y políticas relativas a datos personales. Se cuenta con medios ágiles para determinar la existencia y la naturaleza de datos personales, el

propósito principal para su uso y la identidad y lugar de residencia habitual de quien controla esos datos.

Principio de participación individual

Todo individuo tiene derecho a: Que el controlador de datos u otra fuente le confirme que tiene datos sobre su persona;

Que se le comuniquen los datos relativos a su persona

- ✓ en un tiempo razonable;
- ✓ a un precio, si existiese, que no sea excesivo;
- ✓ de forma razonable; y
- ✓ de manera inteligible;

Que se le expliquen las razones por las que una petición suya según los subapartados (a) y (b) haya sido denegada, así como cuestionar tal denegación; y

Expresar dudas sobre los datos relativos a su persona y, si su reclamación tiene éxito, conseguir que sus datos se eliminen, rectifiquen, completen o corrijan.

Principio de responsabilidad

Con los cambios tecnológicos y la mundialización surge de grandes desafíos y oportunidades para los gobiernos y ciudadanos de todo el mundo, mientras que la privacidad es cada día más objeto de atención, sobresale de un valor fundamental. Por tal razón en diferentes países manejan los principios expuestos anteriormente para proteger la privacidad, por lo que a nivel económico y tecnológico la privacidad es afectada. (*Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 2021, pp. 6-7)

1.4. ISO/IEC 27701:2019

La norma ISO/IEC 27701:2019 (Técnicas de seguridad – Extensión a ISO/IEC 27001 e ISO/IEC 27002 para la gestión de la información de privacidad – Requisitos y directrices) nace de la necesidad de certificar la gestión de la privacidad en el entorno empresarial y lo hace como una ampliación y extensión de la norma ISO/IEC 27001 y la guía ISO/IEC 27002, indicando cómo establecer, implementar,

mantener y mejorar de forma continua un Sistema de Gestión de Información de Privacidad y dar cumplimiento al Reglamento General de Protección de Datos (RGPD).(*ISO 27701: Sistema de gestión de cumplimiento del RGPD.*, 2021)

La protección de la privacidad es una necesidad social en el mundo cada vez más interconectado. A medida, que se fortalecen los requisitos de protección de datos, ISO/IEC 27701 ayuda a las empresas a gestionar sus riesgos de privacidad con libertad.

Ante el número creciente de ciberataques contra las empresas, la ciberseguridad es una cuestión importante; la nueva legislación en la privacidad introducida por los gobiernos en los últimos años, tales como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea o la Ley de privacidad de los consumidores de California, exigen una respuesta de las empresas. Sin embargo, a medida que los distintos países promulgan leyes diferentes en la privacidad de datos, ¿cómo garantizar la total protección de los datos personales?

La ISO/IEC 27701 es una forma sencilla y eficiente de abordar la cuestión de la difusión de unas prácticas uniformes de tratamiento de datos en toda una organización, aunque la ciberseguridad y la privacidad están interrelacionadas, en muchas organizaciones, se trata como proyectos diferentes.

La idea de crear la ISO/IEC 27701 norma de sistema de gestión de información de privacidad, o PIMS por sus siglas en inglés es vincular la norma al mundo de la ciberseguridad a través de la serie ISO/IEC 27000 de sistemas de gestión de seguridad de la información, el PIMS es una capa más de la estructura de ciberseguridad de una organización para establecer prácticas de tratamiento de datos que abarquen las consideraciones de seguridad y de privacidad.

Con el Sistema de Gestión de Información de Privacidad y dar cumplimiento al Reglamento General de Protección de Datos (RGPD), las empresas están obligadas a contar con un delegado de protección de datos que hoy en día es uno de los grandes desafíos para las personas que crean una documentación eficaz;

en otras palabras, el proceso del PIMS permite crear operaciones de privacidad más amplias y, desarrollar la documentación y los comportamientos visibles externamente.

- **¿Por qué implantar la 27701?**

Ayuda a reforzar el compromiso de las organizaciones con la seguridad de la información y el cumplimiento de la regulación vigente en protección de datos.

- Aporta un valor diferencial frente a los competidores
- Mejora la reputación corporativa

Para implantar la ISO 27701 se conoce previamente tanto la norma ISO/IEC 27001 como la guía ISO/IEC 27002 y el RGPD, que proporciona la base de cumplimiento de la norma objeto de estudio.

- **Estructura Norma ISO 27701**

Se toma como referencia a (Solutions, 2019) para la estructura de la Norma ISO 27701 se toma en cuenta los siguientes apartados para la protección de la privacidad de los datos.

La norma está compuesta de 8 apartados y 6 anexos.

> **Cláusula 5:** Los requerimientos establecidos en este apartado tienen trazabilidad con los apartados 4 al 10 de la norma ISO 27001, ampliando los requerimientos sobre protección de la información específicamente para el apartado 4 sobre el contexto organizacional y el apartado 6 relativo a la planificación de la gestión de riesgos, no aportando necesidades adicionales en el resto de los apartados.
> **Cláusula 6:** Este apartado amplía los requerimientos establecidos en la guía de buenas prácticas ISO 27002 y los controles establecidos en el Anexo A de la ISO 27001, haciendo un repaso de los 114 controles y ampliando los

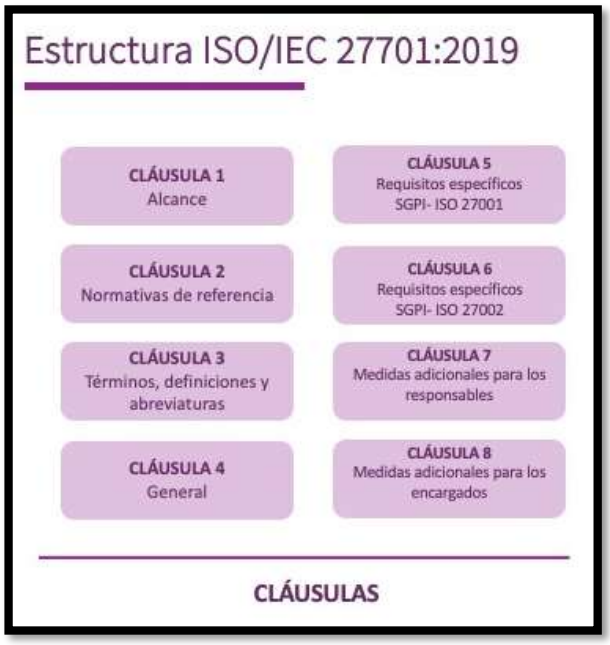
requisitos sobre la protección de la información en controles puntuales de los dominios 5 al 18, con excepción del dominio 17 (Seguridad de la información en la continuidad del negocio) donde no se establecen medidas adicionales a las ya existentes.

Cláusula 7: Determina controles adicionales y la guía de implementación de estos para los propietarios de la Información de identificación personal (PII). Estos controles no han de ser implementados en su totalidad, sino que su aplicabilidad o exclusión están debidamente justificadas.

Cláusula 8: De manera similar a los requerimientos de la cláusula 7, este apartado establece controles adicionales y una recomendación de implantación para los encargados de tratar información personal de terceros contratados, teniendo en cuenta también si éstos, a su vez, subcontratan servicios. (Solutions, 2019)

Para comprender de mejor manera la estructura de la ISO 27701 se muestra en la Figura 3 y 4 las cláusulas y anexos que establece la normativa.

Figura 3. Cláusulas de la ISO/IEC27701



Fuente: https://todopdp.com/anexos-del-estandar-iso-iec-27701/

Figura 4.Anexos de la ISO/IEC 27701



Fuente: https://todopdp.com/anexos-del-estandar-iso-iec-27701/

1.5. Ley Orgánica de Protección de Datos Personales

Con el avance de la tecnología y la globalización, cada día es más fácil vulnerar la privacidad de las personas y dar un mal uso de los datos personales, todos estos cambios disruptivos establecen nuevos retos al derecho de la protección de los datos personales. Por tal razón es importante regular el derecho a la protección de datos como un derecho autónomo, aunque pocos países han logrado darle dicho tratamiento.

Desde el 19 de septiembre del 2019, el presidente de la República presentó el proyecto de Ley de Protección de Datos Personales ante la Asamblea Nacional, Ecuador es uno de los pocos países de América Latina que no contaba con una Ley de Protección de Datos Personales, pese a que la sociedad maneja la digitalización diariamente.

De tal manera la Ley Orgánica de Protección de Datos Personales, publicada en el Quinto Suplemento del Registro Oficial No.459 fue aprobada el 26 de mayo de 2021 en Ecuador; en él, que se establece todos los requerimientos normativos que incluye el establecimiento de procesos y controles, revisar temas legales, definición

de responsabilidades para la gestión de protección de datos, evaluar las relaciones con sus proveedores con quienes intercambian información, implementar los principios de privacidad por diseño y establecer un marco de control de seguridad muy robusto.

Las organizaciones, en general, se evalúan todas las áreas, los procesos para identificar la existencia de datos personales, los cuales están almacenados en cualquier medio físico o digital y sobre esta base, evaluar los riesgos de privacidad y tomar las acciones necesarias, que son: fortalecer los controles y políticas, evitar la captura de datos innecesarios, ajustar los procesos y sistemas, renegociar contratos, capacitar al personal, entre otras.

La nueva Ley Orgánica de Protección de Datos Personales, exige a los responsables y encargados de tratamiento de los datos personales tener claro sus obligaciones y responsabilidades, a su vez los titulares de los datos personales conocer y ejercer positivamente sus derechos, de acuerdo con los derechos constitucionales consagrados.

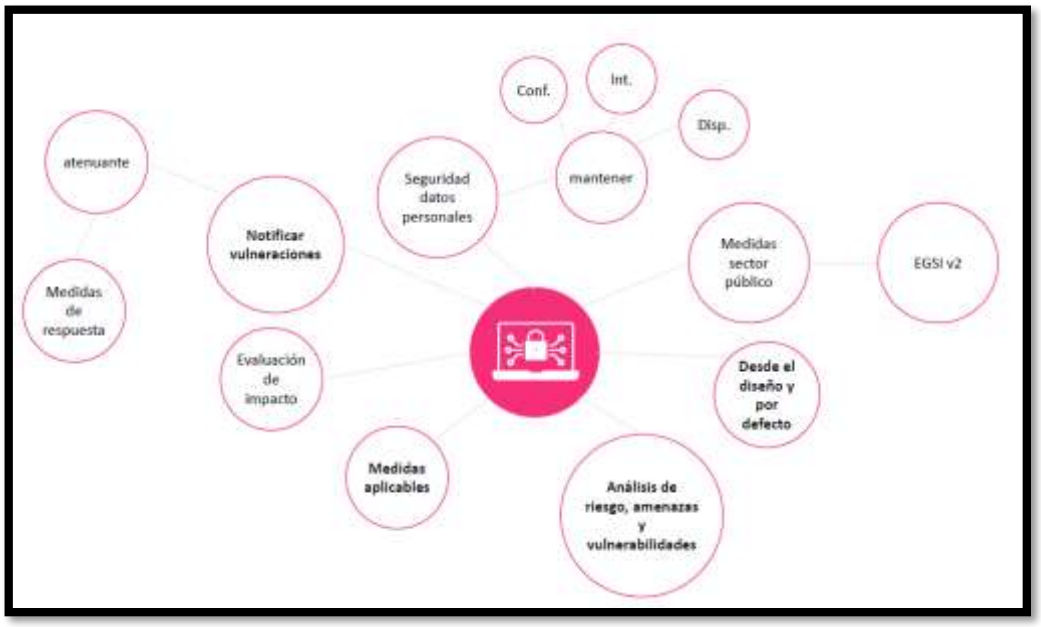
Las organizaciones para garantizar la seguridad de los datos requieren de equipos multidisciplinarios que incluyan profesionales del área legal, seguridad de la información, tecnología, procesos, riesgos, entre otros.

Un aspecto primordial es el cambio de la cultura sobre la propiedad de los datos personales; bajo la Ley, una empresa realiza con los datos personales únicamente lo que el titular autorice. Por esta razón, los datos se usan de manera estratégica, se apoya en un gobierno de datos y, de esta forma, crear la confianza digital que las organizaciones buscan y así fortalecer las estrategias de fidelización de los clientes, el uso adecuado y legítimo de los datos personales se traduce en beneficio para la organización.

Para el desarrollo del diseño de herramientas metodológicas en la seguridad de los datos personales se toma como referencia al capítulo VI, Seguridad de Datos Personales de la Ley Orgánica de Protección de Datos Personales. (Anexo 1)

En la figura 5 se visualiza de forma detallada los artículos de la Seguridad de Datos Personales de la Ley Orgánica Protección de Datos Personales.

Figura 5. Seguridad de Datos Personales



Fuente: https://telefonicatech.com/es

Debido de lo señalado en la ley orgánica de protección de datos personales se dice que la principal herramienta para proteger los datos personales es el titular de los datos personales, por motivo que se tiene la potestad de decidir sobre ellos, así que hay mecanismos para proteger los datos personales donde se cumpla los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad de tal manera que las organizaciones cumplan con todo lo expuesto.

Por esta razón, lo que se pretende en el proyecto es generar mecanismos mediante los cuales la información brindada a la organización sea tratada como confidencial; con la generación de contratos confidenciales, avisos de implementación de medidas de seguridad, entre otros.

CAPITULO II. DISEÑO METODOLÓGICO

2.1. Caracterización de la institución

La empresa Fenix Corp es una empresa proveedora de soluciones empresariales, nace en base a la necesidad de las PYMES de tener una herramienta para el control de sus procesos contables, logísticos, inventarios y facturación; en base a esto Fénix crea una herramienta que permite al usuario controlar todas las operaciones del negocio.

En 1999 se marca el inicio de Fenix Corp, expone al mercado módulos individuales para el control de inventarios, facturación y gestión de cobros, al 2002 se consolida la primera versión de Fenix Corp comercial – contable e inicia su comercialización a nivel nacional.

Fenix Corp es la primera empresa en el centro del país en implementar soluciones tecnológicas para pequeñas y medianas empresas que cuenta con 19 años en el mercado con cobertura a nivel nacional e internacional. El objetivo a largo plazo de Fenix Corp es seguir expandiéndose, llegar a varios países y a varios tipos de empresa con su solución contable.

- **Misión**

Automatizar los procesos administrativos de las micro, pequeñas y medianas empresas y profesionales independientes en todo el Ecuador con soluciones funcionales y adaptables a los continuos cambios.

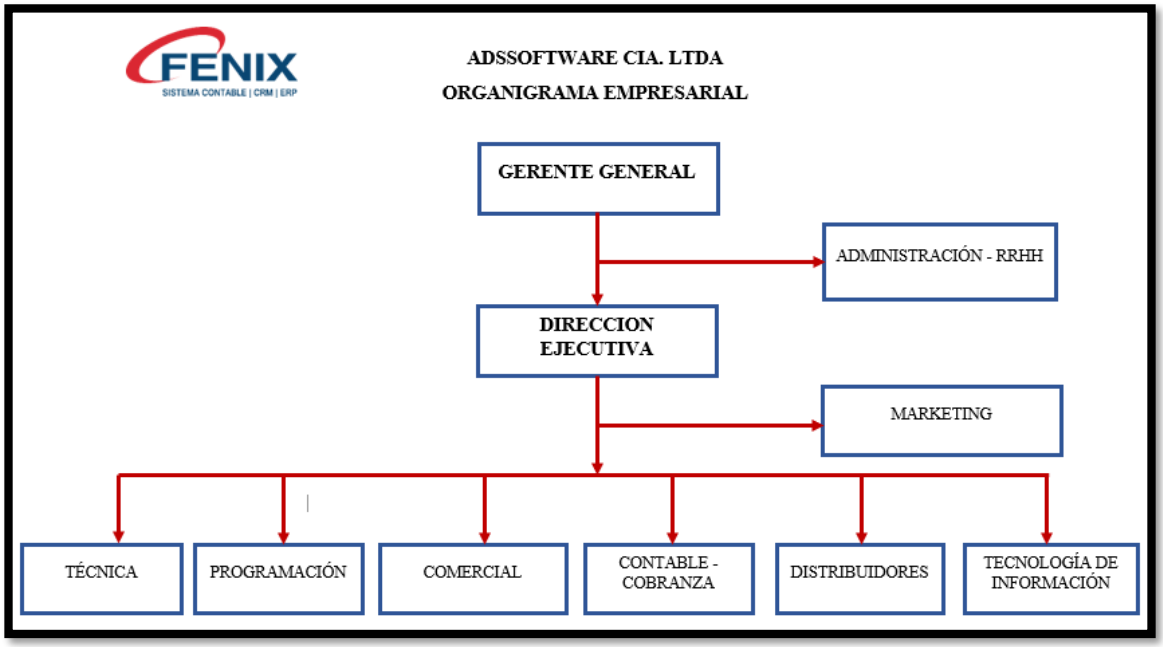
- **Visión**

Consolidarnos como una empresa líder en la automatización de procesos contables y administrativos para los clientes, desarrollando soluciones tecnológicas adaptables, aportando valor a las empresas y negocios gracias a el equipo de profesionales comprometidos con su trabajo, éticos y con alta calidad humana.

Cabe señalar que Fenix Corp cuenta con alrededor de 33 colaboradores entre personal administrativo, soporte técnico, I+D, marketing, comercialización e infraestructura, quienes en conjunto trabajan en las soluciones tecnológicas.

- **Organigrama Funcional**

Figura 6.Organigrama Funcional Fenix Corp



Fuente: Fenix Corp

2.2. Metodología de investigación

El presente proyecto de investigación busca la protección de los datos personales de la compañía, a fin de implementar una cultura preventiva del cumplimiento de protección de datos personales por la empresa, pues la adecuada información y sensibilización constituye el primer paso imprescindible para su difusión y adopción por las empresas, el documento contiene una variada metodología de investigación y, se basa en los métodos detallados a continuación:

Método Inductivo: Según el criterio de Abreu (2014) asegura que “el método inductivo plantea un razonamiento ascendente que fluye de lo particular o individual hasta lo general. Se razona que la premisa inductiva es una reflexión enfocada en el fin”.

Mediante este método, se busca conocer las características generales de la información digital que dispone Fenix Corp. Además, mediante el uso de este método, se tiene como objetivo desarrollar la propuesta de la herramienta metodológica para la seguridad de los datos personales.

Este método está relacionado con el enfoque de los Ítems de la Norma ISO 27701 para la gestión de la información de privacidad a través de requisitos y directrices, según el estado del arte explicado en el capítulo I del presente proyecto.

Método cualitativo: Este método tiene como objetivo recopilar información, por lo general, se usa en estudios basados en una investigación del estado del arte, se considera importante el uso de esta metodología para comprender la importancia de la información que dispone Fenix Corp a través de una encuesta a los implicados.

Acorde a lo mencionado el fin de la encuesta es obtener una justificación técnica-gerencial en el manejo de los datos personales.

Método Deductivo: Una vez obtenidos los resultados de la entrevista y encuesta realizada a la gran autoridad y empleados de Fenix Corp, utiliza el método para realizar el análisis y la justificación de la necesidad del diseño de herramientas metodológicas para la seguridad de los datos.

2.3. Tipos de Investigación

- **Investigación Bibliográfica**

Para el desarrollo del proyecto, se requiere el uso de este método para la revisión de literatura relacionada al campo de estudio, esto en base a que en la actualidad existe una gran vulnerabilidad de la privacidad y uso de los datos personales; por ello es importante conocer a fondo la Ley de Protección de Datos Personales.

- **Investigación de Campo**

El uso de esta investigación permite tener una mejor idea del procesamiento de los datos personales de la empresa, por lo, que se implementa técnicas y directrices donde se aplica la norma ISO/IEC 277001 que emplea la privacidad de la información.

Técnicas e Instrumentos

- **Encuesta**

La técnica por utilizar es la encuesta dirigida a los trabajadores de la empresa, se utiliza como instrumento el cuestionario a través de preguntas cerradas, que permite obtener mayor información.

La encuesta está conformada por 7 preguntas abiertas y cerradas, que son dirigidas al personal de la empresa para medir el nivel de conocimiento en la protección de los datos personales y qué medidas se considera para resguardarlos.

- **Población y Muestra**

Para la presente investigación se trabaja con el personal de la empresa de las diferentes áreas, soporte técnico, comercial, administrativo, finanzas, I+D, marketing, el valor de la población es menor a 100 no se requiere ejecutar el muestreo.

Tabla 1. Población

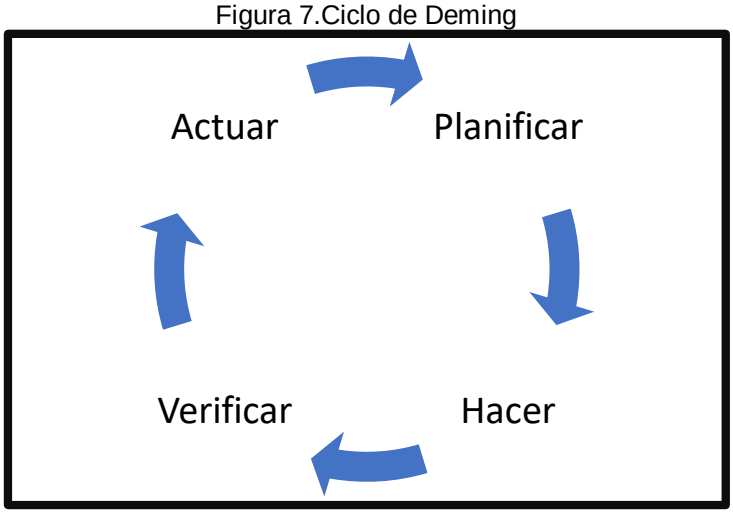
Población	Numero	Porcentaje
Soporte Técnico	12	36%
Comercial	4	12%
Administrativo	2	6%
Finanzas	4	12%
Desarrollo	9	27%
Marketing	2	6%
Total	**33**	**100%**

Fuente: elaboración propia

Metodología de Desarrollo

La ISO 27701 especifica los requisitos para establecer, implementar, mantener y mejorar continuamente en un Sistema de Gestión de Información de Privacidad (PIMS), es así que esta normativa se basa en los requisitos, controles y objetivos; por lo antes mencionado para el diseño de herramientas metodológicas se trabaja con el ciclo PDCA o ciclo PHVA, que viene de las siglas: planificar, verificar y actuar, en inglés: *plan, do, check, act,* también conocido como un ciclo de mejora continua o círculo de Deming. Esta metodología cuenta con cuatro fases que lleva a cabo de forma sistemática para lograr una mejora continua del tratamiento de los datos personales.

Figura 7.Ciclo de Deming



Fuente: elaboración propia

El diseño de las herramientas metodológicas para la seguridad de los datos personales consta de fases fundamentales, mismas que permite a Fenix Corp gestionar de manera eficiente y eficaz la protección de los datos personales.

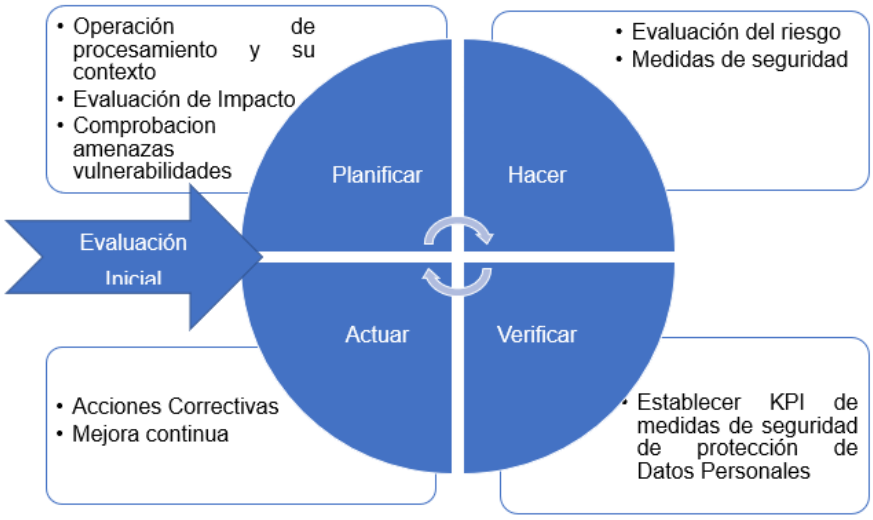
El objetivo del presente documento es diseñar herramientas metodológicas para la seguridad de datos personales en el cual se pone en práctica un modelo, de tal manera que mediante un proceso de mejora continua se logre un nivel de madurez aceptable en el ejercicio de minimizar los riesgos frente al tratamiento de la información personal.

Cabe mencionar que para las herramientas metodológicas es necesario acogerse a las normativas internas y a la legislación vigente en cuanto al tratamiento de los datos se refiere. De tal manera el diseño de herramientas metodológicas para la seguridad de datos personales constituye una estrategia para enfrentar los riesgos de seguridad y amenazas informáticas que comprende la triada CIA, es decir, poner en riesgo la confidencialidad, integridad y disponibilidad de los datos.

- **Detalle de las fases**

En este epígrafe se da a conocer las fases, que se incluyen en el diseño de la herramienta metodológica para la seguridad de los datos personales. En el detalle de las cinco fases se dan a conocer: recopilación de información, herramientas para el cumplimiento de las fases entre otros, que permita la seguridad de los datos personales en la organización.

Figura 8. Descripción de las fases del diseño planteado



Fuente: elaboración propia

En esta etapa se define la estrategia a ejecutarse, con el objetivo de organizar el trabajo a realizar se usa el software JIRA para enlistar las actividades a ejecutar de tal manera que al finalizar una de ellas cambie de etapa hasta la culminación de la actividad de tal forma, que se cumpla con todo el proceso de PDCA.

Figura 9.Planificación con software JIRA



Fuente: elaboración propia

Fase de Planificación

El alcance de la herramienta metodológica es de proveer de un marco referencial para la seguridad de los datos personales, mismos que permita mantener y mejorar la protección de los datos personales para el cumplimiento de entidades regulatorias. Las fases del ciclo PDCA se detalla en el siguiente cuadro:

Cuadro 1. Fases y subfases del desarrollo

FASE	SUBFASES
Planificar	a. Evaluación inicial
	b. Operación de procesamiento y su contexto
	c. Evaluación de Impacto
	d. Comprobación de amenazas y vulnerabilidades

Fuente: elaboración propia

En este apartado se evalúa la situación actual de la organización, mediante mecanismos de control de seguridad en que permiten conocer como los usuarios de los sistemas de información manejan los datos personales.

La siguiente tabla detalla la clasificación de la aplicación del control de seguridad, en las que asignan un puntaje según el estado de aplicabilidad del determinado mecanismo de control.

Tabla 2. Mecanismos de control de seguridad

CRITERIOS	PUNTAJE
No aplica	1
Redundante	2
Efectivo y no se cumple	3
No efectivo y se cumple	4
Efectivo y se cumple	5

Fuente: elaboración propia

En la tabla 2 se muestra los mecanismos de control, que se aplica a la empresa directamente con el encargado del área de TI para conocer que controles son aplicados; en base al anexo de la norma ISO 27001 Sistema de gestión de la seguridad de la información (SGSI) que mantiene la empresa.

Tabla 3. Mecanismos de control

Id	Objetivo de control	Puntaje Obtenido
1	Políticas de gestión de datos personales	3
2	Monitoreo y Evaluación	3
3	Identificación la legislación aplicable	3
4	Registros de evidencia	3
5	Recolección de evidencia	3
6	Revisión del cumplimiento técnico	1
7	Inventario y clasificación de los datos personales	3
8	Inventarios de activos	4
9	Identificación del ciclo de vida de un dato	3
10	Identificar responsabilidades de cada área	4
11	Acuerdo de confidencialidad	5
12	Capacitación	3
13	Proceso disciplinario	1
14	Control perimetral	1
15	Seguridad de cableado	5
16	Control de los activos fuera de las instalaciones	5
17	Destrucción segura de la información.	3
18	Escritorio limpio	4
19	Control ante robo	5
20	Control de cambios operacionales.	3
21	Segregación de tareas	3
22	Protección ante malware	5
23	Registros y auditorías a los funcionarios	3
24	Controles de Red	5
25	Administración de medios de almacenamiento secundario.	5
26	Seguridad de medios que son movilizados	3
27	Manejo de correo electrónico y mensajería instantánea.	5

28	Disociación de datos	1
29	Normas de control de acceso	3
30	Manejo de usuarios y claves de seguridad	1
31	Computadores que dejen de usarse	5
32	Accesos externos a sistemas de información	1
33	Segregación de redes	1
34	Controles de inicio de sesión	4
35	Trazabilidad de tratamiento	3
36	Asilamiento de datos sensibles	3
37	Uso de dispositivos móviles internos.	3
38	Autenticación de segundo factor de autenticación mediante tokens TOTP (*Time One- Time Password*)	3
39	Cifrado	3
40	Firmas Electrónicas	4
41	Procedimientos para el manejo de incidentes	3
42	Procedimientos en caso de incidentes	5
43	Reportes de incidentes de seguridad	3
44	Reporte de fallo en funcionamiento	4
45	Aprendizaje de incidentes	4
46	Actualizaciones del Modelo de Gestión	3

Fuente: elaboración propia

Con el resultado obtenido de la tabla 3 de los mecanismos de control se determina que el 29% de los mecanismos son efectivos, pero no se cumple dentro de la organización, de tal manera que es importante diseñar las herramientas metodológicas para cumplir en su totalidad con los mecanismos de control.

Evaluación de riesgos y medidas de seguridad de datos personales

La evaluación de riesgos es uno de los elementos sobre los que se sustenta cualquier modelo de prevención y control de la información. Las tareas iniciales de la gestión de riesgos son identificar y evaluar los riesgos, identificar los riesgos a los que están expuestos los datos personales es el elemento clave para realizar una evaluación completa. La no identificación de riesgos implica que los mismos no sean tratados y que los datos estén expuesto a riesgos potenciales.

A través de la evaluación de riesgos se conoce la operación del procesamiento de los datos que maneja la empresa; mediante la evaluación realizada adopta medidas de seguridad de acuerdo al nivel de riesgo.

Definición de la operación de procesamiento y su contexto

1. ¿En qué consiste el tratamiento de datos personales?
2. ¿Qué tipos de datos personales recopila?
3. ¿Cómo recopila los datos personales?
4. ¿Cuál es la finalidad del tratamiento?
5. ¿Dónde se almacenan los datos personales?
6. ¿Quién tiene permiso para acceder o manejar los datos personales?

Evaluación de Impacto

La evaluación de impacto se realiza por cada una de las operaciones del tratamiento de datos personales que se lleva a cabo dentro de la empresa u organización que implican un alto riesgo. Además, la evaluación de impacto cubre los datos personales a ser tratados, el tratamiento realizado, el responsable del tratamiento y en su caso a los encargados si existiesen.

La siguiente sección examina la evaluación del impacto sobre los derechos y libertades de las personas; da como resultado las posibles pérdidas de la información personal, se termina cuatro niveles de impacto (Bajo, Medio, Alto, Muy alto) como se muestra en la tabla 4.

Tabla 4. Descripción niveles de impacto

Impacto	Descripción	Puntaje
Bajo	Incidentes menores, que se superan sin ningún problema y menor tiempo.	1
Medio	Incidentes importantes, que se supera a pesar de algunas dificultades.	2
Alto	Se enfrenta a consecuencias significativas, que se supera, aunque con algunas dificultades.	3
Muy Alto	Se enfrenta a consecuencias irreversibles que no se supera.	4

Fuente: elaboración propia

Al comprender los niveles de impacto se determina que es un proceso cualitativo y el responsable de datos revisa una serie de factores como los tipos de datos personales, la criticidad de la operación de procesamiento, volumen de datos

personales, las características especiales del responsable de datos; así como categorías especiales de interesados.

Para la evaluación de impacto se evalúa por separado el impacto de la pérdida de confidencialidad, integridad y disponibilidad; el nivel más alto de estos niveles se considera como el resultado final de la evaluación de impacto.

Tabla 5. Evaluación de impacto

N°	PREGUNTA	EVALUACION	PUNTAJE
1	Nivel de impacto que produce la divulgación no autorizada de los datos personales (confidencialidad), en el contexto que lleva a cabo la actividad comercial.	☐ Bajo ☐ Medio ☐ Alto ☐ Muy Alto	1 2 3 4
2	Nivel de impacto en alteración no autorizada de los datos personales (integridad), en el contexto que lleva a cabo la actividad comercial.	☐ Bajo ☐ Medio ☐ Alto ☐ Muy Alto	1 2 3 4
3	Nivel de impacto en la destrucción o pérdida no autorizada de los datos personales (disponibilidad), en el contexto que lleva a cabo la actividad comercial.	☐ Bajo ☐ Medio ☐ Alto ☐ Muy Alto	1 2 3 4

Fuente: elaboración propia

El resultado final de impacto se calcula con la suma de las tres puntuaciones (confidencialidad, integridad y disponibilidad) de los diferentes niveles obtenidas en la tabla 5 de la evaluación de impacto que se asocia al resultado de la escala de la tabla 6 niveles de impacto.

Tabla 6. Niveles de impacto

TOTAL, IMPACTO	NIVEL DE IMPACTO
4 – 5	**Bajo**
6 – 8	**Medio**
9 – 12	**Alto**
13 – 15	**Muy Alto**

Fuente: elaboración propia

Definición de posibles amenazas y evaluación de su probabilidad.

Esta fase ayuda a comprender las amenazas relacionadas con el entorno general del procesamiento de datos personales de manera externas o internas y evaluar su probabilidad de ocurrencias de amenazas.

El objetivo de esta evaluación es que la empresa u organización sean conscientes del entorno del procesamiento de datos en que son directamente relevantes para las amenazas; se establecen cuatro dimensiones principales de las distintas áreas a evaluar, para la evaluación se desarrolla preguntas relacionadas con la probabilidad de ocurrencias de amenazas.

- Red y recursos técnicos (Hardware y Software)
- Procesos relacionados con la operación de tratamiento de datos
- Diferentes partes involucradas en la operación de tratamiento de datos
- Sector de actividad y escala del procesamiento

Cuadro 2. Posibles amenazas y evaluación de su probabilidad

Red y recursos técnicos (Hardware y Software)	
1	¿El ingreso de datos personales se realiza con uso del internet?
2	¿Se controla el acceso de usuarios a los datos personales?
3	¿El procesamiento de los datos esta interconectado a otros sistemas o servicios de TI?
4	¿Las personas no autorizadas acceden fácilmente al entorno de procesamiento de datos?
5	¿El procesamiento de datos personales está diseñado, implementado o mantenido sin seguir las mejores prácticas relevantes?
Procesos relacionados con la operación de tratamiento de datos	
6	¿Las funciones y responsabilidades con respecto al procesamiento de datos están claramente definidas?
7	¿El uso de la red, el sistema y recursos físicos dentro de la empresa es ambiguo o no está claramente definido?
8	¿El empleado usa su propio dispositivo para iniciar sesión en el sistema de procesamiento de datos personales?
9	¿El empleado transfiere, almacena o procesa datos personales fuera de las instalaciones de la organización?
10	¿Se realiza actividades de procesamiento de datos sin crear archivos de registro?
Diferentes partes involucradas en la operación de procesamiento	
11	¿El tratamiento de datos personales es realizado por los empleados? ¿Número de empleados?
12	¿Parte de la operación de procesamiento de datos es realizada por un tercero (procesador de datos)?
13	¿La obligación de los involucrados en el procesamiento de datos personales son ambiguas o no están claramente establecidas?
14	¿El personal involucrado en el procesamiento de datos personales no está familiarizado con los asuntos de seguridad de la información?
15	¿Los involucrados en la operación de procesamiento de datos no almacenan y/o destruyen de forma segura los datos personales?
Sector de actividad y escala del procesamiento	
16	¿Su sector empresarial es propenso a los ciberataques?
17	¿La empresa ha sufrido un ciberataque u otro tipo de brecha de seguridad en los últimos dos años?
18	¿Ha recibido alguna notificación en relación con la seguridad de los datos personales durante el último año?
19	¿Una operación de procesamiento se refiere a un gran volumen de personas y/o datos personales?
20	¿En su empresa se cumple las políticas de seguridad específicas para el uso adecuado de los datos personales?

Fuente: elaboración propia

Con lo detallado relacionado con la probabilidad de ocurrencias de amenazas se define para cada área la evaluación en tres niveles y calcular su valor final.

Tabla 7. Niveles de probabilidad de amenazas

Nivel	Detalle	Puntaje
Bajo	Probabilidad baja que la amenaza se cumpla	1
Medio	Probabilidad media que la amenaza se cumpla	2
Alto	Probabilidad alta que la amenaza se cumpla	3

Fuente: elaboración propia

Tabla 8. Evaluación de probabilidad

N°	AREA DE EVALUACION	PROBABILIDAD	
		NIVEL	PUNTAJE
1	Red y recursos técnicos (Hardware y Software)	☐ Bajo ☐ Medio ☐ Alto	1 2 3
2	Procesos relacionados con la operación de tratamiento de datos	☐ Bajo ☐ Medio ☐ Alto	1 2 3
3	Diferentes partes involucradas en la operación de tratamiento de datos	☐ Bajo ☐ Medio ☐ Alto	1 2 3
4	Sector de actividad y escala del procesamiento	☐ Bajo ☐ Medio ☐ Alto	1 2 3

Fuente: elaboración propia

La de ocurrencia de amenaza se calcula con la suma de las cuatro puntuaciones de las diferentes áreas obtenidas en la tabla 9 de la evaluación de probabilidad que se asocia al resultado de la escala de probabilidad de la tabla 10.

Tabla 9. Escala de probabilidad

TOTAL, PROBABILIDAD	NIVEL DE PROBABILIDAD
4 – 5	**Bajo**
6 – 8	**Medio**
9 – 12	**Alto**

Fuente: elaboración propia

- **Matriz de Riesgo**

Existen tipos de riesgos que ayudan a determinar el nivel de riesgo a los que están expuestos.

Alto Riesgo **Riesgo Medio** **Riesgo Bajo**

El valor del riesgo es el riesgo ante la falta de una acción que altera a la probabilidad o el impacto del mismo.

A continuación, se presenta una estructura de matriz de riesgo en el cual se llena con la información antes mencionada, en el que se conoce el estado de la información de la empresa y la implementación de algún tipo de control caso contrario proceder con su ejecución.

Cuadro 3. Matriz de Riesgo

		Nivel de Impacto		
Nivel de Probabilidad		**BAJO**	**MEDIO**	**ALTO / MUY ALTO**
	BAJO			
	MEDIO			
	ALTO			

Fuente: elaboración propia

Una vez identificado los riesgos y se obtiene el resultado final, la empresa se ajusta al nivel de riesgo obtenido, se tiene en cuenta las características específicas de los datos personales que no hayan sido evaluados durante el proceso y proporcionar un adecuado ajuste de los mismos,

- **Fase de Hacer**

Evaluación del riesgo

Una vez realizada la evaluación de impacto del tratamiento los datos y la probabilidad de ocurrencia de la amenaza correspondiente se realiza la evaluación de riesgo.

Para la evaluación de riesgo conlleva a seguir las siguientes acciones:

1. Identificar los riesgos a los que están expuestos los datos personales durante el ciclo de vida de su tratamiento.
2. Analizar los factores y elementos que determinan el nivel de riesgo.
3. Evaluar las consecuencias y el impacto que tiene los datos.

4. Reducir el riesgo con la aplicabilidad de medidas de control en el que se reduzcan la probabilidad e impacto.

En esta etapa se identifican los posibles riesgos que afectan al tratamiento de los datos personales y a los derechos de los involucrados.

Una amenaza es de diferentes tipos, sin embargo, existen amenazas que afectan las tres dimensiones de seguridad: confidencialidad, integridad y disponibilidad. Para identificar las amenazas a las que está expuesto el tratamiento de datos, se tiene en cuenta el ciclo de vida de los mismos, se identifica todos los escenarios en los que provoca la vulneración de los datos y derechos de los interesados.

El riesgo al ser identificado se especifica la causa del origen y las conductas inapropiadas que estos generan y clasificar por el nivel de priorización del riesgo.
Al contar con el nivel de riesgo, se procede a evaluar la probabilidad de que se produzca dicho riesgo y las consecuencias que produce. La manera de conocer los riesgos que se presenta en la empresa es mediante una matriz de riesgos.

Medidas de seguridad

Al finalizar con la evaluación del nivel del riesgo, la empresa procede con la selección de medidas de seguridad adecuadas para la protección de datos personales con la guía o apoyo de normas ISO 27001, 27002 y 27701.

Cuadro 4. Medidas de seguridad para el nivel de riesgo

CATEGORÍA	DESCRIPCIÓN	MEDIDA DE SEGURIDAD POR RIESGO
Política de seguridad y procedimientos de protección de datos personales	La organización documentara su política con respecto al procesamiento de datos personales como parte de su política de seguridad de la información.	RIESGO BAJO
	La política de seguridad se revisa y se aprueba, si es necesario, anualmente.	RIESGO BAJO
	La organización documentara una política de seguridad dedicada por separado con respecto al procesamiento de datos personales.	RIESGO MEDIO

	La política es aprobada por la gerencia y comunicada a todos los empleados y partes externas relevantes.	
	La política de seguridad hace referencia al menos a: las funciones y responsabilidades del personal, las medidas técnicas y organizativas básicas adoptadas para la seguridad de los datos personales, los encargados del tratamiento u otros terceros que intervengan en el tratamiento de los datos personales.	RIESGO MEDIO
	Crear y mantener un inventario de políticas/procedimientos específicos relacionados con la seguridad de los datos personales, con base en la política general de seguridad.	RIESGO MEDIO
	La política de seguridad se revisa semestralmente.	RIESGO ALTO
Funciones y responsabilidades	Las funciones y responsabilidades relacionadas con el procesamiento de datos personales están claramente definidas y asignadas de acuerdo con la política de seguridad	RIESGO BAJO
	Durante las reorganizaciones internas o despidos y cambios de empleo, la revocación de derechos y responsabilidades con los respectivos procedimientos de traspaso están claramente definidos.	RIESGO BAJO
	Realizar una designación clara de las personas a cargo de tareas específicas de seguridad, incluido el nombramiento de un oficial de seguridad.	RIESGO MEDIO
	Las tareas y responsabilidades del responsable de seguridad estan claramente establecidas y documentadas.	RIESGO ALTO
Política de control de acceso	Asignar derechos de control de acceso específicos a cada rol (involucrado en el procesamiento de datos personales).	RIESGO BAJO
	Una política de control de acceso es detallada y documentada. La organización determina en este documento las reglas de control de acceso apropiadas, los derechos de acceso y las restricciones para roles de usuario específicos hacia los procesos y procedimientos relacionados con los datos personales.	RIESGO MEDIO
	La segregación de funciones de control de acceso está claramente definida y documentada.	RIESGO MEDIO
	Los roles con derechos de acceso excesivos se definen claramente y	RIESGO ALTO

	asignan a miembros específicos limitados del personal.	
Gestión de recursos/activos	La organización cuenta con un registro de los recursos de TI utilizados para el procesamiento de datos personales (hardware, software y red). El registro incluye la información necesaria como: tipo, ubicación, persona asignada.	RIESGO BAJO
	Los recursos de TI se revisan y actualizan periódicamente.	RIESGO BAJO
	Los roles que tienen acceso a ciertos recursos se definen y documentan.	RIESGO MEDIO
	Los recursos de TI se revisan y actualizan anualmente.	RIESGO ALTO
Gestión del cambio	La organización se asegura de que todos los cambios en el sistema de TI sean registrados y supervisados por una persona específica (por ejemplo, un oficial de TI o de seguridad). Se realiza un seguimiento regular de este proceso.	RIESGO BAJO
	El desarrollo de software se realiza en un entorno de pruebas que no esté conectado al sistema de TI. Cuando se necesitan pruebas, se usa datos ficticios (no datos reales). En los casos en que esto no sea posible, existe procedimientos específicos para la protección de los datos personales utilizados en las pruebas.	RIESGO BAJO
	Existe una política de cambios detallada y documentada.	RIESGO MEDIO
Procesadores de datos	Se define, documenta directrices y procedimientos formales que cubran el procesamiento de datos personales por parte de los procesadores de datos (contratistas/ subcontratación) entre el controlador de datos y el procesador de datos antes del comienzo de las actividades de procesamiento. Estas directrices y procedimientos establecen obligatoriamente el mismo nivel de seguridad de los datos personales que establece la política de seguridad de la organización.	RIESGO BAJO
	Al enterarse de una violación de datos personales, el procesador de datos notifica al controlador in demora indebida.	RIESGO BAJO
	La organización del controlador de datos audita regularmente el cumplimiento del procesador de datos con el nivel acordado de requisitos y obligaciones.	RIESGO MEDIO

	Los empleados que procesan datos personales están sujetos a acuerdos específicos de confidencialidad/no divulgación documentados.	RIESGO ALTO
Tratamiento de incidencias / violaciones de datos personales	Definir un plan de respuesta a incidentes con procedimientos detallados para garantizar una respuesta ordenada a las incidencias relativas a datos personales	RIESGO BAJO
	Las violaciones de datos personales son informadas inmediatamente a la alta gerencia.	RIESGO BAJO
	El plan de respuesta a incidentes está documentado, incluida una lista de posibles acciones de mitigación y una asignación clara de roles.	RIESGO MEDIO
	Los incidentes y las violaciones de datos personales se registran junto con los detalles sobre el evento y las acciones de mitigación posteriores realizadas.	RIESGO ALTO
Continuidad del negocio	La organización establece los principales procedimientos y controles a seguir para asegurar el nivel requerido de continuidad y disponibilidad del sistema de TI que procesa datos personales (en caso de incidente/violación de datos personales).	RIESGO BAJO
	Un BCP es detallado y documentado en el que se incluye acciones claras y asignación de roles.	RIESGO MEDIO
	Se define un nivel de calidad de servicio garantizada en el BCP para los procesos comerciales centrales que brindan seguridad a los datos personales.	RIESGO MEDIO
	Designar personal específico con la responsabilidad, autoridad y competencia necesarias para gestionar la continuidad del negocio en caso de incidente/violación de datos personales.	RIESGO ALTO
	Considerar una instalación alternativa, según la organización y el tiempo de inactividad aceptable del sistema de TI.	RIESGO ALTO
Confidencialidad del personal	La organización asegura de que todos los empleados comprendan sus responsabilidades y obligaciones relacionadas con el procesamiento de datos personales. Los roles y responsabilidades se comunican claramente durante el proceso previo al empleo y/o de inducción.	RIESGO BAJO
	Antes de asumir sus funciones, se solicita a los empleados que revisen y acuerden la política de seguridad de la organización y firmen los	RIESGO MEDIO

	respectivos acuerdos de confidencialidad y no divulgación.	
	Los empleados involucrados en el procesamiento de datos personales de alto riesgo estan sujetos a cláusulas de confidencialidad específicas (en virtud de su contrato de trabajo u otro acto legal).	RIESGO ALTO
Capacitación	La organización se asegura de que todos los empleados estén adecuadamente informados sobre los controles de seguridad del sistema de TI que se relacionan con su trabajo diario. Los empleados involucrados en el procesamiento de datos personales también están debidamente informados sobre los requisitos de protección de datos y las obligaciones legales pertinentes a través de campañas periódicas de concienciación.	RIESGO MEDIO
	Preparar y ejecutar anualmente un plan de capacitación con metas y objetivos definidos.	RIESGO ALTO
Control de Acceso y autenticación	Se implementa un sistema de control de acceso aplicable a todos los usuarios que acceden al sistema de TI. El sistema permite crear, aprobar, revisar y eliminar cuentas de usuario.	RIESGO BAJO
	El uso de cuentas de usuario repetidos es evitado, en caso de ser necesario, se garantiza que todos los usuarios en común tienen los mismos roles y responsabilidades.	RIESGO BAJO
	Un mecanismo de autenticación es utilizar una combinación de nombre de usuario y contraseña. Las contraseñas respetan un cierto nivel de complejidad.	RIESGO BAJO
	El sistema de control de acceso tiene la capacidad de detectar y no permitir el uso de contraseñas que no respeten un determinado nivel de complejidad.	RIESGO BAJO
	Definir y documentar una política de contraseñas específica. La política incluye al menos la longitud de la contraseña, la complejidad, el período de validez, así como la cantidad de intentos de inicio de sesión fallidos aceptables.	RIESGO MEDIO
	Las contraseñas de los usuarios son almacenadas en forma de "hash".	RIESGO MEDIO
	Autenticación de doble factor se utiliza preferentemente para acceder a sistemas que procesan datos personales.	RIESGO ALTO

	Los factores de autenticación son contraseñas, tokens de seguridad, token secreto, biometría, etc.	
Registro y monitoreo	Los archivos de registro se activan para cada aplicación utilizada para el procesamiento de datos personales. Incluyen todos los tipos de acceso a los datos (ver, modificar, borrar).	RIESGO BAJO
	Los archivos de registro tienen una marca de tiempo y estar adecuadamente protegidos contra la manipulación y el acceso no autorizado.	RIESGO BAJO
	Se registra las acciones de los administradores y operadores del sistema, incluida la adición/eliminación/cambio de usuario.	RIESGO MEDIO
	No establecer la posibilidad de eliminación o modificación del contenido de los archivos de registro. El acceso a los archivos de registro también se registra, además, de monitorear para detectar actividad inusual.	RIESGO MEDIO
	Un sistema de monitoreo procesa los archivos de registro y produce informes sobre el estado del sistema y notifica sobre posibles alertas.	RIESGO MEDIO
Seguridad del servidor/base de datos	Los servidores de bases de datos y aplicaciones se configuran para ejecutarse con una cuenta separada, con privilegios mínimos de sistema operativo para funcionar correctamente.	RIESGO BAJO
	Los servidores de bases de datos y aplicaciones solo procesan los datos personales que realmente se necesitan procesar.	RIESGO BAJO
	Las soluciones de cifrado se consideran en archivos o registros específicos a través de la implementación de software o hardware.	RIESGO MEDIO
	Se considera el cifrado de unidades de almacenamiento	RIESGO MEDIO
	Se aplican técnicas de seudonomización se separa los datos de los identificadores directos para evitar vinculación al interesado sin información adicional	RIESGO MEDIO
	Aplicar técnicas que respaldan la privacidad a nivel de base de datos.	RIESGO ALTO
	Los usuarios no acceden a desactivar o eludir la configuración de seguridad.	RIESGO BAJO

Seguridad de la Estación de Trabajo	Las aplicaciones antivirus y las firmas de detección se configuran semanalmente.	RIESGO BAJO
	Los usuarios no cuentan con privilegios para instalar o desactivar aplicaciones no autorizadas.	RIESGO BAJO
	El sistema tiene tiempos de espera de sesión cuando el usuario no ha estado activo durante un período de tiempo determinado.	RIESGO BAJO
	Las actualizaciones de seguridad críticas publicadas por el desarrollador del sistema operativo se instala periódicamente.	RIESGO MEDIO
	El cifrado de disco completo está habilitado en las estaciones de trabajo.	RIESGO ALTO
	Las estaciones de trabajo utilizadas para el procesamiento de datos personales conectadas a Internet, aplicar medidas de seguridad para evitar el procesamiento, la copia y la transferencia no autorizados de datos personales almacenados.	RIESGO ALTO
	El acceso que realice a través de Internet, la comunicación es encriptada mediante protocolos criptográficos (TLS/SSL).	RIESGO BAJO
	El acceso inalámbrico al sistema de TI permite solo para usuarios y procesos específicos. Proteger por mecanismos de encriptación.	RIESGO MEDIO
	Se evita el acceso remoto al sistema de TI. En los casos en que esto sea absolutamente necesario, se realiza solo el bajo control y seguimiento de una persona específica de la organización	RIESGO MEDIO
	El tráfico hacia y desde el sistema de TI es monitoreado y controlado a través de firewalls y Sistemas de detección de intrusos.	RIESGO MEDIO
	No permitir la conexión a Internet a los servidores y estaciones de trabajo utilizados para el procesamiento de datos personales.	RIESGO ALTO
Copias de Seguridad	Los procedimientos de copia de seguridad y restauración de datos se definen, documentan y vinculan claramente a las funciones y responsabilidades.	RIESGO BAJO
	Las copias de seguridad reciben un nivel adecuado de protección física y ambiental de acuerdo con los estándares aplicados a los datos de origen	RIESGO BAJO

	Se monitorea la ejecución de las copias de seguridad para garantizar que estén completas.	RIESGO BAJO
	Se realizan copias de seguridad completas con regularidad.	RIESGO BAJO
	Las copias de la copia de seguridad se almacenan de forma segura en diferentes ubicaciones.	RIESGO MEDIO
	Los medios de respaldo se prueban regularmente para garantizar que se confié en ellos para uso de emergencia.	RIESGO MEDIO
	En caso de que se utilice un servicio de terceros para el almacenamiento de copias de seguridad, la copia es cifrados antes de ser transmitida desde el controlador de datos.	RIESGO MEDIO
	Las copias de las copias de seguridad son cifrados y almacenados de forma segura fuera de línea.	RIESGO ALTO
Dispositivos móviles/portátiles	Los procedimientos de gestión de dispositivos móviles y portátiles están definidos y documentados se establece reglas claras para su uso adecuado.	RIESGO BAJO
	Los dispositivos móviles que tienen permitido el acceso al sistema de información son preregistrados y preautorizados.	RIESGO BAJO
	Los dispositivos móviles están sujetos a los mismos niveles de procedimientos de control de acceso (al sistema de procesamiento de datos) que otros equipos terminales.	RIESGO BAJO
	La organización borra de forma remota los datos personales (relacionados con su operación de procesamiento) en un dispositivo móvil que haya sido comprometido.	RIESGO MEDIO
	Los dispositivos móviles admiten la separación del uso privado y comercial del dispositivo a través de contenedores de software seguros.	RIESGO MEDIO
	Los dispositivos móviles están físicamente protegidos contra robos cuando no estén en uso.	RIESGO MEDIO
	Aplicar doble factor de autenticación para acceder a dispositivos móviles	RIESGO ALTO
	Los datos personales almacenos en los dispositivos móviles están encriptado.	RIESGO ALTO
Seguridad del ciclo de vida de la aplicación	Los requisitos de seguridad específicos se definen durante las primeras etapas del ciclo de vida del desarrollo.	RIESGO BAJO
	Las tecnologías y técnicas específicas diseñadas para respaldar	RIESGO BAJO

	la privacidad y la protección de datos (también denominadas Tecnologías de mejora de la privacidad (PET)) son adoptadas a los requisitos de seguridad.	
	Seguir los estándares y prácticas de codificación segura.	RIESGO BAJO
	Durante el desarrollo, se realizan pruebas y validaciones contra la implementación de los requisitos de seguridad iniciales.	RIESGO BAJO
	La evaluación de vulnerabilidades, las pruebas de penetración de aplicaciones e infraestructuras son realizadas por un tercero de confianza antes de la adopción operativa. La solicitud no se acepta a menos que se alcance el nivel de seguridad requerido.	RIESGO MEDIO
	Se realizan pruebas de penetración periódicas.	RIESGO MEDIO
	Los parches de software son probados y evaluados antes de instalarlos en un entorno operativo.	RIESGO MEDIO
Eliminación de datos	La sobreescritura basada en software se realiza en todos los medios antes de desecharlos. En los casos en que esto no sea posible (Nas, Discos Externos, Usb, etc.) se realiza la destrucción física.	RIESGO BAJO
	Se procede a la trituración del papel y soportes portátiles utilizados para el almacenamiento de datos personales.	RIESGO BAJO
	Si se utilizan los servicios de un tercero para eliminar de forma segura los medios o los registros en papel, existe un acuerdo de servicio y existe un registro de destrucción de registros.	RIESGO MEDIO
	Si se utiliza un tercero, por lo tanto, el procesador de datos, para la destrucción de medios o archivos en papel, se considera que el proceso se lleva a cabo en las instalaciones del controlador de datos (y evitar la transferencia de datos personales fuera del sitio).	RIESGO ALTO
Seguridad física	El acceso físico de la infraestructura del sistema de TI no es accesible por personal no autorizado.	RIESGO BAJO
	Establecer una identificación clara, a través de medios apropiados, por ejemplo, tarjetas de identificación, para todo el personal y los visitantes que accedan a las instalaciones de la organización, según corresponda.	RIESGO MEDIO

	Definir zonas seguras y estar protegido por controles de entrada apropiados.	RIESGO MEDIO
	Instalar sistemas de detección de intrusos en todas las zonas de seguridad.	RIESGO MEDIO
	Implementar en el servidor un sistema automático de supresión de incendios, un sistema de aire acondicionado dedicado de control cerrado y un sistema de alimentación ininterrumpida (UPS).	RIESGO MEDIO
	El personal externo del servicio de apoyo tiene acceso restringido a las áreas seguras.	RIESGO MEDIO

Fuente: elaboración propia

CAPÍTULO III. ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN

Tras la elaboración de herramientas metodológicas para la protección de datos personales se identifica los posibles riesgos a los que está que expuesta la empresa u organización; de tal manera se realiza la comprobación de amenazas y vulnerabilidades a los que enfrenta la empresa.

Para la comprobación de amenazas y vulnerabilidades existentes en la empresa se aplica la herramienta metodológica para la protección de datos personales con la aprobación y aceptación de la junta directiva de Fenix Corp; el personal de la empresa está involucrado en la fase de ingreso de los datos personales que ayuda en el desarrollo de la herramienta en el que se evalúa los riesgos a los que están expuestos los datos y que medidas de seguridad aplicarlo.

Para la aplicabilidad de la herramienta se requiere del personal de TI para la supervisión y revisión de cada una de las fases que son planteadas en la Figura 7, al finalizar el proceso en la junta directiva evalúa que todo lo descrito se cumpla y que es mejorado.

Con lo expuesto anteriormente se procede con la aplicación de la herramienta metodología en las diferentes áreas que conforman la empresa; de esta manera se conoce el grado de aceptación de la herramienta aplicada, se toma como base al documento de la *European Union Agency For Network and Information Security* en su manual titulado *Handbook on Security of Personal Data Processing* (ENISA, 2017)

3.2. Casos de uso y enfoque del informe

Con este fin, se han identificado una serie de operaciones de procesamiento. Estas operaciones de procesamiento varían desde los procesos relacionados con los recursos humanos (RRHH), el marketing, la contabilidad, el I+D, comercial, soporte técnico y la seguridad física/control de acceso, áreas que conforman la empresa.

Los casos de uso se centran únicamente en las medidas de seguridad y no pretenden proporcionar ningún análisis legal, los casos de uso solo pretenden facilitar la provisión de ejemplos prácticos y no brindan ninguna indicación con respecto a la legalidad/cumplimiento de operaciones específicas de procesamiento de datos.

La naturaleza de las actividades comerciales, el tamaño y la organización interna de la empresa, las actividades de Recursos Humanos incluyen procedimientos adicionales, procesar más o menos datos personales o para diferentes propósitos.

- **Casos de uso: Área de recursos humanos**

Las operaciones de tratamiento más comunes que se considera en este informe son:

a) Gestión de nómina
b) Selección de personal
c) Evaluación de personal

- **Gestión de Nomina**

Dentro de la gestión de nómina se procesa datos personales de los empleados de cada área que conforma la empresa, en el que se registra el salario, beneficios y seguridad social. Los datos personales se registran con la información detallada en el cuadro 5 de Operación de procesamiento y su contexto, este proceso facilita al personal de RRHH cumplir con las políticas especificadas dentro de la empresa. Aunque el responsable de los RRHH realiza un contrato de confidencialidad, no se conoce el proceso de seguridad de los datos personales de los empleados.

Definición de la operación de procesamiento y su contexto

Para la operación de procesamiento de datos se detalla de la siguiente manera:

Cuadro 5. Operación de procesamiento Gestión de Nomina

DATOS	TIPO DE DATO
Finalidad del tratamiento	Gestión de Nomina
Medios de procesamiento	Interno
Destinatario de los Datos	Interno
Procesador de datos utilizados	Interno
DATOS PERSONALES DEL EMPLEADO	
Nombres y Apellidos Correo electrónico Dirección Teléfono Foto Lugar y Lugar y fecha de nacimiento Historial de empleo, título del trabajo Hijos	Datos Personales Procesados
DATOS PERSONALES DEL EMPLEADO	
Salario Prestaciones Vacaciones Seguridad Social	Finalidad del tratamiento
DATOS PERSONALES DEL EMPLEADO DENTRO DE LA ORGANIZACIÓN	
Área ID empleado Usuario de acceso Contraseña	Datos sensibles

Fuente: elaboración propia

Con la información obtenida en la operación de tratamiento y su contexto se realiza una evaluación de impacto a los que están expuestos; los datos están expuestos a un cierto número de riesgos que afectan a la integridad, confidencialidad y disponibilidad.

Evaluación de Impacto

Para la evaluación de impacto el encargado de TI realiza la evaluación conforme a la Tabla 4 de la pérdida de confidencialidad, integridad y disponibilidad de los datos personales con la persona encargada del área de recursos humanos de la empresa, donde se observa que los datos entregados por el personal en la ficha del empleado no están seguros; se da como resultado el nivel de impacto de los datos personales a ser tratados, el tratamiento a realizar, a su vez los resultados obtenidos es evaluado por la junta directiva de la empresa para la toma de decisiones.

El resultado final de la evaluación al área de recursos humanos se toma conforme a la tabla 5 de la evaluación de impacto con sus tres niveles de impacto:

Tabla 10. Evaluación de impacto RRHH

N°	EVALUACION DE IMPACTO		
1	Confidencialidad	Alto	3
2	Integridad	Medio	2
3	Disponibilidad	Alto	3
Evaluación de impacto General		MEDIO 8	

Fuente: elaboración propia

- **Pérdida de confidencialidad**

Dentro del alcance de la operación de procesamiento de la gestión de la nómina de los empleados, el impacto de la pérdida de confidencialidad está a la posible divulgación no intencional de información a terceros. Se expone al interesado a consecuencias que van desde la incomodidad derivada del conocimiento público de sus propios datos privados hasta incluso a riesgo potencial de ataques. Esto es más que una simple molestia y, por lo tanto, el impacto de la pérdida de confidencialidad se establece en **ALTA.**

- **Pérdida de integridad**

La pérdida de integridad es **MEDIA**, por lo que se espera que los interesados enfrenten inconvenientes, pero los problemas se superan rápidamente.

- **Pérdida de disponibilidad**

La pérdida de disponibilidad es **ALTA**, por lo que se espera que los interesados enfrenten inconvenientes, pero las dificultades se superan a un tiempo determinado.

El resultado global de la evaluación del impacto los niveles de confidencialidad y disponibilidad son los más altos identificados. Por lo tanto, el impacto general en el caso de Gestión de Nomina se evalúa como **MEDIO**.

Comprobación de amenazas y vulnerabilidades

Mediante la aplicabilidad del cuadro 2 en el que se detalla las posibles amenazas y evaluación de su probabilidad se realiza la comprobación del nivel de probabilidad de ocurrencia de amenazas.

Tabla 11. Comprobación de amenazas y vulnerabilidades

N°	AREA DE EVALUACION	PROBABILIDAD	
		NIVEL	PUNTAJE
1	Red y recursos técnicos (Hardware y Software)	Bajo	1
2	Procesos relacionados con la operación de tratamiento de datos	Medio	2
3	Diferentes partes involucradas en la operación de tratamiento de datos	Alto	3
4	Sector de actividad y escala del procesamiento	Baja	1
Probabilidad general de ocurrencia de amenazas		**MEDIO 7**	

Fuente: elaboración propia

- **Red y recursos técnicos (Hardware y Software)**

La probabilidad de ocurrencia de amenazas es **BAJA,** por lo que el sistema no está conectado al internet y no permite el acceso desde internet a los recursos internos y a los sistemas de TI.

- **Procesos relacionados con la operación de tratamiento de datos**

La probabilidad de ocurrencia de amenazas es **MEDIA,** por lo que el responsable de recursos humanos cumple con algunas de las funciones y responsabilidades claramente definidas junto a las políticas establecidas para el procesamiento de los datos personales.

- **Diferentes partes involucradas en la operación de procesamiento**

La probabilidad de ocurrencia de amenazas es **ALTA,** por la falta de capacitación a los encargados de recursos humanos en temas relevantes de seguridad de la información y de la manera segura en la que se destruye o procesa los datos personales.

- **Sector de actividad y escala del procesamiento**

La probabilidad de ocurrencia de amenazas es **BAJA,** por lo que los empleados tienen limitaciones al procesar la información, a su vez la organización no se considera propenso a los ciberataques.

El resultado global de la probabilidad general de ocurrencia de amenazas se calcula como **MEDIA.**

Evaluación de Riesgo y Adopción de Medidas de Seguridad

En base a los resultados de la evaluación de impacto y la probabilidad de ocurrencia de amenazas, se realiza la evaluación de riesgos con la matriz anteriormente mencionada en el cuadro 3.

Cuadro 6. Evaluación de Riesgo y Adopción de Medidas de Seguridad

		NIVEL DE IMPACTO		
NIVEL DE PROBABILIDAD		BAJO	MEDIO	ALTO / MUY ALTO
	BAJO			
	MEDIO		X	
	ALTO			

Fuente: elaboración propia

El resultado de la evaluación de riesgos de gestión de nómina es considerado como **MEDIO**, lo cual se adapta medidas adecuadas para la prevención de riesgos.

- **Selección de personal**

Dentro de la gestión de contratación del personal el responsable de recursos humanos es la encargada de llevar a cabo el proceso de selección de personas que tienen la capacidad o habilidades para realizar las tareas encomendadas; el proceso de selección se da con la revisión de hojas de vida, nivel de estudios, experiencia laboral, formación profesional, datos personales, entre otros datos. Una vez finalizada la revisión de CV el encargado de RRHH elabora una lista de candidatos para ser invitados a una entrevista. Durante la entrevista, el jefe superior toma nota sobre el desempeño del candidato y al final elabora un informe detallado que se presenta a la alta dirección.

Definición de la operación de procesamiento y su contexto

Para la operación de procesamiento de datos se detalla de la siguiente manera:

Tabla 12. Operación de procesamiento selección de personal

DATOS	TIPO DE DATO
Finalidad del tratamiento	Candidatos
Medios de procesamiento	Interno
Destinatario de los Datos	Interno
Procesador de datos utilizados	Interno sin procesar datos
DATOS PERSONALES	
Nombres y Apellidos Correo electrónico Dirección Teléfono Lugar y fecha de nacimiento Estado Civil Experiencia Laboral Nivel de Estudios Capacitaciones	Datos Personales Procesados
DATOS PERSONALES DEL JEFE SUPERIOR	
Nombre y Apellido Cargo / Área Fecha de entrevista	Finalidad del tratamiento
Informe de Entrevista	

Fuente: elaboración propia

Con la información obtenida en la operación de tratamiento y su contexto se realiza una evaluación de impacto a los que están expuestos; los datos están expuestos a

un cierto número de riesgos que afectan a la integridad, confidencialidad y disponibilidad.

Evaluación de Impacto

Para la evaluación de impacto el encargado de TI realiza la evaluación conforme a la Tabla 6 de la pérdida de confidencialidad, integridad y disponibilidad de los datos personales con la persona encargada del área de recursos humanos de la empresa, donde se observa que los datos entregados para la selección de personal no están seguros; se da como resultado el nivel de impacto de los datos personales a ser tratados, el tratamiento a realizar, a su vez los resultados obtenidos es evaluado por la junta directiva de la empresa para la toma de decisiones.

El resultado final de la evaluación al área de recursos humanos para la selección de personal se toma conforme a la tabla 5 de la evaluación de impacto se realiza el siguiente análisis:

Tabla 13. Evaluación de impacto selección de personal

N°	EVALUACION DE IMPACTO		
1	Confidencialidad	Medio	2
2	Integridad	Medio	2
3	Disponibilidad	Bajo	1
Evaluación de impacto General		BAJO 5	

Fuente: elaboración propia

- **Pérdida de confidencialidad**

Dentro del alcance de la operación de selección de personal, la pérdida de confidencialidad está la posible divulgación de datos de los candidatos, lo que provoca difamación. Esto se relaciona con la divulgación de nivel de estudios, experiencia y capacidad profesional del candidato, se ocasiona daños o se perjudica para que conseguía un empleo. Según lo manifestado el responsable no divulga dicha información; por lo tanto, el nivel de impacto es **MEDIA.**

- **Pérdida de integridad**

La pérdida de integridad es **MEDIA**, la alteración no autorizada de los datos personales o informes de entrevista de un candidato dificulta o suspende el proceso de contratación.

- **Pérdida de disponibilidad**

La pérdida de disponibilidad es **BAJO**, por lo que se espera que los interesados enfrenten inconvenientes.

El resultado global de la evaluación del impacto los niveles de confidencialidad y disponibilidad son los más altos identificados. Por lo tanto, el impacto general en el caso de Gestión de Nomina se evalúa como **BAJO**.

Comprobación de amenazas y vulnerabilidades

Mediante la aplicabilidad del cuadro 2 en el que se detalla las posibles amenazas y evaluación de su probabilidad se realiza la comprobación del nivel de probabilidad de ocurrencia de amenazas.

Tabla 14. Comprobación de amenazas y vulnerabilidades

N°	AREA DE EVALUACION	PROBABILIDAD	
		NIVEL	PUNTAJE
1	Red y recursos técnicos (Hardware y Software)	Bajo	1
2	Procesos relacionados con la operación de tratamiento de datos	Medio	2
3	Diferentes partes involucradas en la operación de tratamiento de datos	Medio	2
4	Sector de actividad y escala del procesamiento	Baja	1
Probabilidad general de ocurrencia de amenazas		MEDIO 6	

Fuente: elaboración propia

- **Red y recursos técnicos (Hardware y Software)**

La probabilidad de ocurrencia de amenazas es **BAJA,** por lo que el sistema no está conectado al internet y no permite el acceso desde internet a los recursos internos y a los sistemas de TI.

- **Procesos relacionados con la operación de tratamiento de datos**

La probabilidad de ocurrencia de amenazas es **MEDIA,** por lo que el responsable de recursos humanos cumple con algunas de las funciones y responsabilidades claramente definidas junto a las políticas establecidas para el procesamiento de los datos personales.

- **Diferentes partes involucradas en la operación de procesamiento**

La probabilidad de ocurrencia de amenazas es **ALTA,** por la falta de capacitación a los encargados de recursos humanos en temas relevantes de seguridad de la información y de la manera segura en la que se destruye o procesa los datos personales.

- **Sector de actividad y escala del procesamiento**

La probabilidad de ocurrencia de amenazas es **BAJA,** por lo que los empleados tienen limitaciones al procesar la información, a su vez la organización no se considera propenso a los ciberataques.

El resultado global de la probabilidad general de ocurrencia de amenazas se calcula como **MEDIA.**

Evaluación de Riesgo y Adopción de Medidas de Seguridad

En base a los resultados de la evaluación de impacto y la probabilidad de ocurrencia de amenazas, se realiza la evaluación de riesgos con la matriz anteriormente mencionada en el cuadro 3.

Tabla 15. Evaluación de Riesgo y Adopción de Medidas de Seguridad

		NIVEL DE IMPACTO		
		BAJO	**MEDIO**	**ALTO / MUY ALTO**
NIVEL DE PROBABILIDAD	**BAJO**		X	
	MEDIO			
	ALTO			

Fuente: elaboración propia

El resultado de la evaluación de riesgos de gestión de selección de personal es considerado como **MEDIO**, lo cual se adapta medidas adecuadas para la prevención de riesgos.

- **Evaluación de personal**

Dentro de la gestión de evaluación del personal el jefe superior de cada área considera evaluar a los empleados anualmente para conocer el nivel de conocimiento que mantiene relacionados con el desempeño y características profesionales, que incluyen confiabilidad, puntualidad, habilidades interpersonales, trabajo en equipo, estado emocional, entre otros; el proceso es realizado por el responsable de recursos humanos con documentación en papel. La evaluación es debidamente firmada por el personal y el departamento de recursos humanos genera un informe final que es enviado electrónicamente a la alta gerencia.

Definición de la operación de procesamiento y su contexto

Para la operación de procesamiento de datos se detalla de la siguiente manera:

Tabla 16. Operación de procesamiento evaluación de personal

DATOS	TIPO DE DATO
Finalidad del tratamiento	Evaluación
Medios de procesamiento	Interno
Destinatario de los Datos	Interno
Procesador de datos utilizados	Interno sin procesar datos
DATOS PERSONALES	
Nombre y Apellido Cargo Fecha de ingreso Habilidades Técnicas Conocimiento Capacitaciones Estado Emocional	Datos Personales Procesados
DATOS PERSONALES DEL JEFE SUPERIOR	
Nombre y Apellido Cargo Fecha de evaluación	Finalidad del tratamiento
Informe de Evaluación	

Fuente: elaboración propia

Con la información obtenida en la operación de tratamiento y su contexto se realiza una evaluación de impacto a los que están expuestos; los datos están expuestos a un cierto número de riesgos que afectan a la integridad, confidencialidad y disponibilidad.

Evaluación de Impacto

Para la evaluación de impacto el encargado de TI realiza la evaluación conforme a la Tabla 5 de la pérdida de confidencialidad, integridad y disponibilidad de los datos personales con la persona encargada del área de recursos humanos de la empresa, donde se observa que los datos entregados en la evolución al personal no están seguros; da como resultado el nivel de impacto de los datos personales a ser tratados, el tratamiento a realizar, a su vez los resultados obtenidos es evaluado por la junta directiva de la empresa para la toma de decisiones.

El resultado final de la evaluación al área de recursos humanos se toma conforme a la tabla 6 de la evaluación de impacto se realiza el siguiente análisis.

Tabla 17. Evaluación de Impacto evaluación del personal

N°	EVALUACION DE IMPACTO		
1	Confidencialidad	Medio	2
2	Integridad	Medio	2
3	Disponibilidad	Bajo	1
Evaluación de impacto General		BAJO 5	

Fuente: elaboración propia

- **Pérdida de confidencialidad**

Dentro del alcance de la operación de evaluación de personal, la pérdida de confidencialidad está la posible divulgación de datos de la evaluación de los empleados el que provoca malestar o incomodidad de los empleados. por lo tanto, el nivel de impacto es **MEDIA.**

- **Pérdida de integridad**

La pérdida de integridad es **MEDIA**, la alteración no autorizada de los datos personales o informes de la evaluación para el beneficio de los resultados de la evaluación.

- **Pérdida de disponibilidad**

La pérdida de disponibilidad es **BAJO**, por lo que se espera que los interesados enfrenten inconvenientes.

El resultado global de la evaluación del impacto los niveles de confidencialidad y disponibilidad son los más altos identificados. Por lo tanto, el impacto general en el caso de Gestión de Nomina se evalúa como **BAJO**.

Comprobación de amenazas y vulnerabilidades

Mediante la aplicabilidad del cuadro 2 en el que se detalla las posibles amenazas y evaluación de su probabilidad se realiza la comprobación del nivel de probabilidad de ocurrencia de amenazas.

Tabla 18. Comprobación de amenazas y vulnerabilidades

N°	AREA DE EVALUACION	PROBABILIDAD	
		NIVEL	PUNTAJE
1	Red y recursos técnicos (Hardware y Software)	Bajo	1
2	Procesos relacionados con la operación de tratamiento de datos	Medio	2
3	Diferentes partes involucradas en la operación de tratamiento de datos	Medio	2
4	Sector de actividad y escala del procesamiento	Baja	1
Probabilidad general de ocurrencia de amenazas		MEDIO 6	

Fuente: elaboración propia

- **Red y recursos técnicos (Hardware y Software)**

La probabilidad de ocurrencia de amenazas es **BAJA,** por lo que el sistema no está conectado al internet y no permite el acceso desde internet a los recursos internos y a los sistemas de TI.

- **Procesos relacionados con la operación de tratamiento de datos**

La probabilidad de ocurrencia de amenazas es **MEDIA,** por lo que el responsable de recursos humanos cumple con algunas de las funciones y responsabilidades claramente definidas junto a las políticas establecidas para el procesamiento de los datos personales.

- **Diferentes partes involucradas en la operación de procesamiento**

La probabilidad de ocurrencia de amenazas es **MEDIA,** por la falta de capacitación a los encargados de recursos humanos en temas relevantes de seguridad de la información y de la manera segura en la que se destruye o procesar los datos personales.

- **Sector de actividad y escala del procesamiento**

La probabilidad de ocurrencia de amenazas es **BAJA,** por lo que los empleados tienen limitaciones al procesar la información, a su vez la organización no se considera propenso a los ciberataques.

El resultado global de la probabilidad general de ocurrencia de amenazas se calcula como **MEDIA.**

Evaluación de Riesgo y Adopción de Medidas de Seguridad

En base a los resultados de la evaluación de impacto y la probabilidad de ocurrencia de amenazas, se realiza la evaluación de riesgos con la matriz anteriormente mencionada en el cuadro 3.

Tabla 19. Evaluación de Riesgo y Adopción de Medidas de Seguridad

		NIVEL DE IMPACTO		
NIVEL DE PROBABILIDAD		BAJO	MEDIO	ALTO / MUY ALTO
	BAJO		X	
	MEDIO			
	ALTO			

Fuente: elaboración propia

El resultado de la evaluación de riesgos de gestión de selección de personal es **MEDIO**, lo cual se adapta medidas adecuadas para la prevención de riesgos.

- **Casos de uso: Área de Marketing**

Las operaciones de tratamiento más comunes que se considera en este informe son:

- **Campañas de Marketing**

Dentro de la gestión de campañas de Marketing se procesa datos personales de clientes potenciales con el fin de promocionar los diferentes productos que oferta la empresa.

Para esta operación de procesamiento, la empresa hace uso de herramientas web, ofrecidas por un proveedor externo especializado en tales actividades, el proveedor externo se rige a las mejores prácticas de seguridad relevantes.

Cada mes, el departamento de marketing, inserta en la herramienta web, a través de una interfaz web adecuada, la información de contacto (nombre y apellido, teléfono, correo electrónico, ciudad, lugar y fecha de nacimiento) de los clientes potenciales.

Cada semana, inicia una nueva campaña de marketing a través de la herramienta web, que luego envía los respectivos correos electrónicos personalizados, a la última lista de destinatarios actualizada. Para cada campaña, la herramienta proporciona un informe con estadísticas sobre el porcentaje de correos electrónicos leídos, no leídos, eliminados sin proporcionar información sobre personas específicas.

Definición de la operación de procesamiento y su contexto

Para la operación de procesamiento de datos se detalla de la siguiente manera:

Cuadro 7. Operación de procesamiento Campañas de Marketing

DATOS	**TIPO DE DATO**
Finalidad del tratamiento	Campañas de Marketing
Medios de procesamiento	Interno
Destinatario de los Datos	Interno y Externo
Procesador de datos utilizados	Proveedor de servicios web de campañas de marketing de terceros
DATOS PERSONALES	
Nombre y Apellido Correo Ciudad Teléfono Lugar y fecha de nacimiento	Datos Personales Procesados
DATOS PERSONALES DEL JEFE SUPERIOR	
Nombre y Apellido Cargo Fecha de informe	Finalidad del tratamiento
Informe Estadístico	

Fuente: elaboración propia

Con la información obtenida en la operación de tratamiento y su contexto se realiza una evaluación de impacto a los que están expuestos; los datos están expuestos a un cierto número de riesgos que afectan a la integridad, confidencialidad y disponibilidad.

Evaluación de Impacto

Para la evaluación de impacto el encargado de TI realiza la evaluación conforme a la Tabla 5 de la pérdida de confidencialidad, integridad y disponibilidad de los datos personales con la persona encargada del área de marketing de la empresa, donde se observa que los datos obtenidos de los clientes en las campañas no están seguros; se obtiene como resultado el nivel de impacto de los datos personales a ser tratados, el tratamiento a realizar, a su vez los resultados obtenidos es evaluado por la junta directiva de la empresa para la toma de decisiones.

El resultado final de la evaluación al área de marketing se toma conforme a la tabla 6 de la evaluación de impacto se realiza el siguiente análisis:

Tabla 20. Evaluación de impacto Campañas de Marketing

N°	EVALUACION DE IMPACTO		
1	Confidencialidad	Bajo	1
2	Integridad	Bajo	1
3	Disponibilidad	Bajo	1
Evaluación de impacto General		BAJO 3	

Fuente: elaboración propia

- **Pérdida de confidencialidad, integridad y disponibilidad**

Dentro del alcance de la operación de campañas de marketing, la pérdida de confidencialidad, integridad y disponibilidad se considera **BAJA;** la posible divulgación no autorizada de datos las campañas llegan al buzón de spam.
El resultado global de la evaluación del impacto los niveles de confidencialidad, integridad se evalúa como **BAJO**.

Comprobación de amenazas y vulnerabilidades

Mediante la aplicabilidad de la tabla 8 en el que se detalla las posibles amenazas y evaluación de su probabilidad se realiza la comprobación del nivel de probabilidad de ocurrencia de amenazas.

Tabla 21. Comprobación de amenazas y vulnerabilidades

N°	AREA DE EVALUACION	PROBABILIDAD	
		NIVEL	PUNTAJE
1	Red y recursos técnicos (Hardware y Software)	Medio	2
2	Procesos relacionados con la operación de tratamiento de datos	Baja	1
3	Diferentes partes involucradas en la operación de tratamiento de datos	Medio	2
4	Sector de actividad y escala del procesamiento	Baja	1
Probabilidad general de ocurrencia de amenazas		MEDIO 6	

Fuente: elaboración propia

- **Red y recursos técnicos (Hardware y Software)**

La probabilidad de ocurrencia de amenazas es **MEDIA,** por lo que el sistema está conectado al internet y permite el acceso desde internet a los recursos internos y externos.

- **Procesos relacionados con la operación de tratamiento de datos**

La probabilidad de ocurrencia de amenazas es **BAJA,** por lo que se asume que el proceso de la aplicación externa es claramente definido junto a las políticas establecidas para el procesamiento de los datos personales.

- **Diferentes partes involucradas en la operación de procesamiento**

La probabilidad de ocurrencia de amenazas es **MEDIA,** por que la operación de procesamiento de datos lo maneja una aplicación externa, por lo tanto, la empresa no tiene el control total de los datos.

- **Sector de actividad y escala del procesamiento**

La probabilidad de ocurrencia de amenazas es **BAJA,** por lo que la empresa toma medidas de seguridad en contra a los ataques cibernéticos por la operación de procesamiento que involucra a una gran cantidad de personas.

El resultado global de la probabilidad general de ocurrencia de amenazas se calcula como **MEDIA.**

Evaluación de Riesgo y Adopción de Medidas de Seguridad

En base a los resultados de la evaluación de impacto y la probabilidad de ocurrencia de amenazas, se realiza la evaluación de riesgos con la matriz anteriormente mencionada en el cuadro 3.

Cuadro 8. Evaluación de Riesgo y Adopción de Medidas de Seguridad

	NIVEL DE IMPACTO			
NIVEL DE PROBABILIDAD		BAJO	MEDIO	ALTO / MUY ALTO
	BAJO			
	MEDIO	X		
	ALTO			

Fuente: elaboración propia

El resultado de la evaluación de riesgos de gestión de campañas de Marketing es considerado como **MEDIO**, lo cual se adapta medidas adecuadas para la prevención de riesgos.

- **Casos de uso: Área de Contabilidad**

Las operaciones de tratamiento más comunes que se considera en este informe son:

- **Estados Financieros**

Dentro de la gestión de Estados Financieros se procesa datos que identifican como está estructurada la empresa y la manera en la que se maneja los ingresos y egresos bajo la supervisión del gerente.

Toda la información contable lo registran dentro de una aplicación propia de la empresa, en que se registra el Ruc, representante legal, teléfono, contador, dirección y correo electrónico.

Definición de la operación de procesamiento y su contexto

Para la operación de procesamiento de datos se detalla de la siguiente manera:

Cuadro 9. Operación de procesamiento Estados Financieros

DATOS	**TIPO DE DATO**
Finalidad del tratamiento	Estados Financieros
Medios de procesamiento	Interno
Destinatario de los Datos	Interno y Externo
Procesador de datos utilizados	Interno sin procesar datos
DATOS PERSONALES	
Nombre y Apellido Correo Ciudad Teléfono Cedula Firma	Datos Personales Procesados
DATOS PERSONALES DEL GERENTE FINANCIERO	
Nombre y Apellido Cargo Fecha de informe	Finalidad del tratamiento
Informe Financiero	

Fuente: elaboración propia

Con la información obtenida en la operación de tratamiento y su contexto se realiza una evaluación de impacto a los que están expuestos; los datos están expuestos a un cierto número de riesgos que afectan a la integridad, confidencialidad y disponibilidad.

Evaluación de Impacto

Para la evaluación de impacto el encargado de TI realiza la evaluación conforme a la Tabla 5 de la pérdida de confidencialidad, integridad y disponibilidad de los datos personales con la persona encargada del área de contabilidad de la empresa, donde se observa que los estados financieros no están seguros; se obtiene como resultado el nivel de impacto de los datos personales a ser tratados, el tratamiento a realizar, a su vez los resultados obtenidos es evaluado por la junta directiva de la empresa para la toma de decisiones.

El resultado final de la evaluación al área de contabilidad se toma conforme a la tabla 6 de la evaluación de impacto se realiza el siguiente análisis:

Tabla 22. Evaluación de impacto de Estados Financieros

N°	EVALUACION DE IMPACTO		
1	Confidencialidad	Alta	3
2	Integridad	Media	2
3	Disponibilidad	Media	2
Evaluación de impacto General		MEDIA 7	

Fuente: elaboración propia

- **Pérdida de confidencialidad**

Dentro del alcance de la operación de procesamiento de estados financieros de la empresa, el impacto de la pérdida de confidencialidad está a la posible divulgación no intencional de información a terceros es **ALTA**. Se expone a la empresa a consecuencias que van desde la divulgación del conocimiento público de sus propios datos privados hasta incluso a riesgo potencial de robos.

- **Pérdida de integridad y disponibilidad**

Dentro del alcance de la operación de estados financieros la pérdida de integridad y disponibilidad es **MEDIA;** la posible divulgación no autorizada de datos los estados financieros son revelados a la competencia.

El resultado global de la evaluación del impacto los niveles de confidencialidad, integridad y disponibilidad se evalúa como **MEDIA**.

Comprobación de amenazas y vulnerabilidades

Mediante la aplicabilidad del cuadro 2 en el que se detalla las posibles amenazas y evaluación de su probabilidad se realiza la comprobación del nivel de probabilidad de ocurrencia de amenazas.

Tabla 23. Comprobación de amenazas y vulnerabilidades

N°	AREA DE EVALUACION	PROBABILIDAD	
		NIVEL	PUNTAJE
1	Red y recursos técnicos (Hardware y Software)	Medio	2
2	Procesos relacionados con la operación de tratamiento de datos	Medio	2
3	Diferentes partes involucradas en la operación de tratamiento de datos	Medio	2
4	Sector de actividad y escala del procesamiento	Baja	1
Probabilidad general de ocurrencia de amenazas		MEDIO 7	

Fuente: elaboración propia

- **Red y recursos técnicos (Hardware y Software)**

La probabilidad de ocurrencia de amenazas es **MEDIA,** por lo que el sistema está conectado al internet y permite el acceso desde internet a los recursos internos y externos.

- **Procesos relacionados con la operación de tratamiento de datos**

La probabilidad de ocurrencia de amenazas es **MEDIA,** por lo que se asume que el proceso de la aplicación externa es claramente definido junto a las políticas establecidas para el procesamiento de los datos personales.

- **Diferentes partes involucradas en la operación de procesamiento**

La probabilidad de ocurrencia de amenazas es **MEDIA,** por que la operación de procesamiento de datos lo maneja una aplicación externa, por lo tanto, la empresa no tiene el control total de los datos.

- **Sector de actividad y escala del procesamiento**

La probabilidad de ocurrencia de amenazas es **BAJA,** por lo que la empresa toma medidas de seguridad en contra a los ataques cibernéticos por la operación de procesamiento que involucra a una gran cantidad de personas.

El resultado global de la probabilidad general de ocurrencia de amenazas se calcula como **MEDIA.**

Evaluación de Riesgo y Adopción de Medidas de Seguridad

En base a los resultados de la evaluación de impacto y la probabilidad de ocurrencia de amenazas, se realiza la evaluación de riesgos con la matriz anteriormente mencionada en el cuadro 3.

Cuadro 10. Evaluación de Riesgo y Adopción de Medidas de Seguridad

	NIVEL DE IMPACTO			
NIVEL DE PROBABILIDAD		BAJO	MEDIO	ALTO / MUY ALTO
	BAJO			
	MEDIO		X	
	ALTO			

Fuente: elaboración propia

El resultado de la evaluación de riesgos de gestión de estados financieros es considerado como **MEDIO**, lo cual se adapta medidas adecuadas para la prevención de riesgos.

- **Casos de uso: Área Comercial**

Las operaciones de tratamiento más comunes que se considera en este informe son:

- **Gestión de clientes**

Dentro de la gestión de clientes se maneja datos personales en que se registran en una aplicación de CRM donde se almacena información de contacto de clientes y posibles clientes, y oportunidades de ventas en los diferentes sectores comerciales. Dentro de la aplicación de Gestión de Relaciones con el Cliente (*CRM)* a través de una interfaz web adecuada, se registra la información de contacto (nombre y apellido, ruc/ci, nombre de la compañía, representante legal, teléfono, correo electrónico, ciudad) de los posibles clientes.

Una vez registrada toda la información solicitada en la interfaz web se realiza el proceso de contacto con el cliente para conocer los requerimientos o necesidades de su empresa para ofertarle el mejor producto que mantiene la empresa.

Cada semana, el jefe del área comercial solicita un informe con estadísticas de los clientes registrados en el CRM y el proceso de gestión de los mismos.

Definición de la operación de procesamiento y su contexto

Para la operación de procesamiento de datos se detalla de la siguiente manera:

Cuadro 11. Operación de procesamiento Gestión Clientes

DATOS	TIPO DE DATO
Finalidad del tratamiento	Gestión Clientes
Medios de procesamiento	Interno
Destinatario de los Datos	Interno
Procesador de datos utilizados	CRM
DATOS PERSONALES	
Nombre y Apellido Ruc / CI Nombre de la Compañía Representante Legal Correo electrónico Ciudad Teléfono	Datos Personales Procesados
DATOS PERSONALES DEL JEFE SUPERIOR	
Nombre y Apellido Cargo Fecha de informe	Finalidad del tratamiento
Informe Estadístico	

Fuente: elaboración propia

Con la información obtenida en la operación de tratamiento y su contexto se realiza una evaluación de impacto a los que están expuestos; los datos están expuestos a un cierto número de riesgos que afectan a la integridad, confidencialidad y disponibilidad.

Evaluación de Impacto

Para la evaluación de impacto el encargado de TI realiza la evaluación conforme a la Tabla 5 de la pérdida de confidencialidad, integridad y disponibilidad de los datos personales con la persona encargada del área comercial de la empresa, donde se observa que los datos obtenidos de los clientes no están seguros; se obtiene como resultado el nivel de impacto de los datos personales a ser tratados, el tratamiento a realizar, a su vez los resultados obtenidos es evaluado por la junta directiva de la empresa para la toma de decisiones.

El resultado final de la evaluación al área comercial se toma conforme a la tabla 6 de la evaluación de impacto se realiza el siguiente análisis:

Tabla 24. Evaluación de impacto Gestión de Clientes

N°	EVALUACION DE IMPACTO		
1	Confidencialidad	Medio	2
2	Integridad	Medio	2
3	Disponibilidad	Medio	2
Evaluación de impacto General		MEDIO 6	

Fuente: elaboración propia

- **Pérdida de confidencialidad, integridad y disponibilidad**

Dentro del alcance de la operación de gestión de clientes, la pérdida de confidencialidad, integridad y disponibilidad es **MEDIA;** la posible divulgación no autorizada de datos, alteración y eliminación de los datos procesados genera inconvenientes significativos para la empresa.

El resultado global de la evaluación del impacto los niveles de confidencialidad, integridad se evalúa como **MEDIA**.

Comprobación de amenazas y vulnerabilidades

Mediante la aplicabilidad del cuadro 2 en el que se detalla las posibles amenazas y evaluación de su probabilidad se realiza la comprobación del nivel de probabilidad de ocurrencia de amenazas.

Tabla 25. Comprobación de amenazas y vulnerabilidades

N°	AREA DE EVALUACION	PROBABILIDAD	
		NIVEL	PUNTAJE
1	Red y recursos técnicos (Hardware y Software)	Medio	2
2	Procesos relacionados con la operación de tratamiento de datos	Baja	1
3	Diferentes partes involucradas en la operación de tratamiento de datos	Medio	2
4	Sector de actividad y escala del procesamiento	Baja	1
Probabilidad general de ocurrencia de amenazas		MEDIO 6	

Fuente: elaboración propia

- **Red y recursos técnicos (Hardware y Software)**

La probabilidad de ocurrencia de amenazas es **MEDIA,** por lo que el sistema está conectado al internet y permite el acceso desde internet a los recursos internos y externos.

- **Procesos relacionados con la operación de tratamiento de datos**

La probabilidad de ocurrencia de amenazas es **BAJA,** por lo que se asume que el proceso de la aplicación externa es claramente definido junto a las políticas establecidas para el procesamiento de los datos personales.

- **Diferentes partes involucradas en la operación de procesamiento**

La probabilidad de ocurrencia de amenazas es **MEDIA,** por que la operación de procesamiento de datos lo maneja una aplicación externa, por lo tanto, la empresa no tiene el control total de los datos.

- **Sector de actividad y escala del procesamiento**

La probabilidad de ocurrencia de amenazas es **BAJA,** por lo que la empresa toma medidas de seguridad en contra a los ataques cibernéticos por la operación de procesamiento que involucra a una gran cantidad de personas.

El resultado global de la probabilidad general de ocurrencia de amenazas se calcula como **MEDIA.**

Evaluación de Riesgo y Adopción de Medidas de Seguridad

En base a los resultados de la evaluación de impacto y la probabilidad de ocurrencia de amenazas, se realiza la evaluación de riesgos con la matriz anteriormente mencionada en el cuadro 3.

Cuadro 12. Evaluación de Riesgo y Adopción de Medidas de Seguridad

	NIVEL DE IMPACTO			
NIVEL DE PROBABILIDAD		BAJO	MEDIO	ALTO / MUY ALTO
	BAJO			
	MEDIO	X		
	ALTO			

Fuente: elaboración propia

El resultado de la evaluación de riesgos de gestión de clientes es considerado como **MEDIO**, lo cual se adapta medidas adecuadas para la prevención de riesgos.

- **Casos de uso: Área Soporte**

Las operaciones de tratamiento más comunes que se considera en este informe son:

- **Gestión de soporte**

Dentro de la gestión de soporte se maneja datos personales en que se registran en una aplicación de CRM donde se almacena información de contacto de los clientes que solicitan soporte del sistema.

Dentro de la aplicación del CRM a través de una interfaz web adecuada, se registra la información de contacto (nombre y apellido, ruc/ci, nombre de la compañía, teléfono, correo electrónico, incidente reportado) de los clientes.

Una vez registrada toda la información solicitada en la interfaz web se realiza el proceso de contacto con el cliente para realizar el soporte solicitado con la persona de contacto.

Cada semana, el jefe del área de soporte genera un informe con estadísticas de los clientes atendidos y el número de ticket pendientes a ser atendidos.

Definición de la operación de procesamiento y su contexto

Para la operación de procesamiento de datos se detalla de la siguiente manera:

Cuadro 13. Operación de procesamiento Gestión de Soporte

DATOS	TIPO DE DATO
Finalidad del tratamiento	Gestión de soporte (Registro de Ticket)
Medios de procesamiento	Interno
Destinatario de los Datos	Interno
Procesador de datos utilizados	CRM
DATOS PERSONALES	
Nombre y Apellido Ruc / CI Nombre de la Compañía Correo electrónico Teléfono Incidente	Datos Personales Procesados
DATOS PERSONALES DEL CALL CENTER	
Nombre y Apellido Cargo Fecha de informe	Finalidad del tratamiento
Informe Estadístico	

Fuente: elaboración propia

Con la información obtenida en la operación de tratamiento y su contexto se realiza una evaluación de impacto a los que están expuestos; los datos están expuestos a un cierto número de riesgos que afectan a la integridad, confidencialidad y disponibilidad.

Evaluación de Impacto

Para la evaluación de impacto el encargado de TI realiza la evaluación conforme a la Tabla 5 de la pérdida de confidencialidad, integridad y disponibilidad de los datos personales con la persona encargada del área de soporte técnico de la empresa, donde se observa que los datos obtenidos de los clientes que solicitan soporte no están seguros; el resultado del nivel de impacto de los datos personales a ser tratados, el tratamiento a realizar, a su vez los resultados obtenidos es evaluado por la junta directiva de la empresa para la toma de decisiones.

El resultado final de la evaluación al área de soporte técnico se toma conforme a la tabla 6 de la evaluación de impacto se realiza el siguiente análisis:

Tabla 26. Evaluación de impacto Gestión de soporte (Registro de Ticket)

N°	EVALUACION DE IMPACTO		
1	Confidencialidad	Medio	2
2	Integridad	Medio	2
3	Disponibilidad	Muy Alto	4
Evaluación de impacto General		MEDIO 8	

Fuente: elaboración propia

- **Pérdida de confidencialidad e integridad**

Dentro del alcance de la operación de gestión de soportes, la pérdida de confidencialidad e integridad es **MEDIA;** la posible divulgación no autorizada de datos, y alteración de los datos procesados genera inconvenientes significativos para la empresa.

- **Pérdida de disponibilidad**

Dentro del alcance de la operación de gestión de soportes, la pérdida de disponibilidad es **MUY ALTA;** la posible eliminación no autorizada de datos procesados genera inconvenientes significativos e incluso la mala reputación para la empresa.

El resultado global de la evaluación del impacto los niveles de confidencialidad, integridad y disponibilidad se evalúa como **MEDIA**.

Comprobación de amenazas y vulnerabilidades

Mediante la aplicabilidad del cuadro 2 en el que se detalla las posibles amenazas y evaluación de su probabilidad se realiza la comprobación del nivel de probabilidad de ocurrencia de amenazas.

Tabla 27. Comprobación de amenazas y vulnerabilidades gestión de soporte

N°	AREA DE EVALUACION	PROBABILIDAD	
		NIVEL	PUNTAJE
1	Red y recursos técnicos (Hardware y Software)	Alto	3
2	Procesos relacionados con la operación de tratamiento de datos	Medio	2
3	Diferentes partes involucradas en la operación de tratamiento de datos	Medio	2
4	Sector de actividad y escala del procesamiento	Baja	1
Probabilidad general de ocurrencia de amenazas		MEDIO 8	

Fuente: elaboración propia

- **Red y recursos técnicos (Hardware y Software)**

La probabilidad de ocurrencia de amenazas es **ALTO,** por lo que el sistema está conectado al internet y permite el acceso desde internet a los recursos internos y externos.

- **Procesos relacionados con la operación de tratamiento de datos**

La probabilidad de ocurrencia de amenazas es **MEDIA,** por lo que se asume que el proceso de la aplicación externa es claramente definido junto a las políticas establecidas para el procesamiento de los datos personales.

- **Diferentes partes involucradas en la operación de procesamiento**

La probabilidad de ocurrencia de amenazas es **MEDIA,** por que la operación de procesamiento de datos lo maneja una aplicación externa, por lo tanto, la empresa no tiene el control total de los datos.

- **Sector de actividad y escala del procesamiento**

La probabilidad de ocurrencia de amenazas es **BAJA,** por lo que la empresa toma medidas de seguridad en contra a los ataques cibernéticos por la operación de procesamiento que involucra a una gran cantidad de personas.

El resultado global de la probabilidad general de ocurrencia de amenazas se calcula como **MEDIA.**

Evaluación de Riesgo y Adopción de Medidas de Seguridad

En base a los resultados de la evaluación de impacto y la probabilidad de ocurrencia de amenazas, se realiza la evaluación de riesgos con la matriz anteriormente mencionada en el cuadro 3.

Cuadro 14. Evaluación de Riesgo y Adopción de Medidas de Seguridad

	NIVEL DE IMPACTO			
NIVEL DE PROBABILIDAD		BAJO	MEDIO	ALTO / MUY ALTO
	BAJO			
	MEDIO		X	
	ALTO			

Fuente: elaboración propia

El resultado de la evaluación de riesgos de gestión de clientes es considerado como **MEDIO**, lo cual se adapta medidas adecuadas para la prevención de riesgos.

- **Casos de uso: Área I+D**

Las operaciones de tratamiento más comunes que se considera en este informe son:

- **Gestión de Testeo de software**

Dentro de la gestión de Testeo de software se maneja datos personales de clientes registrados en su base de datos; el motivo de usar la base de datos del cliente es porque son cambios específicos solicitados por él.

El test de software requiere de datos como (cedula, ruc, correo, teléfono); al finalizar el test de software se elabora un informe con los resultados de los mismos con los cambios realizados, pendientes y próxima fecha de test.

Al final del mes se genera un informe general con todos los resultados de test y fecha de entrega del software ya operativo para la entrega al cliente.

Definición de la operación de procesamiento y su contexto

Para la operación de procesamiento de datos se detalla de la siguiente manera:

Cuadro 15. Operación de procesamiento Gestión de Testeo de Software

DATOS	TIPO DE DATO
Finalidad del tratamiento	Gestión de testeo de Software
Medios de procesamiento	Interno
Destinatario de los Datos	Interno
Procesador de datos utilizados	Interno
DATOS PERSONALES	
Nombre y Apellido Ruc / CI Nombre de la Compañía Correo electrónico Teléfono	Datos Personales Procesados
DATOS PERSONALES DEL JEFE DE I+D	
Nombre y Apellido Cargo Fecha de Test Resultados	Finalidad del tratamiento
Informe Estadístico Fecha de Entrega	

Fuente: elaboración propia

Con la información obtenida en la operación de tratamiento y su contexto se realiza una evaluación de impacto a los que están expuestos; los datos están expuestos a un cierto número de riesgos que afectan a la integridad, confidencialidad y disponibilidad.

Evaluación de Impacto

Para la evaluación de impacto el encargado de TI realiza la evaluación conforme a la Tabla 5 de la pérdida de confidencialidad, integridad y disponibilidad de los datos personales con la persona encargada del área de I+D de la empresa, donde se observa que los datos obtenidos de los clientes para realizar test de software no están seguros; el resultado del nivel de impacto de los datos personales a ser

tratados, el tratamiento a realizar, a su vez los resultados obtenidos es evaluado por la junta directiva de la empresa para la toma de decisiones.

El resultado final de la evaluación al área de I+D se toma Conforme a la tabla 6 de la evaluación de impacto se realiza el siguiente análisis:

Tabla 28. Evaluación de impacto de gestión de testeo de software

N°	EVALUACION DE IMPACTO		
1	Confidencialidad	Medio	2
2	Integridad	Medio	2
3	Disponibilidad	Baja	1
Evaluación de impacto General		MEDIO 8	

Fuente: elaboración propia

- **Pérdida de confidencialidad e integridad**

Dentro del alcance de la operación de gestión de test de software, la pérdida de confidencialidad e integridad se considera **MEDIA;** la posible divulgación no autorizada de datos, y alteración de los datos procesados genera inconvenientes significativos para la empresa.

- **Pérdida de disponibilidad**

Dentro del alcance de la operación de gestión de test de software, la pérdida de disponibilidad se considera **ALTA;** la posible eliminación no autorizada de datos procesados genera inconvenientes significativos e incluso la mala reputación para la empresa.

El resultado global de la evaluación del impacto los niveles de confidencialidad, integridad y disponibilidad se evalúa como **MEDIA**.

Comprobación de amenazas y vulnerabilidades

Mediante la aplicabilidad del cuadro 3 en el que se detalla las posibles amenazas y evaluación de su probabilidad se realiza la comprobación del nivel de probabilidad de ocurrencia de amenazas.

Tabla 29. Comprobación de amenazas y vulnerabilidades

N°	AREA DE EVALUACION	PROBABILIDAD	
		NIVEL	PUNTAJE
1	Red y recursos técnicos (Hardware y Software)	Bajo	1
2	Procesos relacionados con la operación de tratamiento de datos	Medio	2
3	Diferentes partes involucradas en la operación de tratamiento de datos	Medio	2
4	Sector de actividad y escala del procesamiento	Medio	1
Probabilidad general de ocurrencia de amenazas		MEDIO 6	

Fuente: elaboración propia

- **Red y recursos técnicos (Hardware y Software)**

La probabilidad de ocurrencia de amenazas es **BAJO,** por lo que el sistema para el test de software no es necesario la conexión a internet y aplicaciones de terceros.

- **Procesos relacionados con la operación de tratamiento de datos**

La probabilidad de ocurrencia de amenazas es **MEDIA,** por lo que se asume que el proceso de la aplicación externa es claramente definido junto a las políticas establecidas para el procesamiento de los datos personales.

- **Diferentes partes involucradas en la operación de procesamiento**

La probabilidad de ocurrencia de amenazas es **MEDIA,** por que la operación de procesamiento de datos lo maneja una aplicación externa, por lo tanto, la empresa no tiene el control total de los datos.

- **Sector de actividad y escala del procesamiento**

La probabilidad de ocurrencia de amenazas es **BAJA,** por lo que la empresa toma medidas de seguridad en contra a los ataques cibernéticos por la operación de procesamiento que involucra a una gran cantidad de personas.

El resultado global de la probabilidad general de ocurrencia de amenazas se calcula como **MEDIA.**

Evaluación de Riesgo y Adopción de Medidas de Seguridad

En base a los resultados de la evaluación de impacto y la probabilidad de ocurrencia de amenazas, se realiza la evaluación de riesgos con la matriz anteriormente mencionada en el cuadro 3.

Cuadro 16. Evaluación de Riesgo y Adopción de Medidas de Seguridad

	NIVEL DE IMPACTO			
NIVEL DE PROBABILIDAD		BAJO	MEDIO	ALTO / MUY ALTO
	BAJO			
	MEDIO	X		
	ALTO			

Fuente: elaboración propia

El resultado de la evaluación de riesgos de gestión de test de usuarios es considerado como **MEDIO**, lo cual se adapta medidas adecuadas para la prevención de riesgos.

- **Casos de uso: seguridad física/control de acceso**

Las operaciones de tratamiento más comunes que se considera en este informe son:

- **Gestión de Control de Acceso**

Dentro de la gestión de control de acceso se maneja datos personales de sus empleados para el control de acceso físico dentro de las instalaciones, con el fin de garantizar que el personal autorizado tenga acceso.

El sistema de control de acceso implementado en la empresa es el Reloj Biométrico Facial instalado en un punto especifico interconectado con la plataforma de gestión de control de asistencia. Cada empleado al asumir sus responsabilidades es registrado en la plataforma de gestión de asistencia y se le asigna un código para que sea almacenado en el registro del biométrico. Los datos personales utilizados durante el registro incluyen nombre y apellido, cedula, fecha de ingreso, puesto dentro de la organización y registro facial.

Cada vez que un empleado cumpla su jornada de trabajo registra la asistencia y al acceso a la empresa; al finalizar el mes el encargado de la gestión de control de acceso genera un informe de los empleados ingresados y novedades de asistencia.

Definición de la operación de procesamiento y su contexto

Para la operación de procesamiento de datos se detalla de la siguiente manera:

Cuadro 17. Operación de procesamiento Control de Acceso

DATOS	TIPO DE DATO
Finalidad del tratamiento	Gestión control de acceso
Medios de procesamiento	Interno
Destinatario de los Datos	Interno
Procesador de datos utilizados	Interno
DATOS PERSONALES	
Id Nombre y Apellido CI Fecha de ingreso Cargo / Puesto Registro Facial	Datos Personales Procesados
DATOS PERSONALES DEL ENCARGADO DEL CONTROL DE ACCESO	
Nombre y Apellido Cargo Resultados	Finalidad del tratamiento
Informe Estadístico Fecha de Entrega	

Fuente: elaboración propia

Con la información obtenida en la operación de tratamiento y su contexto se realiza una evaluación de impacto a los que están expuestos; los datos están expuestos a un cierto número de riesgos que afectan a la integridad, confidencialidad y disponibilidad.

Evaluación de Impacto

Para la evaluación de impacto el encargado de TI realiza la evaluación conforme a la Tabla 5 de la pérdida de confidencialidad, integridad y disponibilidad de los datos personales con la persona encargada del control de acceso de la empresa, donde se observa que los datos registrados en el reloj biométrico de los empleados no están seguros; el resultado del nivel de impacto de los datos personales a ser tratados, el tratamiento a realizar, a su vez los resultados obtenidos es evaluado por la junta directiva de la empresa para la toma de decisiones.

El resultado final de la evaluación del control de acceso se toma conforme a la tabla 6 de la evaluación de impacto se realiza el siguiente análisis:

Tabla 30. Evaluación de impacto de control de acceso

N°	EVALUACION DE IMPACTO		
1	Confidencialidad	Bajo	1
2	Integridad	Bajo	1
3	Disponibilidad	Baja	1
Evaluación de impacto General		BAJO 3	

Fuente: elaboración propia

- **Pérdida de confidencialidad, integridad y disponibilidad**

Dentro del alcance de la operación de gestión de control de acceso, la pérdida de confidencialidad, integridad y disponibilidad se considera **BAJA;** el personal que tenga inconvenientes de registro es superados sin mayor esfuerzo.

El resultado global de la evaluación del impacto los niveles de confidencialidad, integridad y disponibilidad se evalúa como **BAJA**.

Comprobación de amenazas y vulnerabilidades

Mediante la aplicabilidad del cuadro 2 en el que se detalla las posibles amenazas y evaluación de su probabilidad se realiza la comprobación del nivel de probabilidad de ocurrencia de amenazas.

Tabla 31. Comprobación de amenazas y vulnerabilidades

N°	AREA DE EVALUACION	PROBABILIDAD	
		NIVEL	PUNTAJE
1	Red y recursos técnicos (Hardware y Software)	Media	2
2	Procesos relacionados con la operación de tratamiento de datos	Bajo	1
3	Diferentes partes involucradas en la operación de tratamiento de datos	Bajo	1
4	Sector de actividad y escala del procesamiento	Bajo	1
Probabilidad general de ocurrencia de amenazas		BAJO 5	

Fuente: elaboración propia

- **Red y recursos técnicos (Hardware y Software)**

La probabilidad de ocurrencia de amenazas es **MEDIO,** lo que el sistema requiere la conexión a la red interna de la empresa para el registro de los datos.

- **Procesos relacionados con la operación de tratamiento de datos**

La probabilidad de ocurrencia de amenazas es **BAJA,** por lo que se asume que el proceso de control de acceso es claramente definido junto a las políticas establecidas para el procesamiento de los datos personales.

- **Diferentes partes involucradas en la operación de procesamiento**

La probabilidad de ocurrencia de amenazas es **BAJA,** por lo que el oficial de seguridad no transfiere, almacena o procesa datos personales fuera de la organización, mientras que el uso aceptable de la red, el sistema y los recursos físicos dentro de la empresa está claramente definido.

- **Sector de actividad y escala del procesamiento**

La probabilidad de ocurrencia de amenazas es **BAJA,** por lo que la empresa toma medidas de seguridad en contra a los ataques cibernéticos por la operación de procesamiento que involucra a una gran cantidad de personas.

El resultado global de la probabilidad general de ocurrencia de amenazas se calcula como **BAJA.**

Evaluación de Riesgo y Adopción de Medidas de Seguridad

En base a los resultados de la evaluación de impacto y la probabilidad de ocurrencia de amenazas, se realiza la evaluación de riesgos con la matriz anteriormente mencionada en el cuadro 3.

Cuadro 18. Evaluación de Riesgo y Adopción de Medidas de Seguridad

	NIVEL DE IMPACTO			
NIVEL DE PROBABILIDAD		BAJO	MEDIO	ALTO / MUY ALTO
	BAJO	X		
	MEDIO			
	ALTO			

Fuente: elaboración propia

El resultado de la evaluación de riesgos de gestión de control de acceso es considerado como **BAJO**, lo cual se adapta medidas adecuadas para la prevención de riesgos.

3.3. Establecer KPI de medidas de seguridad

- **Medidas Propuestas para Nivel de Riesgo Bajo**

Cuadro 19. Controles de medida de seguridad riesgo bajo

CATEGORÍA	DESCRIPCIÓN	CONTROLES ISO 27001
Política de seguridad y procedimientos de protección de datos personales	La organización documenta su política con respecto al procesamiento de datos personales como parte de su política de seguridad de la información.	5.1.1 Políticas para la seguridad de la información
	La política de seguridad se revisa y aprueba, si es necesario, anualmente.	5.1.2 Revisión de las políticas de seguridad de la información
Funciones y responsabilidades	Las funciones y responsabilidades relacionadas con el procesamiento de datos personales están claramente definidas y asignadas de acuerdo con la política de seguridad	6.1.1 Funciones y responsabilidades de la Seguridad de la información
	Durante las reorganizaciones internas o despidos y cambios de empleo, la revocación de derechos y responsabilidades con los respectivos procedimientos de traspaso están claramente definidos.	6.1.1 Funciones y responsabilidades de la Seguridad de la información 6.1.2 Separación de funciones
Política de control de acceso	Asignar derechos de control de acceso específicos a cada rol (involucrado en el procesamiento de datos personales).	9.1.1 Política de control de acceso
Gestión de recursos/activos	La organización tiene un registro de los recursos de TI utilizados para el procesamiento de datos personales (hardware, software y red).	8.1.1 Inventario de activos

	El registro incluye la información necesaria como: tipo, ubicación, persona asignada.	8.1.2 Propiedad de los activos
Gestión del cambio	La organización se asegura de que todos los cambios en el sistema de TI sean registrados y supervisados por una persona específica. Se realiza un seguimiento regular de este proceso.	12.1.1 Procedimientos documentados de operación
	El desarrollo de software se realiza en un entorno de pruebas que no esté conectado al sistema de TI. Cuando se necesitan pruebas, se usa datos ficticios (no datos reales). En los casos en que esto no sea posible, existen procedimientos específicos para la protección de los datos personales utilizados en las pruebas.	12.1.4 Separación de los ambientes para desarrollo, prueba y operación
Procesadores de datos	Se define, documenta directrices y procedimientos formales que cubran el procesamiento de datos personales por parte de los procesadores de datos (contratistas/ subcontratación) entre el controlador de datos y el procesador de datos antes del comienzo de las actividades de procesamiento. Estas directrices y procedimientos se establece obligatoriamente el mismo nivel de seguridad de los datos personales que establece la política de seguridad de la organización.	15.1.1 Política de seguridad de la información para las relaciones con los proveedores
	Al enterarse de una violación de datos personales, el procesador de datos notifica al controlador sin demora indebida.	15.1.2 Tener en cuenta la seguridad en los acuerdos con proveedores
Tratamiento de incidencias / violaciones de datos personales	Definir un plan de respuesta a incidentes con procedimientos detallados para garantizar una respuesta ordenada a las incidencias relativas a datos personales	16.1.5 Respuesta a incidentes de seguridad de la información
	Las violaciones de datos personales son informadas inmediatamente a la alta gerencia.	16.1.2 Reporte de eventos de seguridad de la información
Continuidad del negocio	La organización establece los principales procedimientos y controles a seguir para asegurar el nivel requerido de continuidad y disponibilidad del sistema de TI que procesa datos personales (en caso de incidente/violación de datos personales).	17.1.1 Planificación de la continuidad de la seguridad de la información
Confidencialidad del personal	La organización se asegura de que todos los empleados comprendan sus responsabilidades y obligaciones relacionadas con el procesamiento de datos personales. Los roles y responsabilidades se comunican claramente durante el proceso previo al empleo y/o de inducción.	7 seguridad relativa a los recursos

Control de Acceso y autenticación	Se implementa un sistema de control de acceso aplicable a todos los usuarios que acceden al sistema de TI. El sistema permite crear, aprobar, revisar y eliminar cuentas de usuario.	9.1.1 Política de control de acceso
	El uso de cuentas de usuario repetidos es evitado, en caso de ser necesario, se garantiza que todos los usuarios en común tienen los mismos roles y responsabilidades.	9.2.2 Gestión de los derechos de acceso asignados a usuarios
	Un mecanismo de autenticación es utilizar una combinación de nombre de usuario y contraseña. Las contraseñas respetan un cierto nivel de complejidad.	9.4.3 Gestión de contraseñas de usuario.
	El sistema de control de acceso tiene la capacidad de detectar y no permitir el uso de contraseñas que no respeten un determinado nivel de complejidad.	9.4.3 Gestión de contraseñas de usuario.
Registro y monitoreo	Los archivos de registro se activan para cada aplicación utilizada para el procesamiento de datos personales. Incluir todos los tipos de acceso a los datos (ver, modificar, borrar).	12.4.2 Protección de los registros de información.
	Los archivos de registro tienen una marca de tiempo y están adecuadamente protegidos contra la manipulación y el acceso no autorizado.	12.4.2 Protección de los registros de información.
Seguridad del servidor/base de datos	Los servidores de bases de datos y aplicaciones se configuran para ejecutarse con una cuenta separada, con privilegios mínimos de sistema operativo para funcionar correctamente.	12.1 Responsabilidades y procedimientos de operación.
	Los servidores de bases de datos y aplicaciones solo procesan los datos personales que realmente se necesitan procesar.	12.1 Responsabilidades y procedimientos de operación.
Seguridad de la Estación de Trabajo	Los usuarios no acceden a desactivar o eludir la configuración de seguridad.	14.1.1 Análisis y especificación de los requisitos de seguridad
	Las aplicaciones antivirus y las firmas de detección se configuran semanalmente.	14.2 Seguridad en los procesos de desarrollo y soporte
	Los usuarios no cuentan con privilegios para instalar o desactivar aplicaciones no autorizadas.	14.2 Seguridad en los procesos de desarrollo y soporte
	El sistema tiene tiempos de espera de sesión cuando el usuario no ha estado activo durante un período de tiempo determinado.	14.1.1 Análisis y especificación de los requisitos de seguridad
Seguridad de red/comunicación	El acceso que realice a través de Internet, la comunicación esta encriptada mediante protocolos criptográficos (TLS/SSL).	13.1 Gestión de la seguridad en las redes

Copias de Seguridad	Los procedimientos de copia de seguridad y restauración de datos son definidos, documentados y vinculados claramente a las funciones y responsabilidades.	12.3.1 Copias de seguridad de la información
	Las copias de seguridad reciben un nivel adecuado de protección física y ambiental de acuerdo con los estándares aplicados a los datos de origen	12.3 Copias de seguridad
	Se monitorea la ejecución de las copias de seguridad para garantizar que estén completas.	12.3 Copias de seguridad
	Se realiza copias de seguridad completas con regularidad.	12.3.1 Copias de seguridad de la información
Dispositivos móviles/portátiles	Los procedimientos de gestión de dispositivos móviles y portátiles están definidos y documentados se establece reglas claras para su uso adecuado.	6.2 Dispositivos para movilidad y teletrabajo
	Los dispositivos móviles que tienen permitido el acceso al sistema de información son preregistrados y preautorizados.	6.2 Dispositivos para movilidad y teletrabajo
	Los dispositivos móviles están sujetos a los mismos niveles de procedimientos de control de acceso (al sistema de procesamiento de datos) que otros equipos terminales.	6.2 Dispositivos para movilidad y teletrabajo
Seguridad del ciclo de vida de la aplicación	Los requisitos de seguridad específicos se definen durante las primeras etapas del ciclo de vida del desarrollo.	14.2 Seguridad en los procesos de desarrollo y soporte
	Las tecnologías y técnicas específicas diseñadas para respaldar la privacidad y la protección de datos (también denominadas Tecnologías de mejora de la privacidad (PET)) se adoptan a los requisitos de seguridad.	12.6 Gestión de la vulnerabilidad técnica
	Seguir los estándares y prácticas de codificación segura.	14.2 Seguridad en los procesos de desarrollo y soporte
	Durante el desarrollo, se realiza pruebas y validaciones contra la implementación de los requisitos de seguridad iniciales.	12.6 Gestión de la vulnerabilidad técnica
Eliminación de datos	La sobreescritura basada en software se realiza en todos los medios antes de desecharlos. En los casos en que esto no sea posible (Nas, Discos Externos, Usb, etc.) se realiza la destrucción física.	11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento 8.3.2 Eliminación de soportes
	Se procede a la trituración del papel y soportes portátiles utilizados para el almacenamiento de datos personales.	11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento 8.3.2 Eliminación de soportes

Seguridad física	El acceso físico de la infraestructura del sistema de TI no es accesible por personal no autorizado.	11.1 Áreas seguras.

Fuente: elaboración propia

- **Medidas Propuestas para Nivel de Riesgo Medio**

Cuadro 20. Controles de medida de seguridad riesgo medio

CATEGORÍA	DESCRIPCIÓN	MEDIDA DE SEGURIDAD POR RIESGO
Política de seguridad y procedimientos de protección de datos personales	La organización documenta una política de seguridad dedicada por separado con respecto al procesamiento de datos personales. La política es aprobada por la gerencia y comunicada a todos los empleados y partes externas relevantes.	5. Políticas de seguridad.
	La política de seguridad hace referencia al menos a: las funciones y responsabilidades del personal, las medidas técnicas y organizativas básicas adoptadas para la seguridad de los datos personales, los encargados del tratamiento u otros terceros que intervengan en el tratamiento de los datos personales.	5. Políticas de seguridad.
	Crear y mantener un inventario de políticas / procedimientos específicos relacionados con la seguridad de los datos personales, con base en la política general de seguridad.	5. Políticas de seguridad.
Funciones y responsabilidades	Realizar una designación clara de las personas a cargo de tareas específicas de seguridad, incluido el nombramiento de un oficial de seguridad.	6.1.1 Asignación de responsabilidades para la segur. de la información.
Política de control de acceso	Una política de control de acceso es detallada y documentada. La organización determina en este documento las reglas de control de acceso apropiadas, los derechos de acceso y las restricciones para roles de usuario específicos hacia los procesos y procedimientos relacionados con los datos personales.	9.1.1 Política de control de accesos.
	La segregación de funciones de control de acceso es claramente definida y documentada.	9.1.1 Política de control de accesos.
Gestión de recursos/activos	Los roles que tienen acceso a ciertos recursos son definidos y documentados.	8. Gestión de activos.
Gestión del cambio	Existe una política de cambios detallada y documentada.	12.1 Responsabilidades y procedimientos de operación.

Procesadores de datos	La organización del controlador de datos es auditada regularmente el cumplimiento del procesador de datos con el nivel acordado de requisitos y obligaciones.	15.1 Seguridad de la información en las relaciones con suministradores.
Tratamiento de incidencias / violaciones de datos personales	El plan de respuesta a incidentes está documentada, incluida una lista de posibles acciones de mitigación y una asignación clara de roles.	16.1 Gestión de incidentes de seguridad de la información y mejoras.
Continuidad del negocio	Un BCP es detallado y documentado en el que se incluye acciones claras y asignación de roles.	17.1 Continuidad de la seguridad de la información
	Se define un nivel de calidad de servicio garantizada en el BCP para los procesos comerciales centrales que brindan seguridad a los datos personales.	17.1 Continuidad de la seguridad de la información
Confidencialidad del personal	Antes de asumir sus funciones, se solicita a los empleados que revisen y acuerden la política de seguridad de la organización y firmen los respectivos acuerdos de confidencialidad y no divulgación.	7. Seguridad ligada a los recursos humanos.
Capacitación	La organización asegura que todos los empleados estén adecuadamente informados sobre los controles de seguridad del sistema de TI que se relacionan con su trabajo diario. Los empleados involucrados en el procesamiento de datos personales también están debidamente informados sobre los requisitos de protección de datos y las obligaciones legales pertinentes a través de campañas periódicas de concienciación.	7.2.2 Concienciación, educación y capacitación en seguridad de la información.
Control de Acceso y autenticación	Se define y documenta una política de contraseñas específica. La política incluye al menos la longitud de la contraseña, la complejidad, el período de validez, así como la cantidad de intentos de inicio de sesión fallidos aceptables.	9.4 Control de acceso a sistemas y aplicaciones.
	Las contraseñas de los usuarios se almacenan en forma de "hash".	9.4.3 Gestión de contraseñas de usuario.
Registro y monitoreo	Se registran las acciones de los administradores y operadores del sistema, incluida la adición /eliminación /cambio de usuario.	12.4 Registro de actividad y supervisión.
	No establecer la posibilidad de eliminación o modificación del contenido de los archivos de registro. El acceso a los archivos de registro también se registra, además, de monitorear para detectar actividad inusual.	12.4 Registro de actividad y supervisión.

	Un sistema de monitoreo procesa los archivos de registro y producir informes sobre el estado del sistema y notificar sobre posibles alertas.	12.4 Registro de actividad y supervisión.
Seguridad del servidor/base de datos	Las soluciones de cifrado se consideran en archivos o registros específicos a través de la implementación de software o hardware.	12.1 Responsabilidades y procedimientos de operación.
	Se considera el cifrado de unidades de almacenamiento.	10. Cifrado.
	Aplicar técnicas de seudonomización al separar los datos de los identificadores directos para evitar vinculación al interesado sin información adicional	10. Cifrado.
Seguridad de la Estación de Trabajo	Las actualizaciones de seguridad críticas publicadas por el desarrollador del sistema operativo se instala periódicamente.	14. Adquisición, desarrollo y mantenimiento de los sistemas de información.
Seguridad de red/comunicación	El acceso inalámbrico al sistema de TI permite solo para usuarios y procesos específicos. Estar protegido por mecanismos de encriptación.	13. Seguridad en las telecomunicaciones.
	Se evita el acceso remoto al sistema de TI. En los casos en que esto sea absolutamente necesario, se realiza bajo el control y seguimiento de una persona específica de la organización	13. Seguridad en las telecomunicaciones.
Copias de Seguridad	Las copias de la copia de seguridad se almacenan de forma segura en diferentes ubicaciones.	12.3 Copias de seguridad.
	Los medios de respaldo se prueban regularmente para garantizar que se confié en ellos para uso de emergencia.	12.3 Copias de seguridad.
	En caso de que se utilice un servicio de terceros para el almacenamiento de copias de seguridad, la copia es cifrada antes de ser transmitida desde el controlador de datos.	12.3 Copias de seguridad.
Dispositivos móviles/portátiles	La organización borra de forma remota los datos personales (relacionados con su operación de procesamiento) en un dispositivo móvil que haya sido comprometido.	6.2 Dispositivos para movilidad y teletrabajo.
	Los dispositivos móviles admiten la separación del uso privado y comercial del dispositivo a través de contenedores de software seguros.	6.2 Dispositivos para movilidad y teletrabajo.
	Los dispositivos móviles están físicamente protegidos contra robos cuando no estén en uso.	6.2 Dispositivos para movilidad y teletrabajo.

Seguridad del ciclo de vida de la aplicación	La evaluación de vulnerabilidades, las pruebas de penetración de aplicaciones e infraestructuras son realizadas por un tercero de confianza antes de la adopción operativa. La solicitud no se acepta a menos que se alcance el nivel de seguridad requerido.	12.6 Gestión de la vulnerabilidad técnica y 14.2 Seguridad en los procesos de desarrollo y soporte.
	Se realiza pruebas de penetración periódicas.	12.6 Gestión de la vulnerabilidad técnica y 14.2 Seguridad en los procesos de desarrollo y soporte.
	Los parches de software son probados y evaluados antes de instalarlos en un entorno operativo.	12.6 Gestión de la vulnerabilidad técnica y 14.2 Seguridad en los procesos de desarrollo y soporte.
Eliminación de datos	Si se utilizan los servicios de un tercero para eliminar de forma segura los medios o los registros en papel, existe un acuerdo de servicio y existe un registro de destrucción de registros.	8.3.2 Eliminación de soportes y 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento
Seguridad física	Establece una identificación clara, a través de medios apropiados, por ejemplo, tarjetas de identificación, para todo el personal y los visitantes que accedan a las instalaciones de la organización, según corresponda.	11. Seguridad física y ambiental.
	Definir zonas seguras y estar protegido por controles de entrada apropiados.	11.1 Áreas seguras.
	Instalar sistemas de detección de intrusos en todas las zonas de seguridad.	11.1 Áreas seguras.
	Implementar en el servidor un sistema automático de supresión de incendios, un sistema de aire acondicionado dedicado de control cerrado y un sistema de alimentación ininterrumpida (UPS).	11.1 Áreas seguras.
	El personal externo del servicio de apoyo cuenta con acceso restringido a las áreas seguras.	11. Seguridad física y ambiental.

Fuente: elaboración propia

- **Medidas Propuestas para Nivel de Riesgo Alto**

Cuadro 21. Controles de medida de seguridad riesgo alto

CATEGORÍA	DESCRIPCIÓN	MEDIDA DE SEGURIDAD POR RIESGO
Política de seguridad y procedimientos de protección de datos personales	La política de seguridad se revisa semestralmente.	5. Política de seguridad

Funciones y responsabilidades	Las tareas y responsabilidades del responsable de seguridad están claramente establecidas y documentadas.	6.1.1 Roles y responsabilidades de seguridad de la información
Política de control de acceso	Los roles con derechos de acceso excesivos se definen claramente y asignados a miembros específicos limitados del personal.	9.1.1 Política de control de acceso
Gestión de recursos/activos	Los recursos de TI son revisados y actualizados anualmente.	8. Gestión de activos
Procesadores de datos	Los empleados que procesan datos personales están sujetos a acuerdos específicos de confidencialidad/ no divulgación documentados.	15. Relaciones con suministradores.
Tratamiento de incidencias / violaciones de datos personales	Los incidentes y las violaciones de datos personales son registrados junto con los detalles sobre el evento y las acciones de mitigación posteriores realizadas.	16. Gestión de incidentes de seguridad de la información
Continuidad del negocio	Designar el personal específico con la responsabilidad, autoridad y competencia necesarias para gestionar la continuidad del negocio en caso de incidente/ violación de datos personales.	17. Aspectos de seguridad de la información en la gestión de La continuidad del negocio.
	Considerar una instalación alternativa, según la organización y el tiempo de inactividad aceptable del sistema de TI.	17.1 Continuidad de la seguridad de la información
Confidencialidad del personal	Los empleados involucrados en el procesamiento de datos personales de alto riesgo están sujetos a cláusulas de confidencialidad específicas (en virtud de su contrato de trabajo u otro acto legal).	7. Seguridad ligada a los recursos humanos.
Capacitación	Preparar y ejecutar anualmente un plan de capacitación con metas y objetivos definidos.	7.2.2 Concienciación, educación y capacitación en seguridad de la información
Control de Acceso y autenticación	Autenticación de doble factor es utilizado preferentemente para acceder a sistemas que procesan datos personales. Los factores de autenticación son contraseñas, tokens de seguridad, token secreto, biometría, etc.	9. Control de acceso
Seguridad del servidor/base de datos	Aplicar técnicas que respaldan la privacidad a nivel de base de datos.	12. Seguridad de las operaciones
Seguridad de la Estación de Trabajo	El cifrado de disco completo está habilitado en las estaciones de trabajo.	14.1 Requisitos de seguridad de los sistemas de información
	Las estaciones de trabajo utilizadas para el procesamiento de datos personales conectadas a Internet, aplicar medidas de seguridad para evitar el procesamiento, la copia y la transferencia no autorizados de datos personales almacenados.	14.1 Requisitos de seguridad de los sistemas de información

Seguridad de red/comunicación	No permitir la conexión a Internet a los servidores y estaciones de trabajo utilizados para el procesamiento de datos personales.	13.Seguridad de las comunicaciones
Copias de Seguridad	Las copias de las copias de seguridad son cifrados y almacenados de forma segura fuera de línea.	12.3 Copias de seguridad.
Dispositivos móviles/portátiles	Aplicar doble factor de autenticación para acceder a dispositivos móviles	6.2 Dispositivos para movilidad y teletrabajo.
	Los datos personales almacenados en los dispositivos móviles están encriptado.	6.2 Dispositivos para movilidad y teletrabajo.
Eliminación de datos	Si se utiliza un tercero, por lo tanto, el procesador de datos, para la destrucción de medios o archivos en papel, se considera que el proceso se lleva a cabo en las instalaciones del controlador de datos (y evitar la transferencia de datos personales fuera del sitio).	8.3.2 Eliminación de medios y 11.2.7 Eliminación segura o reutilización de equipos

Fuente: elaboración propia

CONCLUSIONES

- La documentación de los artículos científicos enfocados en la seguridad de datos personales existentes en el estado del arte actual refuerza el conocimiento obtenido para aplicar las políticas, controles y medidas de seguridad de la protección de datos personales en la empresa.

- El diagnóstico de la situación actual de la seguridad de datos personales en la empresa Fenix Corp ayuda a identificar las falencias y posibles riesgos con los que cuenta en la organización.

- La aplicación de las herramientas diseñadas para la seguridad de datos personales ayuda a proteger los datos personales que almacenan las empresas, por ende, se establece medidas de seguridad para la protección de los datos.

- La compilación de los datos obtenidos en las herramientas metodológicas de seguridad de datos personales pone en manifiesto las posibles amenazas que se toma en consideración ante la pérdida de información personal; en el que se expone la confidencialidad, disponibilidad e integridad de los datos personales.

RECOMENDACIONES

- Se recomienda a la alta gerencia de la empresa Fenix Corp, realizar capacitaciones de concientización acerca de la información que se maneja internamente, a fin de que el personal genere una cultura de la gravedad de exponer los datos personales.

- Se recomienda realizar una auditoria cada seis meses para validar el cumplimiento de las medidas de seguridad de los niveles de riesgo establecidas en los controles de la ISO/IEC 27002 de la seguridad de la información.

- Se recomienda mantener planes de mejora e implementación de medidas y controles de seguridad y respuesta a incidentes a fin de elevar la protección de los datos personales que maneja la empresa Fenix Corp.

- Se recomienda implementar la herramienta metodológica basadas en las normas ISO/IEC 27001, 27002 y 27701 enfocada en la gestión de la seguridad de la información y de la privacidad en las empresas.

BIBLIOGRAFÍA

Abreu, J. L. (2014). *El Método de la Investigación. Research Method - PDF Free Download*. https:// docplayer. es/ 21252848- El- metodo- de- la-investigacion-research-method.html

Álvarez, L. E. (2017). *Paradigmas de la protección de datos personales en Ecuador. Análisis del proyecto de Ley Orgánica de Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales*. 19.

Becerra, A., & González, N. (s. f.). *Dirección general de prevención y autorregulación*. 102.

Drummond, V. (2004). *Internet, privacidad y datos personales* | (2004.ª ed.). Editorial Reus. http://www.marcialpons.es/libros/internet-privacidad-y-datos-personales/9788429014075/

ENISA. (2017, diciembre). *Handbook on Security of Personal Data Processing* [Report/Study]. ENISA. https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing

Espinosa, J. A. N. (2017). *Magíster en Auditoría de Tecnologías de la Información*. 16.

Gómez-Córdoba, A. I., Arévalo-Leal, S., Bernal-Camargo, D. R., & Rosero de los Ríos, D. (2020). *El derecho a la protección de datos personales, tecnologías digitales y pandemia* por COVID-19 en Colombia. Revista de Bioética y Derecho, 50, 271-294. https://doi.org/10.1344/rbd2020.50.31830

Guerrero Guerrero, B. (2020). *Protección de datos personales en el Poder Judicial*. Revista Chilena De Derecho Y Tecnología. https:// rchdt. uchile. cl/ index. php/RCHDT/article/view/54372/64361

Instituto Nacional de Ciberseguridad. (2020). Proteccion de la informacion. *2020*, 33.

ISO 27701: Sistema de gestión de cumplimiento del RGPD. (2021). Organismo de certificación global. https:// www. nqa. com/ es- co/ certification/ estándar ds/iso-

La protección de datos de las empresas y de los usuarios—El Comercio. (2021, noviembre 24). EL COMERCIO. https://www.elcomercio.com/blogs/solo-para-empresas-y-emprendedores/ley-proteccion-datos-empresas-usuarios.html

Ley-Organica-de-Datos-Personales.pdf. (2021). Recuperado 27 de diciembre de 2021, de https:// www. telecomunicaciones. gob. ec/ wp-content/ uploads/ 2021/06/Ley-Organica-de-Datos-Personales.pdf

Maqueo Ramírez, M. S., Moreno González, J., & Recio Gayo, M. (2017). *Protección de datos personales, privacidad y vida privada: La inquietante búsqueda de un equilibrio global necesario. Revista de derecho (Valdivia)*, *30*(1), 77-96. https://doi.org/10.4067/S0718-09502017000100004

Meraz Espinoza, A. I. (2018b). *Empresa y privacidad: El cuidado de la información y los datos personales en medios digitales*. *Revista ius*, *12*(41). https://doi.org/10.35487/rius.v12i41.2018.313

Moreno, P. S. (s. f.). *Ecuador y la nueva ley de protección de datos*. 4.

Nuñez, E. (2007). La importancia de la protección de datos de carácter personal en las relaciones comerciales. Aproximación al Derecho venezolano. *Revista de Derecho Privado, ISSN 0123-4366, Nº. 12-13, 2007*.

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. (2020). Recuperado 2 de diciembre de 2021, de https:// www. oecd. org/sti/ieconomy/15590267.pdf

Ortiz, A. I. H. (1998). *La violación de la intimidad en la protección de datos personales*. Dykinson. https://dialnet.unirioja.es/servlet/libro?codigo=102769

Payton, T. M., & Claypoole, T. (2015). *Privacy in the age of big data*. https:// www. agapea. com/ libros/ Privacy- in- the- Age -of- Big- Data-978 144 224 2579-i.htm

Paz Canales, M., & Bordachar, M. (2021, enero 22). *Protección de datos personales en Ecuador: El momento es ahora*. Derechos Digitales. https:// www. derechosdigitales.org/15138/proteccion-de-datos-personales-en-ecuador-el-momento-es-ahora/

Roca, A. P. (2020). El derecho a la protección de datos personales y su reflejo en el consentimiento del interesado. *Revista de Derecho Político*, *108*, Art. 108. https://doi.org/10.5944/rdp.108.2020.27998

Solutions, G. (2019, septiembre 3). Nueva ISO / IEC 27701: 2019. *GlobalSuite Solutions*. https://www.globalsuitesolutions.com/es/iso-iec-27701-2019/

Vilches, C. (2021). *Biblioguias: Gestión de datos de investigación: Protección de los datos*. Recuperado 21 de noviembre de 2021, de https:// biblioguias. cepal. org/c.php?g=495473&p=4398118

ANEXOS

ANEXO 1. Ley de protección de datos

- **Capítulo VI: SEGURIDAD DE DATOS PERSONALES**

Ar. 37.- Seguridad de datos personales. El responsable o encargado del tratamiento de datos personales según sea el caso, deberá sujetarse al principio de seguridad de datos personales, para lo cual deberá tomar en cuenta las categorías y volumen de datos personales, el estado de la técnica, mejores prácticas de seguridad integral y los costos de aplicación de acuerdo a la naturaleza, alcance, contexto y los fines del tratamiento, así como identificar la probabilidad de riesgos,
El responsable o encargado del tratamiento de datos personales, deberá implementar un proceso de verificación, evaluación y valoración continua y permanente de la eficiencia, eficacia y efectividad de las medidas de carácter técnico, organizativo y de cualquier otra índole, implementadas con el objeto de garantizar y mejorar la seguridad del tratamiento de datos personales,
El responsable o encargado del tratamiento de datos personales deberá evidenciar que las medidas adoptadas e implementadas mitiguen de forma adecuada los riesgos identificados

¡Entre otras medidas, se podrán incluir las siguientes;

1) Medidas de anonimización, seudonomización o cifrado de datos personales;

2) Medidas dirigidas a mantener la confidencialidad, integridad y disponibilidad permanentes de los sistemas y servicios del tratamiento de datos personales y el acceso a los datos personales, ¡de forma rápida en caso de incidentes; y

3) Medidas dirigidas a mejorar la resiliencia técnica, física, administrativa, y jurídica.

4) Los responsables y encargados del tratamiento de datos personales, podrán acogerse a estándares internacionales para una adecuada gestión de riesgos enfocada a la protección de derechos y libertades, así como para la implementación y manejo de sistemas de seguridad de la información o a códigos de conducta reconocidos y autorizados por la Autoridad de Protección de Datos Personales.

Art. 38.- Medidas de seguridad en el ámbito del sector público. El mecanismo gubernamental de seguridad de la información deberá incluir las medidas que deban implementarse en el caso de tratamiento de datos personales para hacer frente a cualquier nesgo, amenaza, vulnerabilidad, accesos no autorizados, pérdidas, alteraciones, destrucción o comunicación accidental o ilícita en el tratamiento de los datos conforme al principio de seguridad de datos personales.

El mecanismo gubernamental de seguridad de la información abarcará y aplicará a todas las instituciones del sector público, contenidas en el artículo 225 de la Constitución de la República de Ecuador, así como a terceros que presten servicios públicos mediante concesión, u otras figuras legalmente reconocidas. Estas, podrán incorporar medidas adicionales al mecanismo gubernamental de seguridad de la información.

Art. 39.- Protección de datos personales desde el diseño y por defecto. Se entiende a la protección de datos desde el diseño como el deber del responsable del tratamiento de tener en cuenta, en las primeras fases de concepción y diseño del proyecto, que determinados tipos de tratamientos de datos personales entrañan una serie de riesgos para los derechos de los titulares en atención al estado de la técnica, naturaleza y fines del tratamiento, para lo cual, implementará las medidas técnicas, organizativas y de cualquier otra Índole, con miras a garantizar el cumplimiento de las obligaciones en materia de protección de datos, en los términos del reglamento.

La protección de datos por defecto hace referencia a que el responsable debe aplicar las medidas técnicas y organizativas adecuadas con miras a que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines del tratamiento, en los términos del reglamento. **Art. 40.- Análisis de riesgo, amenazas y vulnerabilidades.** Para el análisis de riesgos, amenazas y vulnerabilidades, ¡el responsable y el encargado del tratamiento de los datos personales deberán utilizar una metodología que considere, entre otras;

1) Las particularidades del tratamiento;
2) Las particularidades de las partes involucradas; y,
3) Las categorías y el volumen de datos personales objeto de tratamiento.

Art. 41.- Determinación de medidas de seguridad aplicables. Para determinar las medidas de seguridad, aceptadas por el estado de la técnica,a las que están

obligadas el responsable y el encargado del tratamiento de los datos personales, se deberán tomar en consideración, entre otros:

1) Los resultados del análisis de riesgos, amenazas y vulnerabilidades;

2) La naturaleza de los datos personales;

3) Las características de las partes involucradas; y,

4) Los antecedentes de destrucción de datos personales, la pérdida, alteración, divulgación o impedimento de acceso a los mismos por parte del titular, sean accidentales e intencionales, por acción u omisión, así como los antecedentes de transferencia, comunicación o de acceso no autorizado o exceso de autorización de tales datos.

El responsable y el encargado del tratamiento de datos personales deberán tomar las medidas adecuadas y necesarias, de forma permanente y continua, para evaluar, prevenir, impedir, reducir, mitigar y controlar los riesgos, amenazas y vulnerabilidades, incluidas las que conlleven un alto riesgo para los derechos y libertades del titular, de conformidad con la normativa que emita la Autoridad de Protección de Datos Personales.

Art. 42.- Evaluación de impacto del tratamiento de datos personales. El responsable realizará una evaluación de impacto del tratamiento de datos personales cuando se haya identificado la probabilidad de que dicho tratamiento, por su naturaleza, contexto o fines, conlleve un alto riesgo para los derechos y libertades del titular o cuando la Autoridad de Protección de Datos Personales lo requiera.

La evaluación de impacto relativa a la protección de los datos es de carácter obligatoria en caso de:

a) Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas naturales;

b) Tratamiento a gran escala de las categorías especiales de datos, o de los datos personales relativos a condenas e infracciones penales, u

c) Observación sistemática a gran escala de una zona de acceso público.

La Autoridad de Protección de Datos Personales establecerá otros tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos.

La evaluación de impacto deberá efectuarse previo al inicio del tratamiento de datos personales.

Art. 43.- Notificación de vulneración de seguridad. El responsable del tratamiento deberá notificar la vulneración de la seguridad de datos personales a la Autoridad de Protección de Datos Personales y la Agencia de Regulación y Control de las Telecomunicaciones, tan pronto sea posible, y a más tardar en el término de cinco (5) días después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la Autoridad de Protección de Datos no tiene lugar en el término de cinco (5) días, deberá ir acompañada de indicación de los motivos de la dilación.

El encargado del tratamiento deberá notificar al responsable cualquier vulneración de la seguridad de datos personales tan pronto sea posible, y a más tardar dentro del término de dos (2) días contados a partir de la fecha en la que tenga conocimiento de ella.

Art. 44.- Acceso a datos personales para atención a emergencias e incidentes informáticos. Las autoridades públicas competentes, los equipos de respuesta de emergencias informáticas, los equipos de respuesta a incidentes de seguridad informática, los centros de operaciones de seguridad, los prestadores y proveedores de servicios de telecomunicaciones y los proveedores de tecnología y servicios de seguridad, nacionales e internacionales, podrán acceder y efectuar tratamientos sobre los datos personales contenidos en las notificaciones de vulneración a las seguridades, durante el tiempo necesario, exclusivamente para la detección, análisis, protección y respuesta ante cualquier tipo de incidentes así como para adoptar e implementar medidas de seguridad adecuadas y proporcionadas a los riesgos identificados.

Art. 45.- Garantía del secreto de las comunicaciones y seguridad de datos personales. Para la correcta prestación de los servicios de telecomunicaciones y la apropiada operación de redes de telecomunicaciones, los prestadores de servicios de telecomunicaciones deben garantizar el secreto de las comunicaciones

y seguridad de datos personales. Únicamente por orden judicial, los prestadores de servicios de telecomunicaciones podrán utilizar equipos, infraestructuras e instalaciones que permitan grabar los contenidos de las comunicaciones específicas dispuestas por los jueces competentes. Si se evidencia un tratamiento de grabación o interceptación de las comunicaciones no autorizadas por orden judicial se aplicará lo dispuesto en la presente Ley.

Art. 46.- Notificación de vulneración de seguridad al titular. El responsable del tratamiento deberá notificar sin dilación la vulneración de seguridad de datos personales al titular cuando conlleve un riesgo a sus derechos fundamentales y libertades individuales, dentro del término de tres días contados a partir de la fecha en la que tuvo conocimiento del riesgo. No se deberá notificar la vulneración de seguridad de datos personales al titular en los siguientes casos:

1. Cuando el responsable del tratamiento haya adoptado medidas de protección técnicas organizativas o de cualquier otra índole apropiadas aplicadas a los datos personales afectados por la vulneración de seguridad que se demuestra que son efectivas;
2. Cuando el responsable del tratamiento haya tomado medidas que garanticen que el riesgo para los derechos fundamentales y las libertades individuales del titular, ¡no ocurrirá; y,
3. Cuando se requiera un esfuerzo desproporcionado para hacerlo; en cuyo caso, el responsable del tratamiento deberá realizar una comunicación pública a través de cualquier medio en la que se informe de la vulneración de seguridad de datos personales a los titulares.

La procedencia de las excepciones de los numerales 1 y 2 deberá ser calificada por la Autoridad de Protección de Datos, una vez informada esta tan pronto sea posible, y en cualquier caso dentro de los plazos contemplados en el Articulo 43.

La notificación al titular del dato objeto de la vulneración de segundad contendrá lo señalado en el artículo 43 de esta ley.

En caso de que el responsable del tratamiento de los datos personales no cumpliese oportunamente y de modo justificado con la notificación es sancionado conforme al régimen sancionatorio previsto en esta ley.

La notificación oportuna de la violación por parte del responsable de tratamiento al titular y la ejecución oportuna de medidas de respuesta, es considerada atenuante de la infraestructura. (*Ley-Organica-de-Datos-Personales.pdf*, 2021, pp. 35-40)

ANEXO 2: Lista de controles de la norma ISO 27001

Id	Objetivo de control	Puntaje esperado	Puntaje Obtenido
1	Políticas de gestión de datos personales.	5	3
2	Monitoreo y Evaluación.	5	3
3	Identificación la legislación aplicable.	5	3
4	Registros de evidencia	5	3
5	Recolección de evidencia.	5	3
6	Revisión del cumplimiento técnico.	5	1
7	Inventario y clasificación de los datos personales	5	3
8	Inventarios de activos	5	4
9	Identificación del ciclo de vida de un dato	5	3
10	Identificar responsabilidades de cada área	5	4
11	Acuerdo de confidencialidad.	5	5
12	Capacitación.	5	3
13	Proceso disciplinario.	5	1
14	Control perimetral	5	1
15	Seguridad de cableado	5	5
16	Control de los activos fuera de las instalaciones	5	5
17	Destrucción segura de la información.	5	3
18	Escritorio limpio	5	4
19	Control ante robo	5	5
20	Control de cambios operacionales.	5	3
21	Segregación de tareas	5	3
22	Protección ante malware	5	5
23	Registros y auditorías a los funcionarios	5	3
24	Controles de Red	5	5
25	Administración de medios de almacenamiento secundario.	5	5
26	Seguridad de medios que son movilizados	5	3
27	Manejo de correo electrónico y mensajería instantánea.	5	5
28	Disociación de datos	5	1
29	Normas de control de acceso	5	3
30	Manejo de usuarios y claves de seguridad	5	1
31	Computadores que dejen de usarse	5	5
32	Accesos externos a sistemas de información	5	1
33	Segregación de redes	5	1
34	Controles de inicio de sesión	5	4
35	Trazabilidad de tratamiento	5	3
36	Asilamiento de datos sensibles	5	3
37	Uso de dispositivos móviles internos.	5	3
38	Autenticación de segundo factor de autenticación mediante tokens TOTP (*Time One- Time Password*)	5	3
39	Cifrado	5	3
40	Firmas Electrónicas	5	4
41	Procedimientos para el manejo de incidentes	5	3

42	Procedimientos en caso de incidentes.	5	5
43	Reportes de incidentes de seguridad	5	3
44	Reporte de fallo en funcionamiento	5	4
45	Procedimientos de notificación de vulnerabilidades a los titulares de datos.	5	3
46	Aprendizaje de incidentes	5	4
47	Procedimientos de actualización del modelo de gestión	5	3
	PUNTAJE	**235**	**154**