ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

Marco referencial de seguridad para reducir riesgos en el tratamiento de datos personales en empresas prestadoras de servicios de acceso a internet, utilizando ISO 27001. Caso MUNDOTRONIC

KATHERINE ADRIANA MERINO VILLA

Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de:

MAGÍSTER EN SEGURIDAD TELEMÁTICA

Riobamba – Ecuador

Septiembre 2022

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

EL TRIBUNAL DE TRABAJO DE TITULACIÓN CERTIFICA QUE**:**

El Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, titulado: **Marco referencial de seguridad para reducir riesgos en el tratamiento de datos personales en empresas prestadoras de servicios de acceso a internet, utilizando ISO 27001. Caso MUNDOTRONIC,** es de responsabilidad de la señorita **KATHERINE ADRIANA MERINO VILLA**, ha sido minuciosamente revisado y se autoriza su presentación.

Ing. Luis Eduardo Hidalgo Almeida; Ph.D.
PRESIDENTE

Firmado electrónicamente por:
LUIS EDUARDO HIDALGO ALMEIDA

Ing. Cristian Fabricio Viteri Silva; Mag.
DIRECTOR

Firmado electrónicamente por:
CRISTIAN FABRICIO VITERI SILVA

Ing. Carmen Elena Mantilla Cabrera; Mag.
MIEMBRO

Firmado electrónicamente por:
CARMEN ELENA MANTILLA CABRERA

Ing. Ruth Genoveva Barba Vera; Mag.
MIEMBRO

Firmado electrónicamente por:
RUTH GENOVEVA BARBA VERA

Riobamba, septiembre 2022

DERECHOS INTELECTUALES

Yo, Katherine Adriana Merino Villa, declaro que soy responsable de las ideas, doctrinas y resultados expuestos en el **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, y que el patrimonio intelectual generado por la misma pertenece exclusivamente a la Escuela Superior Politécnica de Chimborazo.

Firmado electrónicamente por:
KATHERINE
ADRIANA MERINO
VILLA

Ing. Katherine Adriana Merino Villa,

C.C. 0605764109

DECLARACIÓN DE AUTENTICIDAD

Yo, Katherine Adriana Merino Villa, declaro que el presente proyecto de investigación, es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otras fuentes están debidamente citados y referenciados.

Como autor, asumo la responsabilidad legal y académica de los contenidos de este Trabajo de Titulación de Maestría.

Firmado electrónicamente por:
KATHERINE ADRIANA MERINO VILLA

Ing. Katherine Adriana Merino Villa

C.C. 0605764109

AGRADECIMIENTO

A Dios por guiarme en cada paso.

A mis maestros y miembros del tribunal quienes con humildad y responsabilidad supieron guiarme e impartir sus conocimientos para la culminación del proyecto trabajo de titulación.

A MUNDOTRONIC, por brindarme el espacio para la implementación del proyecto trabajo de titulación.

A mis padres por su apoyo y fortaleza para seguir adelante.

A todos mis familiares y amigos por su apoyo incondicional.

Katherine.

DEDICATORIA

A Dios por guiarme e iluminarme siempre por el camino correcto y permitirme cumplir cada una de mis metas en el momento más adecuado de mi vida.

A mis padres, hermanos, abuelitos y sobrinos que son las personas más importantes de mi vida, quienes han sido mi motivación, inspiración y felicidad.

A mis profesores, miembros del tribunal y amigos que han aportado a mi crecimiento profesional y personal.

Katherine.

TABLA DE CONTENIDO

CAPÍTULO IV

CAPÍTULO V

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE ANEXOS

RESUMEN

El objetivo fue elaborar un marco referencial de seguridad para reducir riesgos en el tratamiento de datos personales en empresas prestadoras de servicios de acceso a internet, utilizando ISO27001.Caso MUNDOTRONIC. El presente marco referencial de seguridad se ha diseñado identificando los requerimientos establecidos en la Ley Orgánica de Telecomunicaciones vinculados a 13 dominios y 31 controles de la norma ISO 27001 aplicables a las empresas prestadoras de servicios de acceso a internet dinámicamente mediante el ciclo Demming, para descubrir vulnerabilidades existentes e identificar y aprovechar las oportunidades de mejora y definir nuevas y mejores soluciones de seguridad. Para dar cumplimiento a las necesidades establecidas se identifica y categoriza los tipos de datos personales de acuerdo con las recomendaciones de la Agencia Española de Protección. Mientras que el impacto de la amenaza es determinado en función al riesgo al que se ve expuesto un activo que contiene datos personales y su nivel de incidencia sobre la confidencialidad, integridad y disponibilidad establecida por la metodología MAGERIT. Es decir, el marco referencial de seguridad para reducir riesgos en el tratamiento de datos personales en empresas prestadoras de servicios de acceso a internet, utilizando ISO 27001 tiene como fin salvaguardar los datos personales de los clientes, usuarios y abonados para brindar garantías e incrementar la confianza de los usuarios aportando seguridad jurídica e incorporando obligaciones y principios relacionados con la gobernanza empresarial.

Palabras claves: <SEGURIDAD DE LA INFORMACIÓN>, <AMENAZAS>, <DATOS PERSONALES>, <NORMA ISO 27001>., <MARCO REFERENCIAL DE SEGURIDAD>, <RIESGOS>

ABSTRACT

The objective was to design a security frame of reference to reduce the risks involved in the management of personal data, for companies that provide internet services using ISO27001. MUNDOTRONIC Case Study. Moreover, such security frame of reference has been developed by identifying the requirements contained in the Organic Law of Telecommunications, which is linked to 13 domains and 31 controls related to the ISO norm 27001, applicable to internet service providers, in a dynamic way through the Demming cycle. In order to discover the existent vulnerabilities and identify improvement opportunities so to define new and better security solutions. To meet the identified needs, personal data has been categorized and identified according to the recommendations of the Spanish Data Protection Agency. Meanwhile, the impact caused by the threat is determined in relation to the risk that personal data has been exposed to, and its incidence level over the confidentiality, integrity and availability stablished by the MAGERIT methodology. That is to say, the security frame of reference reduces the risks involving the management of personal data of internet service providers, using ISO 27001, which aims to protect clients, users and creditors personal data in order to guarantee data security. Resulting in an increase in clients' trust by providing legal security and introducing principles and obligations related to corporate governance.

Key words: <INFORMATION SECURITY> <THREATS>, < PERSONAL DATA>, <ISO 27001 NORM>, <SECURITY FRAME OF REFERENCE>, <RISKS>.

CAPÍTULO I

1. INTRODUCCIÓN

1.1. Planteamiento del problema

Elaboración de un marco referencial de seguridad para reducir riesgos en el tratamiento de datos personales en empresas prestadoras de servicios de acceso a internet, utilizando ISO 27001. Caso práctico MUNDOTRONIC

1.2. Situación Problemática

De acuerdo con la revista de Seguridad de la Universidad Nacional Autónoma de México, en América Latina las leyes de protección de datos personales surgen como una necesidad derivada del incremento del uso de las tecnologías de la información y el aumento de las vulnerabilidades asociadas.

En el caso de América Latina, países como Argentina, Chile, Panamá, Brasil, Paraguay y Uruguay cuentan con leyes que se asemejan al modelo europeo, el cual busca proteger la información y la propiedad de esta, con el fin de conservar la honorabilidad de la persona aun cuando ésta hubiese fallecido, este modelo se basa en los derechos humanos de los individuos. (Sánchez & Rojas, 2012).

Este modelo europeo se renovó, y a partir del 25 de mayo del 2018 entró en vigor el Reglamento General de Protección de datos, el cual contiene un único conjunto de normas para todas las empresas de la Unión Europea independientemente de la ubicación de sus sedes, implicando que las personas tengan más control sobre el manejo de sus datos (Comisión Europea, 2018).

A diferencia de estos países, en Ecuador la protección de datos personales se encuentra regulada dispersamente, ya que no posee una normativa específica relativa a Protección de Datos Personales, pero si se lo alude en la constitución del Ecuador en su Capítulo sexto, Derechos de libertad, Artículo 66, literal 19, el cuál menciona: “El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.” (Const., 2008, art. 66)

Para mayo de 2015, el presidente de la República aprueba el proyecto de ley para el desarrollo de la tecnología y del talento humano donde se declara al acceso a internet como un derecho básico para todos los ecuatorianos, incrementando la inversión de empresas privadas tanto en áreas urbanas y rurales para proveer el servicio de acceso a internet.

Estos Prestadores de Servicios de Acceso a internet se rigen en la Ley Orgánica de Telecomunicaciones que en su Título VII Secreto de las Comunicaciones y Protección de Datos Personales, Capítulo II Protección de los datos personales, estipula el derecho a la intimidad, deber de información, procedimiento de revelación, entre otros contenidos. Al igual que lo mencionado anteriormente, sobre el tema en la constitución, el contenido está abierto a interpretaciones, sin mecanismos, ni metodologías específicas de cómo tratar estos datos.

Esto no provee una definición de datos personales y deja temas abiertos para la interpretación, además no establece regulaciones, ni reglamentos preventivos específicos sobre el manejo de datos personales por partes de las instituciones, dificultando la aplicación de medidas cautelares, sanciones y el ejercicio de las garantías constitucionales. Aunque en el art. 229 del Código Orgánico Integral Penal se menciona la sanción de tres años de prisión a quien revele datos que "violen el secreto, la intimidad y la privacidad de las personas" (Código Orgánico Integral Penal [COIP], 2016).

Por esta razón la elaboración de un marco referencial de seguridad para reducir riesgos en el tratamiento de datos personales utilizando ISO 27001 permitirá establecer criterios, medidas técnicas y de gestión, procedimientos y mecanismos de coordinación para ser aplicados por parte de los prestadores de servicios de acceso a internet durante la recolección, tratamiento y posible transmisión de datos personales de los abonados, clientes y usuarios de los servicios de telecomunicaciones.

1.3. Formulación del problema

¿De qué manera contribuirá la elaboración de un marco referencial de seguridad para reducir riesgos en el tratamiento de datos personales en servicios de acceso a internet utilizando ISO 27001, siendo el caso de estudio MUNDOTRONIC?

1.4. Preguntas directrices de la investigación

¿Cuáles son las normativas vigentes en Ecuador relacionadas con la protección de datos personales que deben cumplir los prestadores de servicios de acceso a internet?

¿Cuáles son las coincidencias entre las normativas del Ecuador, el Reglamento General de Protección de Datos Personales de la Unión Europea y otras normativas existentes?

¿Cuáles son los derechos de los titulares de los datos personales y los principios que rigen el tratamiento de los datos personales en Ecuador?

¿Cómo evaluar y administrar la protección de datos personales?

¿Qué procedimientos reducirán los riesgos en el tratamiento de datos personales?

1.5. Justificación de la investigación

1.5.1. Teórico

Con la aparición de las Tecnologías de la Información y Comunicación (TIC's) el mundo ha cambiado notablemente (Ron, 2018) y la gran cantidad de información de carácter personal que es de suma importancia para el titular es almacenada y al mismo tiempo tratada y transmitida desconociéndose cómo, por qué y para qué son tratados los datos personales de los usuarios. (legaltech, 2018)

No obstante, el almacenamiento y tratamiento de datos personales otorga una ventaja en el mercado, como es el caso de la publicidad vía electrónica, donde las empresas obtienen ventaja con los datos de sus clientes y posibles clientes notificándolos a través de correo electrónico de sus nuevos productos u ofertas, incluso, en muchos de los casos las empresas envían dicha información a personas que no son sus clientes sin consentimiento de su titular y de manera arbitraria. (Ron, 2018)

Por esta razón, para el caso de la Unión Europea, garantizar una protección uniforme y coherente en el tratamiento de los datos personales es el objetivo del Reglamento General de Protección de Datos, aportando seguridad jurídica e incorporando obligaciones y principios relacionados con la gobernanza empresarial, convirtiéndose en un instrumento de unificación y uniformidad aplicable a los estados miembros de la Unión Europea. (Martínez, 2018) Por el contrario, en América del Sur diversos países han creado sus propias leyes de protección de datos y otros como Venezuela, Bolivia, Surinam, Guyana y Ecuador no poseen este tipo de ley. (MINTEL, 2018)

Sin embargo en el caso de Ecuador, en su Constitución de la República se establece la protección de datos personales como un derecho fundamental y paralelamente a la normativa constitucional, en diversos cuerpos legales se regula o aborda la protección de datos personales desde diferentes ámbitos como en el caso de la Ley Orgánica de Telecomunicaciones, que establece como derecho de los abonados, clientes y usuarios la privacidad y protección de sus datos personales los cuales deben ser garantizados por parte del prestador de servicios, con sujeción al ordenamiento jurídico vigente (Ley Orgánica, 2015).

Ante la situación planteada, actualmente la Dirección Nacional de Registro de Datos Públicos (Dinardap) y el Ministerio de Telecomunicaciones y de la Sociedad de la Información (Mintel), trabajan en la construcción de estrategias para la protección de datos personales y sus derechos que es parte de uno de los ejes del Plan de la Sociedad de la Información y del Conocimiento (PSIC) que está conformado por cinco ejes: Infraestructura digital, Seguridad de la Información y uso responsable de las TIC; Economía Digital; Inclusión y Competencias Digitales; Tecnologías emergentes para el desarrollo sostenible y Protección de Datos Personales, con el propósito de

promover la seguridad de la información y el uso responsable de las Tecnologías de la Información y Comunicación (TIC) (Dirección Nacional de Registro de Datos Públicos, 2018).

Por tanto, la elaboración de un marco referencial de seguridad para reducir riesgos en el tratamiento de datos personales de los abonados/clientes y usuarios en empresas prestadoras de servicios de acceso a internet las cuales han crecido veinte y un veces a nivel nacional (ARCOTEL, 2019) que determine cómo, para qué y durante cuánto tiempo se utilizarán los datos personales, servirá como una herramienta que permita contar con mejor acceso a información del tratamiento de datos personales, establecerá un límite legal para el manejo de datos personales y permitirá el libre flujo de datos, el desarrollo tecnológico y progreso económico; siempre de una manera ordenada y evitando que se vulneren los derechos de los titulares respecto de sus datos personales.

1.5.2. Metodológico

La elaboración de un marco referencial de seguridad para reducir riesgos en el tratamiento de datos personales en servicios de acceso a internet utilizando ISO 27001 reforzará el control de los abonados, clientes y usuarios sobre el uso de sus datos, además de obligar a las empresas a adoptar actitudes preventivas sobre el manejo de estos datos e informar fallos de seguridad.

La metodología de trabajo para elaborar un marco referencial de seguridad consiste en tomar la Ley Orgánica de Telecomunicaciones en conjunto con normas internacionales para la Gestión de Seguridad de la Información y de Protección de Datos Personales, para obtener y desarrollar mejores prácticas para el manejo de datos personales de los abonados, clientes y usuarios. Todo esto acorde a los principios que rigen el tratamiento de datos personales, y los derechos de los titulares de estos datos. Para el desarrollo del marco referencial de seguridad se elegirá la que mejor se adapte a las necesidades de la investigación.

Para lo cual, será necesario realizar un registro de actividades del tratamiento de los datos personales existentes en las organizaciones, es decir, listar todas las actividades y procesos que se realizan con los datos y documentos personales recolectados dentro de la organización, mientras que para analizar los riesgos se debe identificar los activos existentes y los datos personales que son gestionados dentro de estos, para posteriormente identificar las amenazas y proceder con el análisis de riesgos considerando las recomendaciones de la metodología Magerit versión 3.

Posterior a la identificación del nivel de riesgo se realizar un plan de acción basada en políticas o procedimientos capaces de reducir los niveles de riesgos de la materialización de las amenazas, además de establecer su periodicidad para aplicar la mejora continua, identificando acciones o actividades innecesarias que deben ser eliminadas o estableciendo nuevas acciones que mejoren las políticas y procesos.

1.5.3. Práctico

La elaboración de un marco referencial de seguridad establecerá unas buenas prácticas para mejorar el control sobre los datos personales, es decir, guiar a los prestadores de servicios de acceso a internet en el diseño de procesos de localización y gestión de datos con el fin de protegerlos y reportar en el debido tiempo brechas de seguridad que afecte a estos.
El marco referencial de seguridad será implementado en la empresa MUNDOTRONIC, el cual permitirá que los prestadores de servicios de acceso a internet brinden garantías e incremente la confianza de los abonados, clientes y usuarios para el tratamiento de datos personales, informando claramente para qué serán utilizados, durante cuánto tiempo y limitando la recolección de datos personales a lo estrictamente necesario para el fin para el cual son recolectados. Mejorando la privacidad del tratamiento de datos personales, la transparencia e información sobre el uso de estos al momento de recopilar o procesar información personal.

1.6. Objetivos

1.6.1. General

Elaborar un marco referencial de seguridad para reducir riesgos en el tratamiento de datos personales en empresas prestadoras de servicios de acceso a internet, utilizando ISO27001.Caso MUNDOTRONIC.

1.6.2. Específicos

- Analizar normativas vigentes relacionadas con protección de datos personales en Ecuador, aplicable a empresas prestadoras de servicios de acceso a internet.
- Estudiar los estándares de seguridad de la información para establecer los procedimientos adecuados en la recolección, tratamiento y transmisión de datos personales.
- Adaptar los procedimientos del marco referencial de seguridad propuesto con las normativas vigentes en el Ecuador.
- Implementar y evaluar el marco referencial de seguridad en un servicio de acceso a internet.

1.7. Hipótesis

1.7.1. Hipótesis General

La implementación del marco referencial utilizando ISO 27001 reducirá riesgos en el tratamiento de datos personales en empresas prestadoras de servicios de acceso a internet.

1.8. Identificación de variables

1.8.1. Variable Independiente:

Marco referencial de seguridad.

1.8.2. Variable Dependiente:

Reducción de riesgos en el tratamiento de datos personales.

1.8.3. Operacionalización

Tabla 1-1: Variables

VARIABLE	TIPO	CONCEPTO
Marco referencial de seguridad	Variable Independiente	Establecer procedimientos para el tratamiento de datos personales basados en las normativas vigentes en Ecuador, Normas ISO 27001 y considerar conceptos del Reglamento General de Protección de Datos
Reducir riesgos en el tratamiento de datos personales	Variable dependiente	Atenuar la probabilidad de no conformidades en la seguridad de datos personales de los abonados, clientes y usuarios.

Realizado por: Merino. Katherine, 2022.

Tabla 2-1: Indicadores e índices

VARIABLE	INDICADORES	ÍNDICES	TÉCNICA E INSTRUMENTOS
Marco referencial de seguridad	Normativas en vigencia en Ecuador	Procedimientos administrativos • Verificación de cumplimiento de requisitos establecidos en la Normativa ecuatoriana	Observación, evaluación y análisis de las siguientes normas y normativas: Ley Orgánica de Telecomunicaciones Normas ISO Reglamento General de Protección de datos
	Normas y Reglamentos Internacionales	Procedimientos administrativos • Verificación de cumplimiento de requisitos OBLIGATORIOS/ NO	

		OBLIGATORIOS	
Reducir riesgos en el tratamiento de datos personales	Confidencialidad	Escala numérica para la probabilidad: • Lineal: 0,1; 0,3; 0,5; 0,7; 0,9 • No lineales: 0,1; 0,2; 0,4 Descriptores de rangos: • Muy bajo • Bajo • Moderado • Alto • Muy alto Valoración de Activos • Aplicación de la recomendación de la metodología Magerit V3. Valoración de Amenazas del activo en función de la confidencialidad, integridad y disponibilidad: • Aplicación de la recomendación de la metodología Magerit V3. Riesgo • Riego = Probabilidad x Impacto	Matriz de Riesgo basado en MAGERIT Versión3 y recomendaciones IS0 31000:2018 Situación inicial. Situación Post-Implementación.
	Integridad		
	Disponibilidad		

Realizado por: Merino. Katherine, 2022.

1.8.4 Matriz de consistencia

Tabla 3-1: Matriz de consistencia

FORMULACIÓN DEL PROBLEMA	OBJETIVO GENERAL	HIPÓTESIS GENERAL	VARIABLE	INDICADORES	ÍNDICES	TÉCNICA E INSTRUMENTOS
¿De qué manera contribuirá la elaboración de un marco referencial de seguridad para reducir riesgos en el tratamiento de datos personales en servicios de acceso a internet utilizando ISO 27001, siendo el caso de estudio MUNDOTRONIC?	Elaborar un marco referencial de seguridad para reducir riesgos en el tratamiento de datos personales en empresas prestadoras de servicios de acceso a internet, utilizando ISO27001.Caso MUNDOTRONIC.	La implementación del marco referencial utilizando ISO 27001 reducirá riesgos en el tratamiento de datos personales en empresas prestadoras de servicios de acceso a internet. .	Marco referencial de seguridad	Normativas en vigencia en Ecuador	Procedimientos administrativos • Verificación de cumplimiento de requisitos establecidos en la Normativa ecuatoriana	Observación, evaluación y análisis de las siguientes normas y normativas: Ley Orgánica de Telecomunicaciones Normas ISO Reglamento General de Protección de datos
				Normas y Reglamentos Internacionales	Procedimientos administrativos • Verificación de cumplimiento de requisitos OBLIGATORIOS/ NO OBLIGATORIOS	
			Reducir riesgos en el tratamiento de datos personales	Confidencialidad	Escala numérica para la probabilidad: • Lineal: 0,1; 0,3; 0,5; 0,7; 0,9 • No lineales: 0,1; 0,2; 0,4 Descriptores de rangos: • Muy bajo • Bajo • Moderado	Matriz de Riesgo basado en MAGERIT Versión3 y recomendaciones IS0 31000:2018 e ISO 31010:2019. Encuesta de para determinar la situación inicial. Encuesta Post-Implementación.

				Integridad	• Alto • Muy alto Valoración de Activos • Aplicación de la recomendación de la metodología Magerit V3. Valoración de Amenazas del activo en función de la confidencialidad, integridad y disponibilidad: • Aplicación de la recomendación de la metodología Magerit V3. Riesgo • Riego = Probabilidad x Impacto	
				Disponibilidad		

Realizado por: Katherine Merino. 2020

CAPÍTULO II

2. MARCO TEÓRICO

2.1. Antecedentes del problema

2.1.1. Legislación Vigente

En el caso de Europa, a partir del 25 de mayo de 2018 se encuentra vigente el Reglamento General de Protección de Datos, el cual es un marco normativo que busca fortalecer y unificar la protección de datos en todos los países que forman la Unión Europea, constituyéndose como el mayor cambio en las normas de protección de datos en más de 20 años en la Unión Europea (Comisión Europea, 2018).

En el caso de Latinoamérica, no se cuenta con una regulación común y cada país lo aborda de diferente manera, como son los casos de Argentina, Uruguay, México, Perú, Costa Rica, Nicaragua, Colombia, República Dominicana, los cuales poseen leyes generales de protección de datos y en proyectos de ley sobre protección de datos a estudio en el parlamento se encuentran los países de Brasil y Chile.

Argentina y Uruguay fueron declarados con un nivel adecuado de protección de datos según la directiva 95/46 del Parlamento Europeo y del Consejo. Sin embargo, la Red Iberoamericana de Protección de Datos (RIPD) en junio de 2017 impulsó un marco regulatorio para protección de datos para los Estados Iberoamericanos. (Brian, 2018)

En el caso de Ecuador la protección de datos se garantiza mediante El Art. 66 de la Constitución de la República, donde "…Se reconoce y garantizará a las personas: 19. "El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos de información requerirán la autorización del titular y el mandato de la ley" (Const., 2008, art. 66)

Y la vulneración a estos datos se sanciona mediante el Código Integral Penal del 10 de febrero de 2014, mediante el artículo 178 que establece que la "Violación a la intimidad.- La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años." Además, los artículos 186, 190, 191, 192, 195, 211, 229, 230, 231, 232, 233, 234 y el 476 ya tipifican y establecen ciertas sanciones para los delitos que son considerados como informáticos. (COIP, 2016)

2.1.2. Ley Orgánica de Telecomunicaciones

En el caso de los prestadores de Servicios de telecomunicaciones, estos se rigen la Ley Orgánica de Telecomunicaciones, la cual aborda la protección de datos personales de la siguiente manera: En el Título III Derechos y obligaciones que hace referencia a los derechos y obligaciones de los abonados, clientes y usuarios se encuentran tipificados los artículos:

- Artículo 22.-En este se hace referencia al derecho que tiene el abonados, cliente y usuario a la privacidad y protección de sus datos personales por parte del prestador y al derecho que tienen a que se excluyan gratuitamente sus datos personales guías de información nacional
- Artículo 23.- Aquí se establece las obligaciones de los abonados, clientes y usuarios con respecto a los empadronamientos o registro de identidad, tales como proporcionar sus datos personales de identificación asociados a la línea o número telefónico
- Artículo 24.- En este apartado se menciona obligaciones de los prestadores de servicios de telecomunicaciones en adoptar las medidas necesarias para la protección de los datos personales de sus usuarios y abonados

Mientras que en el Título VIII Secreto de las comunicaciones y protección de datos personales se divide en dos capítulos que son:

CAPÍTULO I: Secreto de las comunicaciones, el cual está compuesto por dos artículos:

Artículo 76.- Es este se menciona la responsabilidad del prestador de servicios de telecomunicaciones en implementar las medidas técnicas de seguridad e invulnerabilidad adecuadas para preservar la seguridad de sus servicios y la invulnerabilidad de la red y garantizar el secreto de las comunicaciones y de la información transmitida por sus redes e informar a sus abonados, clientes o usuarios sobre dicho riesgo y, si las medidas para atenuar o eliminar ese riesgo no están bajo su control, sobre las posibles soluciones

Artículo 77.- Aquí se menciona las que las interceptaciones solo se podrán realizar cuando exista una orden judicial a consecuencia de una investigación de un delito o por razones de seguridad pública y del Estado, por lo que, los prestadores de servicios deberán proveer toda la información requerida en la orden de interceptación, incluso los datos de carácter personal de los involucrados en la comunicación, dichos contenidos estarán sujetos a los protocolos y reglas de confidencialidad que establezca el ordenamiento jurídico vigente. (Ley Orgánica, 2015)

CAPÍTULO II: Protección de los datos personales está compuesto por dos artículos los cuales son:

Artículo 78.- Se refiere al derecho a la intimidad el cual está establecido en el artículo 66, numeral 20 de la Constitución de la República, por lo que es responsabilidad de los prestadores de servicios de telecomunicaciones el garantizar la protección de los datos de carácter personal. Para lo cual se deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad de su

red con el fin de garantizar la protección de los datos de carácter personal de conformidad con la ley. Dichas medidas incluirán, como mínimo:

1. La garantía de que sólo el personal autorizado tenga acceso a los datos personales.
2. La protección de los datos personales almacenados o transmitidos de la destrucción accidental o ilícita, la pérdida o alteración accidentales o el almacenamiento, tratamiento, acceso o revelación no autorizados o ilícitos.
3. La garantía de la aplicación efectiva de una política de seguridad con respecto al tratamiento de datos personales." (Ley Orgánica, 2015)

Artículo 81.- Aquí se hace alusión a las Guías telefónicas o de abonados en general donde se menciona que los abonados, clientes o usuarios tienen el derecho a no figurar en guías telefónicas o de abonados, por lo que deberán ser informados de sus derechos con respecto a la utilización de sus datos personales en las guías telefónicas o de abonados y, en particular, sobre el fin o los fines de dichas guías, así como sobre el derecho que tienen, en forma gratuita, a no ser incluidos, en tales guías." (Ley Orgánica, 2015)

2.1.3. Reglamento General de Protección de Datos RGPD

Este reglamento recoge los derechos de las personas y establece las obligaciones de los encargados y responsables del tratamiento de los datos. Además, instaura los métodos a seguir para el cumplimiento de lo dispuesto en este Reglamento y el alcance de las sanciones.

El reglamento aborda los siguientes aspectos:

- **Derechos de los interesados. –** Al aplicarse esto derechos se otorgar mayor control a las personas sobre sus datos debido a:
  - La necesidad de un consentimiento sobre el tratamiento de datos.
  - Acceso más fácil del interesado a sus datos.
  - Los derechos de rectificación, supresión y al olvido.
  - El derecho de oponerse incluso al uso de datos personales a efectos de elaboración de perfiles.
  - El derecho a la portabilidad de los datos de un prestador de servicios a otro.

También se establece que los responsables del tratamiento de datos deben ofrecer información transparente y de fácil acceso.

- **Cumplimiento. -** Dentro del reglamento se especifica las obligaciones generales que tendrán los responsables y encargados del tratamiento. Así como la aplicación de medidas de seguridad en función del riesgo de operaciones realizadas para el tratamiento de datos. En el caso de darse incidentes los responsables deberán realizar las correspondientes notificaciones. Y para aquellas empresas que realicen operaciones arriesgadas de tratamiento deberán nombran un delegado de datos.

- **Seguimiento e indemnización. -** El reglamento obliga a los estados miembros (países) crear una autoridad de control independiente a nivel nacional. En el caso de empresas con filiales en varios Estados miembros solo se tratará con la autoridad de protección de datos del Estado donde se encuentre el establecimiento principal, a este principio se lo conoce como ventanilla única.

El reglamento reconoce el del interesado a presentar un reclamo a la autoridad de control, así como el derecho al recurso judicial, la indemnización y la responsabilidad.

- **Transferencias a terceros países. -** El Reglamento también abarca la transferencia de datos personales a terceros países u organizaciones internacionales. (Consejo Europeo & Consejo de la Unión Europea, 2018)

2.2. Marco conceptual

El Reglamento para la prestación de servicios de telecomunicaciones y servicios de radiodifusión por suscripción establece la siguiente descripción:

Servicio de acceso a internet. "Es el servicio que permite la provisión del acceso a la red mundial internet, por medio de plataformas y redes de acceso implementadas para tal fin." (ARCOTEL, 2016)

El Reglamento General de Protección de Datos vigente desde mayo de 2018 establece las siguientes definiciones:

Datos Personales. Es información sobre una persona física identificada o identificable directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona. (Reglamento General, 2016, p. 33)

Tratamiento. Operaciones realizadas sobre datos personales, ya sea por medio de procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción. (Reglamento General, 2016, p. 33)

Limitación del tratamiento. El marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro. (Reglamento General, 2016, p. 33)

Elaboración de perfiles. Es la forma automática de tratamiento de datos personales para evaluar los distintos aspectos personales de una persona física, que permitan analizar o predecir aspectos relacionados al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física. (Reglamento General, 2016, p. 33)

Seudonimización. Es el tratamiento adecuado de datos personales para que ya no puedan atribuirse a un individuo, siempre que dicha información adicional se muestre por separado y esté sujeta a ciertas medidas organizativas y legales que garanticen que los datos personales no se atribuyan a una persona física identificada o identificable. (Reglamento General, 2016, p. 33)

Fichero. Todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica. (Reglamento General, 2016, p. 33)

Responsable del tratamiento o responsable. La persona física o jurídica que determinen los fines y medios del tratamiento. (Reglamento General, 2016, p. 33)

Encargado del tratamiento o encargado. La persona física o jurídica responsable de tratar datos personales por cuenta del responsable del tratamiento. (Reglamento General, 2016, p. 33)

Destinatario. La persona física o jurídica, autoridad, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. (Reglamento General, 2016, p. 33,34)

Consentimiento del interesado. Toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen. (Reglamento General, 2016, p. 34)

Violación de la seguridad de los datos personales. Toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos. (Reglamento General, 2016, p. 34)

Datos biométricos. Datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona. (Reglamento General, 2016, p. 34)

Empresa. Persona física o jurídica dedicada a actividades económicas, independientemente de su forma jurídica, incluidas las sociedades o asociaciones que desempeñen regularmente una actividad económica. (Reglamento General, 2016, p. 34).

2.3. Datos personales

2.3.1. Datos personales

Son todos aquellos datos que permite identificar directa e indirectamente a un individuo como: nombres, apellidos, número de identificación, datos de localización, elementos propios de la identidad física, fisiológica, direcciones ip, matrículas de vehículos, datos biométricos, entre otros. (Reglamento General, 2016, p. 33). También se incluye:

- Direcciones postales
- Direcciones de correos electrónicos

- Números de teléfono
- Fechas de nacimiento
- Datos bancarios
- Cookies

2.3.2. Recopilación de datos

Para la recopilación de datos se debe tener las siguientes consideraciones.

- Deben ser lo más minimizados posibles.
- Deben ser exactos y estar actualizados.
- Se debe aclarar la finalidad de estos, es decir para qué se está recopilando datos de carácter personal.
- Se debe limitar el plazo de conservación de los datos.
- Se deben tratar con integridad y confidencialidad.

2.4. Tratamiento de Datos y tipos de datos

El tratamiento de datos se puede considerar como toda operación que afecta a los datos personales, desde la obtención, uso, registro, organización, estructuración y conservación de estos.
De acuerdo con la agencia española de protección de datos se tiene los siguientes tipos de datos:

- Documentos personales
- Información de aplicaciones de registro de actividades vitales
- Aspectos personales
- Preferencias de consumo, hábitos, gustos, necesidades, etc. que no permitan inferir informaciones relacionadas con categorías especiales de datos
- Rendimiento laboral
- Situación económica
- Estado financiero
- Datos de medios de pago
- Datos de comportamiento
- Datos de localización
- Datos muy personales91 no recogidos en clasificaciones anteriores
- Datos sanitarios
- Datos biométricos
- Datos genéticos
- Categorías especiales de datos o que permitan inferirlos

- Categorías especiales de datos seudonimizados
- Datos personales relativos a condenas e infracciones penales
- Metadatos
- Identificadores únicos
- Datos y metadatos de las comunicaciones electrónicas y datos inferidos de las comunicaciones electrónicas
- Datos de navegación web (Agencia Española de Protección de Datos)

2.5. Cumplimiento del Reglamento General de Protección de Datos RGPD

Los pasos para cumplir con la implementación del RGPD son:

- Realizar un Registro de actividades de tratamiento
- Realizar un Análisis de riesgos
- Elaborar una Evaluación de impacto
- Solicitar el consentimiento a los clientes
- Firmar los contratos con Encargados del tratamiento
- Firmar los contratos con los empleados
- Notificar las brechas de seguridad
- Nombrar un delegado de Protección de Datos
- Facilitar copia de los datos personales
- Derechos de los usuarios

2.6. ISO 27001

ISO (Organización Internacional de Normalización) e IEC (la Comisión Electrotécnica Internacional) constituyen el sistema especializado para la normalización a nivel mundial. Esta norma proporciona los requisitos para el establecimiento, implementación mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información ya que exige procesos y recursos para cumplir los objetivos planteados.

Este sistema de gestión de la seguridad de la información busca preservar la confidencialidad, la integridad y la disponibilidad de la información a través de la aplicación de un proceso de gestión de riesgos y entrega confianza a las partes interesadas sobre la correcta gestión de los riesgos.

Para ISO (International Organization for Standardization) un sistema de gestión queda definido por un proceso de 4 etapas, Planificar (Plan), Implementar (Do), Medir (Check) y Mejorar (Act). ISO/IEC 27001 se divide en 11 secciones y el anexo A; las secciones 0 a 3 son introductorias no obligatorias, mientras que las secciones 4 a 10 son obligatorias, lo que implica que una

organización debe implementar todos sus requerimientos si quiere cumplir con la norma. Los controles del Anexo A deben implementarse sólo si se determina que corresponden en la Declaración de aplicabilidad.

Sección 0: Introducción. – Contiene el objetivo de ISO 27001 y su compatibilidad con otras normas.

Sección 1: Alcance. – Menciona que ISO 27001 es aplicable a cualquier tipo de organización.

Sección 2: Referencias normativas. – Toma a ISO/IEC 27000 como estándar en el que se proporcionan términos y definiciones.

Sección 3: Términos y definiciones. – Lista términos importantes de ISO 27001.

Sección 4: Contexto de la organización. – esta sección es parte del ciclo PDCA y define los requerimientos, las partes interesadas, sus requisitos y el alcance del SGSI.

Sección 5: Liderazgo. - Es parte de la fase de Planificación del ciclo PDCA y define las responsabilidades de la dirección, los roles y responsabilidades y la política de seguridad de la información.

Sección 6: Planificación. - Es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para la evaluación de riesgos, el tratamiento de riesgos, la Declaración de aplicabilidad, el plan de tratamiento de riesgos y la determinación de los objetivos de seguridad de la información.

Sección 7: Apoyo. - Es parte de la fase de Planificación del ciclo PDCA y define los requerimientos sobre disponibilidad de recursos, competencias, concienciación, comunicación y control de documentos y registros.

Sección 8: Funcionamiento. - Es parte de la fase de Planificación del ciclo PDCA y define la implementación de la evaluación y el tratamiento de riesgos, y los controles a implementarse.

Sección 9: Evaluación del desempeño. - Es parte de la fase de Revisión del ciclo PDCA y define los requerimientos para monitoreo, medición, análisis, evaluación, auditoría interna y revisión por parte de la dirección.

Sección 10: Mejora. - Es parte de la fase de Mejora del ciclo PDCA y define los requerimientos para el tratamiento de no conformidades, correcciones, medidas correctivas y mejora continua.

Anexo A: proporciona 114 controles (medidas de seguridad) distribuidos en 14 secciones.

2.7. Ciclo de Demming

El ciclo Demming o PDCA se encuentra implícito en la norma ISO 27001:2013 que busca una mejora continua para conseguir el mayor nivel de eficacia operativa de los sistemas de gestión. Este ciclo permite descubrir puntos vulnerables existentes en una organización, identificar y aprovechar las oportunidades de mejorar para definir nuevas y mejores soluciones de procesos y procedimientos de seguridad.

Este ciclo PDCA está formado por cuatro etapas que se repiten constantemente con el fin de evaluar periódicamente las actividades e incorporar nuevas mejoras y son:

- **Planificación (Plan)**

Permite establecer la política, objetivos, procesos y procedimientos relativos a la gestión del riesgo y mejorar la seguridad de la información de la organización para obtener resultados de acuerdo con las políticas y objetivos generales de la organización.

- **Ejecución (Do)**

Permite implementar y gestionar el SGSI de acuerdo con la política, controles, procesos y procedimientos. De lo posible se deber realizar entornos de prueba para poder verificar sus resultados antes de implantarlo en el sistema real.

- **Seguimiento (Check)**

Ayuda a verificar, medir y revisar las prestaciones de los procesos del SGSI. Es decir, permite comprobar si las medidas adoptadas están dando el efecto esperado, para lo cual es necesario volver a recopilar datos y monitorizar el comportamiento del sistema.

- **Mejora (Act)**

En esta fase se debe adoptar acciones correctivas y preventivas basadas en auditorías y revisiones internas con el objetivo de mejorar el SGSI. En caso de la ocurrencia de un mal funcionamiento, se deberá repetir el ciclo nuevamente. Si el funcionamiento ha sido correcto, se instalarán definitivamente las modificaciones. (Bustamante & Osorio, 2014)

2.8. Gestión de la Seguridad

Garantizar un nivel de protección completo es imposible, incluso en el caso de disponer de un presupuesto ilimitado. Por lo que el propósito de un sistema de gestión de la seguridad de la información es garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías. La metodología de un SGSI según ISO 27001 se resume de la siguiente manera:

Figura 1-2: Ciclo del SGCI
Fuente: https://www.normas-iso.com/iso-27001/

Además, se debe considerar que un SGCI posee tres pilares que interactúan mutuamente y son: las personas, los procesos y la tecnología empleada. Por lo que es importante considerar correctamente el contexto de empresa y su característica para posteriormente aplicar un ciclo PDCA y lograr un sistema de gestión dinámico capaz de cumplir los objetivos planteados inicialmente. (Bustamante & Osorio, 2014)

2.9. Relación entre el RGPD y la ISO/IEC 27001:2013

El reglamento General de Protección de datos es una norma legal implementada en los países miembros de la Unión Europea, mientras que la ISO/IEC 27001:2013 es una guía para establecer su Sistema de Gestión de Seguridad de la Información que utiliza a nivel internacional, pero ambas normas pueden ser completarías, ya que la implementación de ISO/IEC 27001:2013 permite dar cumplimientos lo estipulado en el RGPD.

A continuación, se presentan los controles de ISO/IEC 27001:2013 que permiten da cumplimiento a lo solicitado por el RGPD.

Tabla 1-2: Relación entre la RGPD y la ISO/IEC 27001

	RGPD	**ISO/IEC 27001:2013**
Artículo	**Título del artículo y breve descripción**	**Objetivos de control relacionados**
Capítulo I – Disposiciones Generales		
1	Objeto	18.1
2	Ámbito de aplicación material	5.1 - 8.2 - 8.3 - 9.1 - 10.1 - 12.3 - 13.2 - 14.3
3	Ámbito territorial	5.1 - 15.1 - 18.1
4	Definiciones	N / A
Capítulo II – Principios		
5	Principios relativos al tratamiento	5.1 - 6.1 - 8.1 - 8.2 - 9.2 - 9.3 - 9.4 - 10.1 - 14.3 - 17.1
6	Licitud del tratamiento	5.1 - 14.1 - 18.1
7	Condiciones para el consentimiento	5.1 - 8.2 - 8.3 - 12.1 - 13.2 - 14.3 - 15.1
8	Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información	
9	Tratamiento de categorías especiales de datos personales	5.1 -8.2 - 8.3 -12.1 - 13.2 - 14.3 - 15.1
10	Tratamiento de datos personales relativos a condenas e infracciones penales	5.1 - 8.2 - 8.3 - 14.1 - 18.1
11	Tratamiento que no requiere identificación	5.1 - 8.2 - 8.3 - 10.1 - 13.2 - 14.1 - 15.1
Capítulo III – Derechos del interesado		
12	Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado	5.1 - 8.2 - 8.3 - 12.1 - 14.1
13	Información que deberá facilitarse cuando los datos personales se obtengan del interesado	5.1 - 8.2 - 8.3 - 12.1 - 14.1
14	Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado	5.1 - 8.2 - 8.3 - 12.1 - 14.1
15	Derecho de acceso del interesado	5.1 - 8.1 - 8.2 - 12.1 - 13.2 - 14.1 - 15.1
16	Derecho de rectificación	
17	Derecho de supresión (el derecho al olvido)	5.1 - 8.1 - 8.2 - 8.3 - 12.1 - 12.3 - 13.2 - 14.1 - 15.1
18	Derecho a la limitación del tratamiento	5.1 - 8.1 - 8.2 - 12.1 - 12.3 - 13.2 - 14.1 - 15.1

19	Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento	5.1 - 8.1 - 12.1 - 13.2 - 14.1 - 15.1
20	Derecho a la portabilidad de los datos	5.1 - 8.3 - 13.1 - 13.2 - 14.1 - 15.1
21	Derecho de oposición	5.1 - 8.1 - 8.2 - 12.1 - 12.3 - 13.2 - 14.1 - 15.1
22	Decisiones individuales automatizadas, incluida la elaboración de perfiles	5.1 - 8.2 - 12.1 - 13.2 - 14.1 - 15.1
23	Limitaciones	5.1 - 18.1
Capítulo IV – Responsable y encargado del tratamiento		
24	Responsabilidad del responsable del tratamiento	No se identifican un control en particular.
25	Protección de datos desde el diseño y por defecto	No se identifican un control en particular.
26	Corresponsables del tratamiento	5.1 - 6.1 - 12.1 - 13.2 - 15.1 - 16.1 - 18.1
27	Representantes de responsables o encargados del tratamiento no establecidos en la Unión	12.1 - 13.2 - 14.1 - 15.1 - 18.1
28	Encargado del tratamiento	5.1 - 12.1 - 15.1
29	Tratamiento bajo la autoridad del responsable o del encargado del tratamiento	No se identifican un control en particular.
30	Registro de las actividades de tratamiento	5.1 - 6.1 -12.1 - 12.4
31	Cooperación con la autoridad de control	5.1 - 6.1
32	Seguridad del tratamiento	No se identifican un control en particular.
33	Notificación de una violación de la seguridad de los datos personales a la autoridad de control	5.1 - 16.1 - 18.1
34	Comunicación de una violación de la seguridad de los datos personales al interesado	
35	Evaluación de impacto relativa a la protección de datos	5.1 - 6.1 - 8.2 - 12.1 - 13.1 - 13.2 - 14.1 - 15.1
36	Consulta previa	5.1 - 6.1 - 8.2 - 12.1 - 13.1 - 13.2 - 14.1 - 15.1
37	Designación del delegado de protección de datos	5.1 - 6.1 - 18.1
38	Posición del delegado de protección de datos	
39	Funciones del delegado de protección de datos	
40	Códigos de conducta	
41	Supervisión de códigos de conducta aprobados	
42	Certificación	
43	Organismo de certificación	
Capítulo V – Transferencias de datos personales a terceros países u organizaciones internacionales		
44	Principio general de las transferencias	N / A
45	Transferencias basadas en una decisión de adecuación	18.1
46	Transferencias mediante garantías adecuadas	
47	Normas corporativas vinculantes	
48	Transferencias o comunicaciones no autorizadas por el Derecho de la Unión	
49	Excepciones para situaciones específicas	
50	Cooperación internacional en el ámbito de la protección de datos personales	N / A
Capítulo VI – Autoridades de control independientes		
51	Autoridad de control	N / A

52	Independencia	N / A
53	Condiciones generales aplicables a los miembros de la autoridad de control	N / A
54	Normas relativas al establecimiento de la autoridad de control	N / A
55	Competencia	N / A
56	Competencia de la autoridad de control principal	N / A
57	Funciones	N / A
58	Poderes	N / A
59	Informe de actividad	N / A
Capítulo VII – Cooperación y coherencia		
60	Cooperación entre la autoridad de control principal y las demás autoridades de control interesadas	N / A
61	Asistencia mutua	N / A
62	Operaciones conjuntas de las autoridades de control	N / A
63	Mecanismo de coherencia	N / A
64	Dictamen del Comité	N / A
65	Resolución de conflictos por el Comité	N / A
66	Procedimiento de urgencia	N / A
67	Intercambio de información	N / A
68	Comité Europeo de Protección de Datos	N / A
69	Independencia	N / A
70	Funciones del Comité	N / A
71	Informes	N / A
72	Procedimiento	N / A
73	Presidencia	N / A
74	Funciones del presidente	N / A
75	Secretaría	N / A
76	Confidencialidad	N / A
Capítulo VIII – Recursos, responsabilidad y sanciones		
77	Derecho a presentar una reclamación ante una autoridad de control	N / A
78	Derecho a la tutela judicial efectiva contra una autoridad de control	N / A
79	Derecho a la tutela judicial efectiva contra un responsable o encargado del tratamiento	N / A
80	Representación de los interesados	N / A
81	Suspensión de los procedimientos	N / A
82	Derecho a indemnización y responsabilidad	18.1
83	Condiciones generales para la imposición de multas administrativas	
84	Sanciones	
Capítulo IX – Disposiciones relativas a situaciones específicas de tratamiento		
85	Tratamiento y libertad de expresión y de información	18.1
86	Tratamiento y acceso del público a documentos oficiales	

87	Tratamiento del número nacional de identificación	
88	Tratamiento en el ámbito laboral	
89	Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos	
90	Obligaciones de secreto	
91	Normas vigentes sobre protección de datos de las iglesias y asociaciones religiosas	
Capítulo X – Actos delegados y actos de ejecución		
92	Ejercicio de la delegación	18.1
93	Procedimiento de comité	
Capítulo XI – Disposiciones Finales		
94	Derogación de la Directiva 95/46/CE	18.1
95	Relación con la Directiva 2002/58/CE	
96	Relación con acuerdos celebrados anteriormente	
97	Informes de la Comisión	
98	Revisión de otros actos jurídicos de la Unión en materia de protección de datos	
99	Entrada en vigor y aplicación	

Realizado por: Merino. Katherine, 2022.

2.10. Ley Orgánica de Telecomunicaciones y el Reglamento General de Protección de Datos

Tanto la Ley Orgánica de Telecomunicaciones con el Reglamento General de Protección de Datos son normativas legales que debe ser estrictamente acatadas, a continuación, se presenta los temas en común que contienen estas dos normas, cade destacar que Ley Orgánica de Telecomunicaciones posee contextos muy generales en relación Reglamento General de Protección de Datos.

Tabla 2-2: Ley Orgánica de Telecomunicaciones vs Reglamento General de Protección de Datos

	Ley Orgánica de Telecomunicaciones	**Reglamento General de Protección de Datos**
Derechos	Intimidad	• Acceso del interesado • Rectificación • Oposición • Supresión ("al olvido") • Limitación del tratamiento • Portabilidad de los datos • No ser objeto de decisiones individuales automatizadas • Información
Garantías mínimas /Principios	1. Garantizar que sólo el personal autorizado tenga acceso a los datos personales.	**Licitud:** Los datos personales deben ser tratados de forma lícita, leal y transparente.

	2. Proteger los datos personales almacenados o transmitidos de la destrucción accidental o ilícita, la pérdida o alteración accidentales o el almacenamiento, tratamiento, acceso o revelación no autorizados o ilícitos. 3. Garantizar la aplicación efectiva de una política de seguridad de tratamiento de datos personales. 4. Garantizar que la información suministrada no sea utilizada, salvo que se cuente con el consentimiento previo y autorización expresa de cada cliente, abonado o usuario.	**Limitación:** Los datos personales deben ser recogidos con fines determinados explícitos y legítimos.
		Proporcionalidad: Los datos personales deben ser adecuados, pertinentes y limitados en relación con el tratamiento.
		Exactitud: Los datos personales deben ser exactos y estar siempre actualizados.
		Integridad y confidencialidad: Los datos personales deben mantenerse no más tiempo del necesario para los fines del tratamiento.
		Responsabilidad proactiva y enfoque de Riesgo: Los datos personales deben ser tratados de tal manera que se garantice su seguridad.

Realizado por: Merino. Katherine, 2022.

2.11. Ley Orgánica de Telecomunicaciones e ISO/IEC 27001:2013

A continuación, se presenta los controles del anexo A que permiten dar cumplimiento a lo solicitado en la Ley Orgánica de Telecomunicaciones.

Tabla 3-2: Ley Orgánica de Telecomunicaciones vs ISO/IEC 27001:2013

LEY ORGÁNICA DE TELECOMUNICACIONES	ISO/IEC 27001:2013 (Controles)
Art. 22: Derechos de los abonados, clientes y usuarios.	A.18.1.3
	A.18.1.4
Art. 23: Obligaciones de los abonados, clientes y usuarios.	A.18.1
Art. 24: Obligaciones de los prestadores de servicios de telecomunicaciones.	A.18.2
	A.18.2.1
Art. 78: Derecho a la intimidad	A.5.1.1
	A.5.1.2
	A.6.1.1
	A.6.1.4
	A.8.1.2
	A.8.1.3
	A.8.1.4
	A.9.1.1
	A.9.1.2
	A.9.2.3
	A.9.4
	A.9.4.1
	A.11.2.7
	A.11.2.9
	A.12.3.1
	A.12.4.1
	A.12.4.2

	A.12.4.3
	A.14.1.1
	A.14.1.2
	A.14.1.3
	A.17.2.1

Realizado por: Merino. Katherine, 2022.

2.12. Servicio de acceso a internet

De acuerdo con la RESOLUCIÓN 05-03-ARCOTEL-2016 y la ficha descriptiva de servicio de telecomunicación, los servicios de acceso a internet son parte de la denominación de servicio Acceso a Internet, el cual tiene como fin proveer el acceso a la red mundial Internet, para lo cual necesita el registro de un título habilitante.

Para dar servicios a los abonados, clientes o suscriptores se realiza a través de servicios portadores o redes del servicio de telefonía fija, utilizando tanto medios alámbricos o inalámbricos vinculados con dichos servicios. (Agencia de Regulación y Control de las Telecomunicaciones, 2016)

Para dimensionar la población a la cual se va a servir se considerar como un hogar como unidad de la población. Por lo que la penetración del servicio de acceso a internet por hogar se debe dividir el número de cuentas de internet fijo para el número de hogares correspondiente a la división política de estudio que puede ser nacional, provincial, cantonal o parroquial.

De acuerdo con las estadísticas presentadas por la ARCOTEL hasta junio de 2020, el servicio de acceso a Internet fijo presenta aproximadamente 2,21 millones de cuentas de internet fijo (12,7% penetración poblacional o por habitante y 48,4% de penetración por hogar).

Mediante un análisis geográfico y de cobertura, se identificó que de las 1.0453 parroquias urbanas y rurales que tiene el Ecuador, existen SAI en 726 parroquias y 319 parroquias no tienen cuentas de SAI en sus territorios.

A continuación, se presenta la forma de funcionamiento de un prestador de servicio de accesos a internet. En esta imagen se pude identificar que un SAI tiene:

- Una red corporativa interna. - Se conecta al proveedor de internet y también gestiona la red interna de la organización
- Estaciones bases. - En estas estaciones se localizan a las antenas de transmisoras que proveen internet a diferentes zonas rurales funcionando como puntos de acceso.
- Sectores o zonas de servicio. - En esto sectores se encuentran las casas de los usuarios, abonados o clientes quienes poseen módems receptores de señal de internet.

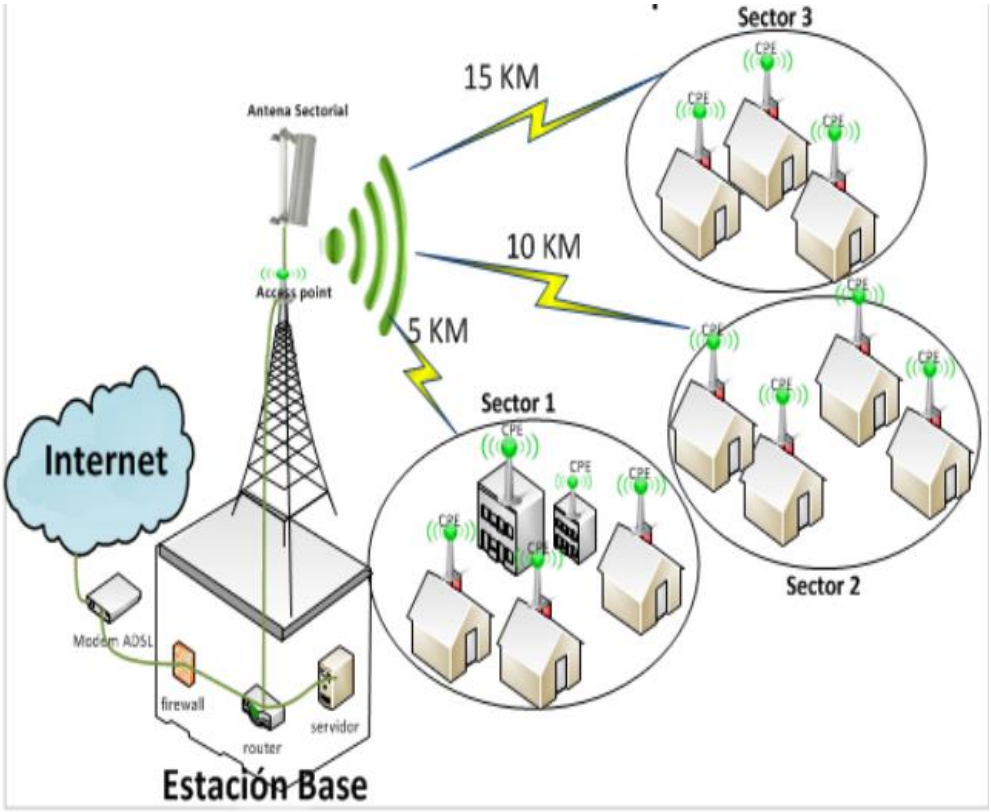


Figura 2-2: Esquema de un prestador de servicios de acceso a internet.
Realizado por: Jhon Reyes. 2016

CAPÍTULO III

3. METODOLOGÍA DE LA INVESTIGACIÓN

3.1. Tipos y diseño de la investigación

3.1.1. Diseño de la investigación

La investigación es del tipo cuasiexperimental ya que se escoge varios métodos, normas, normativas y buenas prácticas que se utilizarán como base para la creación de un marco referencial de seguridad para empresas prestadoras de servicios de acceso a internet para el correcto manejo de datos personales, además los datos a obtenerse de las pruebas serán generados por el autor de esta investigación.

3.1.2. Tipo de la investigación

Es de tipo descriptiva y aplicativa, ya que se basa en conocimientos existentes derivados de investigaciones previas, dirigida al desarrollo tecnológico en la seguridad de datos personales de los registros que contienen los prestadores de servicios de acceso a internet para establecer un nuevo esquema o marco de trabajo para mejorar los existentes.

3.2. Métodos

3.2.1. Método de investigación

Se utiliza el método científico ya que se refiere a la serie de etapas que hay que recorrer para obtener un conocimiento válido desde el punto de vista científico, utilizando para esto instrumentos que resulten fiables, el cual consta de las siguientes etapas:

- Planteamiento del problema
- Formulación de la hipótesis
- Levantamiento de la información
- Análisis e interpretación de resultados
- Comprobación de la hipótesis
- Difusión de resultados

Método deductivo debido que, al estudiar el riesgo generado por las no conformidades encontradas en la seguridad en el tratamiento de datos personales, se trata de encontrar un marco

de trabajo adecuado de seguridad que contenga las mejores características de Normas ISO y la Ley Orgánica Telecomunicaciones considerando conceptos del Reglamento General de Protección de Datos Personales.

3.2.2. Plan General del Trabajo

Planteamiento del problema

- Analizar normativas vigentes relacionadas con protección de datos personales en Ecuador, aplicable a empresas prestadoras de servicios de acceso a internet.
- Estudiar los estándares de seguridad de la información para establecer los procedimientos adecuados en la recolección, tratamiento y transmisión de datos personales.

Formulación del problema

- Identificar las coincidencias entre las normativas del Ecuador, el Reglamento General de Protección de Datos Personales de la Unión Europea y otras normativas existentes.
- Identificar los derechos de los titulares de los derechos personales y los principios que rigen el tratamiento de los datos personales.

Sistematización del problema

- Analizar como evaluar y administrar la protección de datos personales.
- Analizar los procedimientos reducirán los riesgos en el tratamiento de datos personales.

Recolección de información

- Recolección de información proporcionada por la empresa.
- Búsqueda bibliográfica.
- Investigar Base de Datos de tesis.
- Lluvia de ideas / marco lógico.

Elaboración del marco referencial de seguridad

- Elaborar un cuadro comparativo entre los controles de la Norma ISO 27001 y el Reglamento General de Protección de Datos.
- Identificar las coincidencias entre la Norma ISO 27001 y el Reglamento General de Protección de Datos.
- Realizar el análisis de riesgos para el tratamiento de datos personales.
- Desarrollar la evaluación de impacto e identificar el riesgo.
- Desarrollar el marco referencial de seguridad en base a las coincidencias entre la Norma ISO 27001 y el Reglamento General de Protección de Datos.

Implementación del marco referencial de seguridad

- Implementar el marco referencial de seguridad según las coincidencias entre la Norma ISO 27001 y el Reglamento General de Protección de Datos.

Validación del marco referencial de seguridad

- Comprobar la aplicación del marco referencial de seguridad mediante una validación de cumplimiento de parámetros.

Análisis del marco referencial de seguridad

- Evaluar la situación anterior y la actual de la empresa MUNDOTRONIC.

Informe Final

- Presentar un documento escrito.
- Defender el proyecto final ante un tribunal.

3.3. Enfoque de la investigación

La investigación presenta un enfoque cuantitativo porque se utilizará para responder preguntas de investigación en lo referente a la situación de los riesgos a los que se enfrenta el tratamiento de datos personales de los abonados, clientes y usuarios, y así establecer buenas prácticas para reducir la probabilidad de la materialización de las amenazas.

3.4. Alcance de la investigación

La investigación presenta buenas prácticas para el tratamiento de los datos personales de los abonados, clientes y usuarios que manejan las empresas prestadoras de servicios de acceso a internet sustentadas en ISO 27001, los cuales son validados mediante el cumplimento de parámetros por lo que se realizará una evaluación antes y después de la aplicación del marco referencial de seguridad.

El marco referencial de seguridad se enfocará en los lineamientos establecidos en la Ley Orgánica de Telecomunicaciones que aborda el tratamiento de los datos personales de los abonados, clientes y usuarios, por lo que a continuación se presentan las bases de este:

- Se identificarán los requerimientos de la Ley Orgánica de Telecomunicaciones necesarios para el tratamiento de datos personales.
- Se seleccionarán los controles ISO 27001 necesarios para dar cumplimiento a los requerimientos de la Ley Orgánica de Telecomunicaciones.
- Se desarrollará un análisis de riesgos utilizando la metodología Magerit V3.
- El marco referencial de seguridad contará con un ciclo de mejora continua para identificar actividades que deben ser eliminadas, reformadas o creadas que mejoren los procesos del marco referencial.

3.5. Población

El reglamento para la prestación de servicios de telecomunicaciones y servicios de radiodifusión por suscripción describe al servicio de acceso a internet como el servicio que permite la provisión del acceso a la red mundial Internet, por medio de plataformas y redes de acceso implementadas para tal fin.

Los prestadores de servicios de acceso a internet de acuerdo con la norma anteriormente mencionada deben cumplir las siguientes especificaciones técnicas, operativas y legales:

- El acceso de abonados, clientes o suscriptores puede realizarse a través de servicios portadores o redes del servicio de telefonía fija, utilizando tanto medios alámbricos o inalámbricos vinculados con dichos servicios.
- Se pueden también utilizar servicios portadores para el establecimiento de conectividad de transporte entre nodos del prestador del servicio de acceso a internet, para lo cual el prestador del servicio de acceso a internet deberá suscribir los acuerdos o contratos correspondientes, pudiendo utilizar tanto medios alámbricos como inalámbricos.

El presente estudio es realizado en la empresa prestadora de servicio de acceso a internet MUNDOTRONIC ubicada en la ciudad de Riobamba como representante de los prestadores de servicios de acceso a internet, la cual provee el servicio por medios inalámbricos. Esta empresa cuenta con 5 empleados fijos y 3 externos, los cuales laboran de forma permanente.

3.6. Unidad de análisis

Para el presente estudio la unidad de análisis es la empresa MUNDOTRONIC ubicada en la ciudad de Riobamba con sus 5 empleados fijos, la cual brinda el servicio de acceso a internet a diversos sectores dentro de la provincia de Chimborazo.

3.7. Selección de la muestra

La misma que la población.

3.8. Tamaño de la muestra

La misma que la población.

3.9. Técnicas de recolección de datos primarios y secundarios

Se basa en revisión de fuentes de información bibliográficas primarias como información proporcionada por la empresa MUNDOTRONIC, Pruebas y Observación de resultados y secundarias como:

- Tesis realizadas nacionales e internacionales de cuarto nivel.
- Trabajos de investigaciones nacionales e internacionales.
- Artículos científicos en base de datos de bibliotecas virtuales.
- Diccionarios especializados.
- Conferencias académicas, congresos, seminarios.
- Revistas indexadas y no indexadas publicadas de prestigio.
- Revistas electrónicas.
- Páginas de internet que brinden información confiable.
- Normativas Ecuatorianas:
  - Constitución de la República del Ecuador 2008
  - Código Orgánico Integral Penal
  - Ley Orgánica de Telecomunicaciones
- Estándares internacionales:
  - Reglamento General de Protección de Datos
  - ISO 27001
  - ISO 27002

3.10. Instrumentos de recolección de datos primarios y secundarios

La recolección de datos utilizada es la validación del cumplimiento de parámetros antes y después de la implementación del marco referencial de seguridad a la población establecida y la verificación de un análisis documental que se aplica en un momento en particular, con la finalidad de buscar información que será útil para evaluar los indicadores de las variables, para lo cual se realiza una entrevista, inventario de datos personales recogidos por MUNDOTRONIC y un análisis de riesgos.

3.11. Instrumentos para procesar los datos recopilados

Como instrumentos para procesar los datos recolectados se utiliza el software Microsoft Excel y SPSS para la tabulación y análisis estadístico de las encuestas aplicadas y los reportes de auditoría.

3.12. Justificación de la selección de la empresa MUNDOTRONIC

MUNDOTRONIC con el afán de mejorar sus procedimientos de seguridad y dar cumplimiento a lo estipulado en la Ley Orgánica de Telecomunicaciones para la Protección de Datos Personales, para lo cual se analizó de forma general el estado actual de MUNDOTRONIC.

Se realiza el análisis FODA para identificar fortalezas, oportunidades, debilidades y amenazas al que se enfrenta MUNDOTRONIC. Este análisis se realiza en función de a procesos y políticas referentes a Protección de Datos.

Tabla 1-3: Análisis FODA

Fortalezas	**Debilidades**
• Varios proveedores de internet para mantener el servicio disponible. • Políticas de seguridad internas sobre equipos • Área de porte técnico dentro de la empresa. • Uso de contraseñas para el acceso a los equipos y sistemas. • Nivel tecnológico robusto • Buena calidad del servicio	• Falta de conocimiento en hardening de servidores. • Falta de políticas y procedimientos de seguridad de datos personales • Falta de conocimiento sobre seguridad de la información. • No cuenta con políticas estandarizadas internacionales. • Falta de capacitación continua sobre seguridad de la información. • Incorrecta segregación de actividades del personal.
Oportunidades	**Amenazas**
• Contar con el apoyo de la gerencia para implementar procesos y políticas de seguridad. • Aumento de confianza de la organización • Cumplimiento de la ley Orgánica de telecomunicaciones • Necesidad del servicio en la población • Buen posicionamiento en el mercado.	• Competencia • Cambios tecnológicos constantes. • Métodos de seguridad inapropiados • Falta de conocimiento de acciones a aplicar para dar cumplimiento con lo establecido en la ley orgánica de telecomunicaciones • Resisten a la aplicación de políticas y procedimientos de seguridad por parte del personal interno.

Realizado por: Merino. Katherine, 2022.

Del análisis FODA se concluye que MUNDOTRONIC es una empresa estable que mantienen la disponibilidad de sus servicios con sus clientes y posee un nivel tecnológico robusto con un área técnica al servicio de sus clientes y dispuesto a dar solución a los incidentes presentados, que aplica políticas de orientadas a proteger equipos, además se asegura que los accesos están restringidos por contraseñas.

También se identifica que existe falta de conocimientos en procesos y políticas de aseguramiento de los datos personales, que sus políticas aplicadas no siguen un estándar internacional además de que no cuenta con personal capacitado en seguridad de la información y una incorrecta segregación de funciones.

Al ser un proveedor de acceso a internet y sus años de trayectoria, MUNDOTRONIC busca posicionarse en el mercado y cumplir con sus deberes legales para mejorar su imagen corporativa y sus servicios, por lo que necesita mejorar la confianza en su organización para mejorar su

servicio. Pero se enfrenta a amenazas como la competencia, cambios tecnológicos, legales y en especial a la resistencia al cambio de la cultura de seguridad dentro de su empresa.

Por lo anterior menciona es necesario que MUNDOTRONIC implemente un marco referencial de seguridad para reducir riesgos en el tratamiento de datos lo cual mejoraría sus servicios, aumentaría la confianza con sus clientes, mejoraría su imagen corporativa, sobresaldría entre el mercado al proteger los datos de sus clientes, cumpliría con las normativas que la rigen y robustecerían su red de servicios.

3.13. Identificación y priorización de riesgos

De acuerdo con la norma NTC-ISO/IEC 27000:2014, se define el riesgo como la *"Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias"*.

3.13.1. Inventario y clasificación de datos personales

La agencia española de protección de datos ha clasificado los diferentes tipos de datos personales que se pueden encontrar, para el caso de MUNDOTRONIC solo se han identificado el manejo de ocho tipos de datos los cuales se detallan a continuación con su contenido.

- Aspectos personales. - Nombres, apellidos, nacionalidad, actividades económicas
- Identificadores únicos. - Números de teléfonos, número de cédula, IP, dirección MAC.
- Datos de localización. - Direcciones domiciliaria, Coordenadas
- Preferencias de consumo. - Servicios de consumo
- Metadatos. - Tráfico de red
- Estado financiero. - Estados financieros
- Datos de medios de pago. - Método de pago del cliente
- Documentos personales. - Documentos que servicios básicos, copias de documentos personales.

Los datos que maneja MUNDOTRONIC son los siguientes:

- **Datos del cliente**: Estos se recopilan cuando se establece el contrato con el cliente

Tabla 2-3: Datos del cliente

DATOS DEL CLIENTE	TIPO DE DATOS
Nombre del cliente	Aspectos personales
Nacionalidad	Aspectos personales
Sexo	Aspectos personales
Número de Cédula	Identificadores únicos
RUC	Identificadores únicos
Representante legal	Aspectos personales
Razón Social	Aspectos personales
Actividad Económica	Aspectos personales
Dirección del domicilio	Datos de localización
Referencia	Datos de localización
Ciudad	Datos de localización
Parroquia	Datos de localización
Barrio	Datos de localización
Coordenada latitud	Datos de localización
Coordenada longitud	Datos de localización
Tipo de edificación	Datos de localización
Número convencional	Identificadores únicos
Número celular	Identificadores únicos
Correo electrónico	Aspectos personales
Nombre Referencia familiar	Identificadores únicos
Número telefónico Referencia familiar	Identificadores únicos

Realizado por: Merino. Katherine, 2022.

- **Datos de ubicación del servicio:** Estos datos son receptados al inicio del contrato y se los conserva para realizar las instalaciones y los mantenimientos y forman parte del diseño de red física.

Tabla 3-3: Datos de ubicación del servicio

DATOS DE UBICACIÓN DEL SERVICIO	TIPO DE DATOS
Dirección de instalación	Datos de localización
Coordenada latitud	Datos de localización
Coordenada longitud	Datos de localización
Referencia	Datos de localización
Ciudad	Datos de localización
Parroquia	Datos de localización
Tipo de edificación	Datos de localización
Teléfono del sitio	Identificadores únicos
Persona para contactar	Aspectos personales

Realizado por: Merino. Katherine, 2022.

- **Datos del servicio contratado**: Estos se recopilan cuando se establece el contrato con el cliente y se los mantiene para la provisión del servicio y se lo utiliza para clasificar el servicio y el tipo de cliente y estimar el ingreso por cliente.

Tabla 4-3: Datos del servicio contratado

SERVICIOS CONTRATADOS		TIPO DE DATOS
Características del plan	Tipo de plan (home, corporativo)	Preferencias de consumo
	Medio (FTTH, DSL, otro)	Preferencias de consumo
	Compartición	Preferencias de consumo
	Tasa máxima de bajada (Mbps)	Metadatos
	Tasa mínima de bajada (Mbps)	Metadatos
	Tasa máxima de subida (Mbps)	Metadatos
	Tasa mínima de subida (Mbps)	Metadatos
Servicios y tarifas	Tipo de Servicio	Preferencias de consumo
	Costo de instalación	Estado financiero
	Pago mensual	Estado financiero
	Promociones	Estado financiero
	Productos o servicios adicionales	Estado financiero
	Descuentos	Estado financiero
	Tipo de pago	Datos de medios de pago

Realizado por: Merino. Katherine, 2022.

- **Documento**: Estos documentos se receptan al inicio del contrato como respaldo de la veracidad de los datos entregados y para ubicar lugar de residencia de este. Además de almacena documentos como copias de las facturas para dar cumplimiento al Sistema legal que rigen a las empresas como es el Servicio de Rentas Internas.

Tabla 5-3: Documentos receptados y almacenados por MUNDOTRONIC

DOCUMENTOS	TIPO DE DATOS
Copia de cédula de Identidad o pasaporte	Documentos personales
Copia de una factura de un servicio básico que demuestre la residencia del solicitante para acceder al servicio.	Documentos personales
Copia del RUC	Documentos personales
Copia de cédula o pasaporte de representante legal.	Documentos personales
Nombramiento de representante legal	Documentos personales
Facturas de consumo	Documentos personales
Correos electrónicos	Documentos personales

Realizado por: Merino. Katherine, 2022.

- **Datos de Equipos**: Los datos identificadores de los equipos se los registra en el diseño lógico de la red para accesos remotos, los datos de monitoreo de los almacena periódicamente.

Tabla 6-3: Datos de los equipos de MUNDOTRONIC

DATOS DE EQUIPOS	TIPO DE DATOS
IP del equipo del cliente	Identificadores únicos
MAC del equipo del cliente	Identificadores únicos
Datos de monitoreo de comunicaciones	Metadatos
ID de los equipos	Metadatos
Tipos de equipos	Metadatos

Realizado por: Merino. Katherine, 2022.

No se identifica procesos y procedimiento para que los datos cumplan su ciclo de vida, Todos los datos deben cumplir las siguientes etapas:

- Obtención
- Almacenamiento
- Uso
  - Acceso
  - Manejo
  - Aprovechamiento
  - Monitoreo
  - Procesamiento
- Divulgación
  - Remisiones
  - Transferencias
- Bloqueo
- Cancelación, supresión o destrucción.

3.13.2. Categoría de los datos de acuerdo con el factor de riesgos

Para categorizar el factor y el nivel de riesgo de los datos personales se emplea la misma categoría que recomienda la agencia española de protección de datos, tal como se presenta en la tabla a continuación en una tabla resumen.

Tabla 7-3: Nivel de riesgo de acuerdo con el tipo de dato.

FACTOR DE RIESGO	NIVEL DE RIESGO
Aspectos personales	Medio
Identificadores únicos	Medio
Datos de localización	Medio
Preferencias de consumo	Medio
Metadatos	Medio
Estado financiero	Medio
Datos de medios de pago	Alto
Documentos personales	Medio

Realizado por: Merino. Katherine, 2022.

3.13.3. Análisis del riesgo

MAGERIT es una metodología abierta formal que sirve para identificar los riesgos en sistemas de información con mejor alineamiento con la norma ISO. Esta metodología permite identificar y valorar a los activos de información, ayuda a identificar las amenazas que pueden afectar negativamente a estos y sus vulnerabilidades, logrando determinar el impacto que puede tener la materialización de una amenaza sobre los activos dentro de la organización. (Cordero, 2015)

MAGERIT está basada en el dominio de administración de recursos que establece la norma ISO 27001 por lo que es más compatible con esta, a diferencia de la metodología CRAMM quien tiene una mejor alineación con la norma ISO27002 (Cordero, 2015). MAGERIT también establece una metodología más concreta y profunda con respecto a la norma ISO 27005 debido a que esta norma no se adentra a la realización de la gestión de los riesgos y solo se queda en la declaración de la determinación de los riesgos. (Manuel, 2009)

Por lo que para el análisis de riesgo de la presente investigación se aplica MAGERIT Versión 3, teniendo como alcance identificar los riesgos a los que se ve expuesto los activos que contienen datos personales de los abonados/clientes y usuarios de MUNDOTRONIC y poder establecer los procedimientos de mitigación que peritan salvaguardar los datos, por lo que es necesario realizar las siguientes actividades:

Identificar los activos

1. Identificar los activos y los tipos de datos que son contenidos y procesados.
2. Identificar la vulnerabilidad y las amenazas a las que están expuestos estos tipos de activos.
3. Para valorar el riesgo se toma como base la probabilidad de ocurrencia y su impacto al materializarse. Se considera los riesgos a los que está expuesto los datos personales además del nivel de control que se va a implementar sobre las amenazas.

3.13.4. Identificación de activos.

Se identifica todos los activos de MUNDOTRONIC y se analiza que tipo de información procesan para determinar solo aquellos que procesen datos personales. Obteniendo la siguiente lista de activos los cuales son clasificados de acuerdo con el tipo de activo según lo recomendado por la metodología MAGERIT.

Tabla 8-3: Lista de activos de MUNDOTRONIC.

IDENTIFICADOR	TIPO DE ACTIVO	ACTIVO	TIPOS DE DATOS QUE ADMINISTRAN
[D]	DATOS/INFORMACIÓN	DATOS DEL CLIENTE	Aspectos personales
			Identificadores únicos
			Datos de localización
			Identificadores únicos
		DATOS DE UBICACIÓN DEL SERVICIO	Datos de localización
			Identificadores únicos
			Aspectos personales

		DATOS DE SERVICIOS CONTRATADOS	Preferencias de consumo
			Metadatos
			Estado financiero
			Datos de medios de pago
		DOCUMENTOS DEL CLIENTE	Documentos personales
		DATOS DE LOS EQUIPOS	Identificadores únicos
			Metadatos
[P]	PROCESOS DEL NEGOCIO	PROCESOS DE FACTURACIÓN	Aspectos personales
			Identificadores únicos
			Datos de medios de pago
		PROCESO DE CONTRATACIÓN	Aspectos personales
			Identificadores únicos
			Datos de localización
			Identificadores únicos
[HW]	HARDWARE	COMPUTADORA CENTRAL	Identificadores únicos
			Datos de localización
			Preferencias de consumo
			Metadatos
			Estado financiero
			Datos de medios de pago
			Documentos personales
		DISPOSITIVOS MÓVILES	Identificadores únicos
			Datos de localización
[MEDIA]	SOPORTES	DISCO EXTERNOS	Metadatos
		DISPOSITIVOS USB	Metadatos
[SW]	SOFTWARE	WINDOWS 10	Aspectos personales
			Identificadores únicos
			Datos de localización
			Preferencias de consumo
			Metadatos
			Estado financiero
			Datos de medios de pago
			Documentos personales
		CCLEANER	Metadatos
		SISTEMA DE FACTURACIÓN	Aspectos personales
			Identificadores únicos
			Datos de medios de pago
[COM]	REDES Y COMUNICACIONES	FIREWALL	Identificadores únicos
			Metadatos
		ROUTERS	Identificadores únicos
			Metadatos
		SWITCH	Metadatos
		MODEMS	Metadatos
[L]	INSTALACIONES	ANTENA TX 1	Identificadores únicos
			Metadatos
		ANTENA TX 2	Identificadores únicos
			Metadatos
		ANTENA TX 3	Identificadores únicos
			Metadatos
[P]	PERSONAL	GERENTE	Aspectos personales
			Identificadores únicos

			Datos de localización
			Preferencias de consumo
			Metadatos
			Estado financiero
			Datos de medios de pago
			Documentos personales
		ADMINISTRADOR	Aspectos personales
			Identificadores únicos
			Datos de medios de pago
		PERSONAL TÉCNICO	Identificadores únicos
			Metadatos

Realizado por: Merino. Katherine, 2022.

3.13.5. Identificación de las amenazas

Para determinar las amenazas se considera lo establecido por la Ley Orgánica de Telecomunicaciones que menciona que:

- Se debe proteger los datos personales de destrucciones, pérdidas, alteraciones, almacenamientos, tratamientos, accesos y revelaciones ilícitas, accidentales y no autorizadas.
- La interceptación de comunicaciones requiere de orden expresa de un juez competente.

Y considerando las amenazas del análisis FODA de MUNDOTRONIC se procede a relacionarlas con el listado de amenazas que establece ISO 27001 (Escuela Europea de Excelencia), las cuales también se encuentran en la metodología MAGERIT.

Tabla 9-3: Amenazas FODA vs Amenazas ISO 27001.

AMENAZAS FODA	**AMENAZAS ISO 27001**
Competencia	Fuga de información Suplantación de identidad Interceptación de información
Cambios tecnológicos constantes.	Error de usuarios Error de configuración Vulnerabilidades en software
Métodos de seguridad inapropiados	Error del Administrador
Falta de conocimiento de acciones a aplicar para dar cumplimiento con lo establecido en la ley orgánica de telecomunicaciones.	Deficiencia en la organización
Resisten a la aplicación de políticas y procedimientos de seguridad por parte del personal interno.	Difusión de software malicioso Error de mantenimiento Revelación de la información

Realizado por: Merino. Katherine, 2022.

Identificadas las amenazas se procede a relacionarlas con los activos de acuerdo la metodología MAGERIT versión 3.0 dando como resultado la siguiente tabla que relaciona el activo y la amenaza.

Tabla 10-3: Lista de amenazas con respecto a los activos de MUNDOTRONIC.

ACTIVOS	**AMENAZA**
[D]	Error de usuarios

	Error del Administrador
	Error de configuración
	Fuga de información
	Suplantación de identidad
	Revelación de la información
[COM]	Error del Administrador
	Fuga de información
	Error de mantenimiento
	Suplantación de identidad
	Interceptación de información
	Revelación de la información
[HW]	Error del Administrador
[L]	Fuga de información
	Error de mantenimiento
	Revelación de la información
[Media]	Error de usuarios
	Error del Administrador
	Fuga de información
	Error de mantenimiento
	Revelación de la información
[P]	Deficiencia en la organización
	Fuga de información
[SW]	Error de usuarios
	Error del Administrador
	Difusión de software malicioso
	Fuga de información
	Vulnerabilidades en software
	Error de mantenimiento
	Suplantación de identidad
	Revelación de la información

Realizado por: Merino. Katherine, 2022.

A continuación, se muestra el listado de amenazas que se presentan en los activos MUNDOTRONIC y el orden de relevancia en la afectación con respecto a la disponibilidad, integridad y confidencialidad según la metodología Magerit en su versión 3.

Donde:

- [D] representa la Disponibilidad. [I] representa la Integridad y [C] representa la confiabilidad.
- 1 equivale a mayor relevancia, 2 relevancia media y 3 menor relevancia.

Tabla 11-3: Lista de amenazas y su orden de relevancia.

ID	AMENZA	DESCRIPCIÓN	DIMENSIONES /ORDEN DE RELEVANCIA

[A1]	Error de usuarios	Equivocaciones de las personas cuando utilizan los datos o servicios	[D]	3
			[I]	1
			[C]	2
[A2]	Error del Administrador	Fallas por parte del personal responsable en la realización de los procesos.	[D]	1
			[I]	2
			[C]	3
[A3]	Error de configuración	Fallas en la realización de las configuraciones.	[D]	N/A
			[I]	1
			[C]	N/A
[A4]	Deficiencia en la organización	Fallas en la segregación de funciones.	[D]	1
			[I]	N/A
			[C]	N/A
[A5]	Difusión de software malicioso	Propagación de software que altere el correcto funcionamiento de los sistemas (virus, troyano, gusano, etc.)	[D]	1
			[I]	2
			[C]	3
[A6]	Fuga de información	Revelación de datos personales de la organización.	[D]	N/A
			[I]	N/A
			[C]	1
[A7]	Vulnerabilidades en software	Fallas en código fuente de los programas, aplicaciones, sistemas operativos	[D]	1
			[I]	2
			[C]	3
[A8]	Error de mantenimiento	Fallas de personas en la realización de los procedimientos de control y monitoreo de los sistemas	[D]	1
			[I]	2
			[C]	N/A
[A9]	Suplantación de identidad	Fallas del personal al momento de utilizar los activos	[D]	1
			[I]	2
			[C]	3
[A10]	Interceptación de información	Acceso a la información (se mantiene en escucha)	[D]	N/A
			[I]	N/A
			[C]	1
[A11]	Revelación de la información	Revelación de la información de los clientes, usuario o abonados	[D]	N/A
			[I]	N/A
			[C]	1

Realizado por: Merino. Katherine, 2022.

Para definir la probabilidad se considera las recomendaciones de uso de escala numéricas lineales 0.1; 0.3; 0.5; 0.7; 0.9 o no lineales como 0.1; 0.2; 0.4 y descriptores de rangos como: “muy bajo”, “bajo”, “moderado”, “alto” y “muy alto” y al indicador de prioridad tiempo. (UNAM)Ya que para este estudio es importante identificar cada cuanto tiempo se puede producir el riesgo. Además, se considera que la probabilidad del riesgo debe ser superior a cero, ya que si la probabilidad es cero dejaría de ser un riesgo, Según Andréi Kolmogórov (Barragán, 2017)

Como la Ley Orgánica establece que los prestadores de servicios de acceso a internet deben someterse a una auditoría de seguridad y considerando que lo recomendado es como mínimo una vez al año realizar la revisión del SGCI. (ISO 27001)Para este estudio se considera un año como tiempo total de análisis y la recurrencia por semana, mes y año que soportaría la organización, para esto se ha considerado los históricos de incidentes de la organización. La probabilidad de ocurrencia estará basada en los siguientes criterios de valoración:

Tabla 12-3: Probabilidad del riesgo

NIVELES DE PROBABILIDAD DE OCURRENCIA		DESCRIPCIÓN
0,9-1	**Muy alta**	Riesgo de materialización es recurrente (Más de tres veces por semana) (Casi seguro).
0,7-0,8	**Alta**	Riesgo que puede materializarse de manera habitual (Más de ocho veces al mes) (Probable).
0,5-0,6	**Moderada**	Riesgo que se presenta de forma casual o accidental (Menos de cuatro veces al mes) (Posible).
0,3-0,4	**Baja**	Riesgo que puede presentarse de manera eventual (Menos de doce veces al año) (Raro).
<0,2	**Muy baja**	Riesgo cuya probabilidad de materializarse es mínima (Menos de seis veces al año) (Improbable).

Realizado por: Merino. Katherine, 2022.

3.13.6. Impacto del riesgo

El impacto nos permite medir la gravedad de las consecuencias al materializarse un evento adverso. Para este caso de estudio el impacto se lo calculará sumando la afectación en la integridad, disponibilidad y confidencialidad a cada activo teniendo como máximo valor 21 y minino 1. Se consideran los descriptores de rangos como: “muy bajo”, “bajo”, “moderado”, “alto” y “muy alto” y los valores en base a lo calculado en la Tabla 23-3 considerando los siguientes criterios:

Un activo va a ser afectado totalmente si su ponderación es 3 y parcialmente si su ponderación es igual que dos y mínimamente si es 1. Por lo que se establece los siguientes rangos en función a la cantidad de activos que están siendo afectados total y parcialmente:

Rango 1-3: Representa que solo está siendo afectado un activo totalmente o que dos activos se ven afectados en máximo dos aspectos con respecto a la confiabilidad, disponibilidad e integridad y no pondría en riesgo a la empresa.
Rango 4-8: Representa que solo está siendo afectado dos activos totalmente o están siendo afectados como máximo 4 activos parcialmente, lo cual si va a afectar a ciertas áreas de la empresa.
Rango 9-13: Representa que están siendo afectados tres activos totalmente o están siendo afectados 7 activos parcialmente, esta cantidad de activos si va a afectar el funcionamiento de la empresa pues representa casi el 50% de los activos analizaos están siendo afectados totalmente o que todos los activos se encuentras parcialmente comprometidos.

Rango 14-18: Representa que están siendo afectados cuatro activos totalmente o están siendo afectados 7 activos, esta cantidad de activos si afecta el funcionamiento de la empresa pues representa el 50% de los activos comprometidos o que todos los activos se encuentran comprometidos y no pueden garantizar un adecuado nivel de confiabilidad, disponibilidad e integridad.

Rango 19-21: Representa que están siendo afectados como mínimo seis activos totalmente o están siendo afectados los 7 activos, esta cantidad de activos comprometidos podría llegar a cesar las funciones de la empresa pues no se podría garantizar la confiabilidad, disponibilidad e integridad de los datos que procesan estos activos.

Tabla 13-3: Impacto del riesgo

NIVEL	CONCEPTO	DESCRIPCIÓN (En caso de presentarse el hecho)	SEGURIDAD DE LA INFORMACIÓN
1-3	**Muy Bajo**	No afecta el funcionamiento de la empresa	Afecta a una actividad del proceso.
4-8	**Bajo**	Afecta a ciertos departamentos de la empresa	Afecta a una persona, grupo de personas
9-13	**Moderado**	Puede afectar parcialmente el funcionamiento a de la empresa	Afecta a un conjunto de datos personales o en la realización de proceso.
14-18	**Alto**	Pone en riesgo el funcionamiento a la empresa	Afecta a varios de datos personales o a uno o varios procesos de la organización.
19-21	**Muy Alto**	Cese de funciones de la empresa	Afecta toda la organización. Sanciones legales.

Realizado por: Merino. Katherine, 2022.

3.13.7. Valoración de los riesgos

Considerando los valores de probabilidad y la valoración del impacto asignado a cada amenaza se obtiene el siguiente rango de valoración del riesgo y se procede a determinar la tolerancia que se va a tener al riesgo y el nivel de acción requerido.

Para la realización de la dimensión del riesgo y el mapa de calor se consideran las recomendaciones de IS0 31000:2018 e ISO 31010:2019 que establecen que a los riesgos se los debe establecer elementos cualitativos en base a un análisis y criterios con el fin de establecer acciones y tomar de decisiones de acuerdo con la capacidad de manejo del riesgo (Escuela Europea de Excelencia, Cómo realizar la evaluación de riesgos según ISO 31000:2018), siendo un análisis recomendó por ISO 31010:2019 el impacto del riesgo sobre el negocio.

Para establecer los límites se consideran como al tener una probabilidad muy alta va impactando a la empresa los siguientes rangos:

0,1-1: Representa que se va a tener una muy alta probabilidad y un muy bajo impacto o una probabilidad muy baja y un impacto moderado, es decir no afecta en gran medida a la empresa y esta podría asumir el riesgo.

1,1-3: Representa que se va a tener una muy alta probabilidad y un muy bajo impacto o una probabilidad muy baja y un impacto alto, es decir no afecta en gran medida a la empresa y esta podría asumir el riesgo.

3,1-6: Representa que se va a tener una muy alta probabilidad y un bajo impacto o una probabilidad baja y un impacto muy alto, en este caso al incrementarse el nivel de impacto, es decir que el funcionamiento de la empresa se ve afectado.

6,1-12: Representa que se va a tener una muy alta probabilidad y un impacto moderado o una probabilidad moderad y un impacto muy alto, para este nivel el funcionamiento de la empresa está comprometido en gran medida ya que todos los activos no están funcionando correctamente.

12,01-21: Representa que se va a tener una alta y muy alta probabilidad y un impacto alto y muy alto para este caso los todos los activos estarían comprometidos y la empresa debería cesar sus funciones.

Tabla 14-3: Valoración de los riesgos

DIMENSIÓN DEL RIESGO	RANGO ASIGNADO	ACCIÓN REQUERIDA
Riesgo Extremo	12,01-21	Evitar el riesgo aplicando controles que reduzcan el nivel de probabilidad, reducir el riesgo empleando controles orientados a minimizar el impacto.
Riesgo Alto	6,1-12	Evitar o mitigar el riesgo aplicando medidas adecuadas y aprobadas, para trasladarlo a la zona de riesgo moderado o a su vez compartir y/o transferir el riesgo.
Riesgo Moderado	3,1-6	Evitar o mitigar el riesgo aplicando prontamente medidas que permitan reducir o compartir el riesgo.
Riesgo Bajo	1,1-3	Asumir el riesgo. Mitigar el riesgo con acciones detectivas y preventivas.
Riesgo Muy Bajo	0,1-1	Asumir el riesgo. Mitigar el riesgo con acciones administrativas.

Realizado por: Merino. Katherine, 2022.

Del dimensionamiento anterior del riesgo se obtiene el siguiente mapa de calor que se genera multiplicando la probabilidad por el impacto.

Tabla 15-3: Mapa de calor

			IMPACTO																				
			Muy Bajo			Bajo					Moderado					Alto					Muy Alto		
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
PROBABILIDAD	Muy baja	0,10	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9	1	1,1	1,2	1,3	1,4	1,5	1,6	1,7	1,8	1,9	2	2,1
		0,20	0,2	0,4	0,6	0,8	1	1,2	1,4	1,6	1,8	2	2,2	2,4	2,6	2,8	3	3,2	3,4	3,6	3,8	4	4,2
	Baja	0,30	0,3	0,6	0,9	1,2	1,5	1,8	2,1	2,4	2,7	3	3,3	3,6	3,9	4,2	4,5	4,8	5,1	5,4	5,7	6	6,3
		0,40	0,4	0,8	1,2	1,6	2	2,4	2,8	3,2	3,6	4	4,4	4,8	5,2	5,6	6	6,4	6,8	7,2	7,6	8	8,4

	Moderada	0,50	0,5	1	1,5	2	2,5	3	3,5	4	4,5	5	5,5	6	6,5	7	7,5	8	8,5	9	9,5	10	10,5
		0,60	0,6	1,2	1,8	2,4	3	3,6	4,2	4,8	5,4	6	6,6	7,2	7,8	8,4	9	9,6	10,2	10,8	11,4	12	12,6
	Alta	0,70	0,7	1,4	2,1	2,8	3,5	4,2	4,9	5,6	6,3	7	7,7	8,4	9,1	9,8	10,5	11,2	11,9	12,6	13,3	14	14,7
		0,80	0,8	1,6	2,4	3,2	4	4,8	5,6	6,4	7,2	8	8,8	9,6	10,4	11,2	12	12,8	13,6	14,4	15,2	16	16,8
	Muy alta	0,90	0,9	1,8	2,7	3,6	4,5	5,4	6,3	7,2	8,1	9	9,9	10,8	11,7	12,6	13,5	14,4	15,3	16,2	17,1	18	18,9
		1,00	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
			EVALUACIÓN DE RIESGO																				

Realizado por: Merino. Katherine, 2022.

Para determinar la aceptabilidad del riesgo se considera la siguiente tabla:

Tabla 16-3: Aceptabilidad del Riesgo.

NIVEL DEL RIESGO	ACEPTABILIDAD DEL RIESGO
Extremo	No aceptable
Alto	Aceptable
Moderado	
Bajo	
Muy Bajo	

Fuente: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1815-59362012000200002&lng=es&nrm=iso

Realizado por: Medardo Ulloa. 2012

Considerando la aceptabilidad del riesgo se establece las acciones para aplicarse según la zona de riesgo:

Tabla 17-3: Acciones según la zona de riesgo

ZONA	ACCIÓN REQUERIDA
Zona de Riesgo Mínimo	**Asumir el Riesgo:** Cuando el nivel de exposición del riesgo es adecuado y por lo tanto se acepta.
Zona de Riesgo Aceptable	**Asumir el Riesgo:** Cuando el nivel de exposición del riesgo es adecuado y por lo tanto se acepta.
Zona de Riesgo Moderado	**Mitigar o Evitar el Riesgo:** Cuando se requiere fortalecer los controles existentes y/o agregar nuevos controles.
Zona de Riesgo Importante	**Mitigar o Evitar el Riesgo: Se debe** Implementar controles adicionales fortaleciendo los actuales.
Zona de Riesgo Inaceptable	**Evitar el Riesgo:** Implementar acciones inmediatas que para reducir la probabilidad y el impacto de materialización.

Realizado por: Merino. Katherine, 2022.

3.13.8. Cálculo del impacto para cada amenaza

Tabla 18-3: Evaluación de los riesgos

ID		[D]	[COM]	[HW]	[L]	[Media]	[P]	[SW]	IMPACTO	IMPACTO	
[A1]	**[D]**	1	0	0	0	1	0	1	3	9	Moderado
	[I]	1	0	0	0	1	0	1	3		
	[C]	1	0	0	0	1	0	1	3		

[A2]	**[D]**	1	1	1	0	1	0	1	5	15	Alto
	[I]	1	1	1	0	1	0	1	5		
	[C]	1	1	1	0	1	0	1	5		
[A3]	**[D]**	0	0	0	0	0	0	0	0	1	Muy Bajo
	[I]	1	0	0	0	0	0	0	1		
	[C]	0	0	0	0	0	0	0	0		
[A4]	**[D]**	0	0	0	0	0	1	0	1	1	Muy Bajo
	[I]	0	0	0	0	0	0	0	0		
	[C]	0	0	0	0	0	0	0	0		
[A5]	**[D]**	0	0	0	0	0	0	1	1	3	Muy Bajo
	[I]	0	0	0	0	0	0	1	1		
	[C]	0	0	0	0	0	0	1	1		
[A6]	**[D]**	0	0	0	0	0	0	0	0	6	Bajo
	[I]	0	0	0	0	0	0	0	0		
	[C]	1	1	0	1	1	1	1	6		
[A7]	**[D]**	0	0	0	0	0	0	1	1	3	Muy Bajo
	[I]	0	0	0	0	0	0	1	1		
	[C]	0	0	0	0	0	0	1	1		
[A8]	**[D]**	0	1	0	1	1	0	1	4	8	Bajo
	[I]	0	1	0	1	1	0	1	4		
	[C]	0	0	0	0	0	0	0	0		
[A9]	**[D]**	1	1	0	0	0	0	1	3	9	Moderado
	[I]	1	1	0	0	0	0	1	3		
	[C]	1	1	0	0	0	0	1	3		
[A10]	**[D]**	0	0	0	0	0	0	0	0	1	Muy Bajo
	[I]	0	0	0	0	0	0	0	0		
	[C]	0	1	0	0	0	0	0	1		
[A11]	**[D]**	0	0	0	0	0	0	0	0	5	Bajo
	[I]	0	0	0	0	0	0	0	0		
	[C]	1	1	0	1	1	0	1	5		

Realizado por: Merino. Katherine, 2022.

CAPÍTULO IV

4. RESULTADOS Y DISCUSIÓN

4.1. Presentación de resultados

A continuación, se presenta los resultados obtenidos de la investigación realizada en la empresa MUNDOTRONIC y los criterios de sus ponderaciones considerando las variables de la investigación y el cumplimiento de los objetivos de esta.

También se presenta la etapa posterior a la implementación del Marco referencial de seguridad para reducir riesgos en el tratamiento de datos para determinar su madurez en el tratamiento de datos Personales y el cumplimiento de con lo estipulado en la Ley Orgánica de Telecomunicaciones.

4.1.1. Análisis de resultados de la situación inicial

Dado a que los riesgos a los que están expuesto los datos de los cliente, usuario o abonados han sido identificados, la probabilidad de ocurrencia de los mismo se puede obtener mediante las respuestas realizadas al personal de la empresa sobre la situación actual de la misma. Se crea una encuesta en base a las amenazas identificadas con un total de (24) preguntas a realizarse, tomando como referencia ciertas preguntas relacionadas a esta investigación del listado de cumplimiento normativo del RGPD. (Agencia Española de Protección de Datos, 2018)

A continuación, se presenta los resultados obtenidos de la encuesta realizada al personal del proveedor de servicios de acceso a internet MUNDOTRONIC de la ciudad de Riobamba. Dicha encuesta está realizada en base a las amenazas que se enfrenta los datos personales que están siendo tratados dentro de la organización. Además, se presenta el nivel de satisfacción sobre el cumplimiento con lo estipulado con la Ley Orgánica de Telecomunicaciones.

De la encuesta realizada se establece la probabilidad de ocurrencia de la que la amenazase materialice en función de a los promedios de las respuestas de las preguntas correspondiente a cada amenaza.

Del nivel de satisfacción se estable el porcentaje de cumplimiento de la Ley Orgánica de Telecomunicaciones

Para el cálculo de la probabilidad de la materialización de la amenaza se aplica la siguiente fórmula:

$$Probabilidad = \frac{Promedio\ de\ respuestas\ negativas}{Total\ de\ la\ Población\ encuestada}$$

Total, población encuestada = (5) personas

Tabla 1-4: Resultados de la encuesta realizada en la situación inicial

ID	N°	PREGUNTAS	SI	NO	PORCENTAJE (SI)	PORCENTAJE (NO)	TOTAL	PROMEDIO DE LAS RESPUESTAS DE NO	PROBABILIDAD	CUMPLE SATISFACTORIAMENTE	CUMPLE PARCIALMENTE	NO CUMPLE	EVIDENCIA
[A1]	1	¿Existen procedimientos de seguridad para evitar la pérdida, destrucción o daño accidental?	0	5	0%	100%	100%	4,5	0,9			x	No registra
	2	¿Existen procedimientos que restringa el acceso a los diferentes tipos de datos?	1	4	20%	80%	100%				x		Listado de responsabilidades en el contrato de trabajo
[A2]	3	¿Para determinar las medidas a aplicar se tiene en cuenta el alcance, contexto y fines del tratamiento, así como riesgos de probabilidad y los derechos de las personas físicas?	4	1	80%	20%	100%	3	0,6		x		Proformas de los softwares y hardware a implementar en sistema de red
	4	¿Existe un proceso de verificación, evaluación y valoración regular de la eficacia de las medidas técnicas y organizativas implementadas para garantizar la seguridad del tratamiento?	0	5	0%	100%	100%					x	No registra
[A3]	5	¿Existen procedimientos que indiquen la forma de uso de los sistemas y equipos?	5		100%	0%	100%	5	1		x		Software y equipos de seguridad
	6	¿Existe medidas para asegurar la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico?	0	5	0%	100%	100%					x	No registra
[A4]	7	¿Existen procesos que permitan la continuidad del funcionamiento correcto de la organización?	0	5	0%	100%	100%	5	1			x	No registra
	8	¿Existen medidas técnicas y organizativas apropiadas que garanticen un nivel de seguridad adecuado de protección contra el riesgo?	5		100%	0%	100%				x		Acciones de respuestas a incidentes
[A5]	9	¿Se ha establecido un procedimiento para identificar y gestionar las brechas de seguridad?	0	5	0%	100%	100%	5	1			x	No registra
	10	¿Existe procesos de verificación, evaluación y valoración de la eficacia de las medidas técnicas y organizativas	0	5	0%	100%	100%					x	No registra

		aplicadas para garantizar la seguridad del tratamiento de datos personales?											
[A6]	11	¿Se ha establecido procedimientos de eliminación segura de información de dispositivos que haya cumplido con su vida útil?	0	5	0%	100%	100%	5	1			x	No registra
	12	¿Se ha establecido procedimientos de protección de datos en ambientes de prueba?	0	5	0%	100%	100%					x	No registra
	13	¿Se ha establecido procesos que restrinjan el acceso a los datos?	0	5	0%	100%	100%					x	No registra
[A7]	14	¿Se ha implementado procedimientos para identificar y gestionar las brechas de seguridad?	4	1	80%	20%	100%	3	0,6		x		Software y equipos de seguridad
	15	¿Existe procedimientos que se identifiquen procedimientos para salvaguardar los aplicativos?	0	5	0%	100%	100%					x	No registra
[A8]	16	¿Existe documentación que registre las medidas técnicas y organizativas apropiadas al riesgo de los tratamientos?	0	5	0%	100%	100%	4	0,8			x	No registra
	17	¿Se han establecido medidas para asegurar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento?	2	3	40%	60%	100%					x	Acciones de respuestas a incidentes
[A9]	18	¿Existen procedimientos de accesos a los sistemas solo por personal autorizado?	2	3	40%	60%	100%	4	0,8		x		Listado de responsabilidades en el contrato de trabajo
	19	¿Existen procedimientos de restricción de acceso a la información?	0	5	0%	100%	100%					x	No registra
[A10]	20	¿Existen procesos de seguridad en las redes de datos de la organización?	5	0	100%	0%	100%	2,5	0,5		x		Software y equipos de seguridad
	21	¿Existe procesos de documentación de brechas de seguridad que afecten a la información?	0	5	0%	100%	100%					x	No registra
[A11]	22	¿Existe procedimientos que las personas autorizadas para tratar datos personales se comprometen a respetar la confidencialidad o están sujetas a una obligación de confidencialidad de naturaleza legal?	0	5	0%	100%	100%	5	1			x	No registra
	23	¿Existen procedimientos para la transferencia de información?	0	5	0%	100%	100%					x	No registra
	24	¿Existe cláusulas que indique que se requiere autorización del propietario de los datos personales para realizar un tratamiento?	0	5	0%	100%	100%					x	No registra

Realizado por: Merino. Katherine, 2022.

Para determinar el estado de cumplimiento se considera la siguiente tabla

Tabla 2-4: Estado de las acciones implementadas.

ESTADO	DESCRIPCIÓN
Cumple satisfactoriamente	Existe, es gestionado, se está cumpliendo con lo que estipula la norma ISO27001 versión 2013 y la Ley Orgánica de Telecomunicaciones, está documentado, es comunicado y aplicado. Cumple 100%.
Cumple parcialmente	Lo que la norma requiere la norma ISO27001 versión 2013 y la Ley Orgánica de Telecomunicaciones se está haciendo de manera parcial, se está haciendo diferente, no está documentado, se definió y aprobó, pero no se gestiona.
No cumple	No existe y/o no se está aplicando.

Realizado por: Merino. Katherine, 2022.

La tabla 23-4: Resultados de la encuesta realizada presenta los resultados de la encuesta en función de lo que respondieron el personal de MUNDOTRONIC sobre el conocimiento de aplicación de procedimiento para asegurar los datos personales considerando si la respuesta fue SI o NO. También nos presenta el estado de cumplimento de la empresa con respecto a los requerimientos de la norma ISO27001 versión 2013 y la Ley Orgánica de Telecomunicaciones.

La probabilidad calculada indica que tan probable es la materialización de la amenaza. A continuación, se presenta el cálculo del riesgo al multiplicar el impacto por la probabilidad. De los cálculos realizados se obtiene el nivel de riesgo con respecto a la disponibilidad, integridad y confiabilidad de los datos dependiendo la amenaza. También se presenta el nivel de riesgo de materialización de la amenaza.

Para el cálculo del Riesgo se aplica la siguiente fórmula:

$$Riesgo = Impacto\ x\ Probabilidad$$

Teniendo como un máximo riesgo la ponderación de 21 y como mínimo el valor de 0,1. Para determinar el nivel de riesgo y la zona de Riesgo se considera la Tabla 19-3: Valoración de los riesgos y Tabla 21-3: Acciones según la zona de riesgo respectivamente.

Tabla 3-4: Nivel de riesgo de la materialización de las amenzas (Situación inicial)

ID	AMENAZA		[D]	[COM]	[HW]	[L]	[Media]	[P]	[SW]	IMPACTO	IMPACTO		PROBABILIDAD GENERAL		PONDERANCIA (Riesgo)	
[A1]	**Error de usuarios**	**[D]**	1	0	0	0	1	0	1	3	9	Moderado	0,9	Muy Alta	8,1	**Alto**
		[I]	1	0	0	0	1	0	1	3						
		[C]	1	0	0	0	1	0	1	3						
[A2]	**Error del Administrador**	**[D]**	1	1	1	0	1	0	1	5	15	Alto	0,6	Moderada	9	**Alto**
		[I]	1	1	1	0	1	0	1	5						
		[C]	1	1	1	0	1	0	1	5						
[A3]	**Error de configuración**	**[D]**	0	0	0	0	0	0	0	0	1	Muy Bajo	1	Muy Alta	1	**Muy Bajo**
		[I]	1	0	0	0	0	0	0	1						
		[C]	0	0	0	0	0	0	0	0						
[A4]	**Deficiencia en la organización**	**[D]**	0	0	0	0	0	1	0	1	1	Muy Bajo	1	Muy Alta	1	**Muy Bajo**
		[I]	0	0	0	0	0	0	0	0						
		[C]	0	0	0	0	0	0	0	0						
[A5]	**Difusión de software malicioso**	**[D]**	0	0	0	0	0	0	1	1	3	Muy Bajo	1	Muy Alta	3	**Bajo**
		[I]	0	0	0	0	0	0	1	1						
		[C]	0	0	0	0	0	0	1	1						
[A6]	**Fuga de información**	**[D]**	0	0	0	0	0	0	0	0	6	Bajo	1	Muy Alta	6	**Moderado**
		[I]	0	0	0	0	0	0	0	0						
		[C]	1	1	0	1	1	1	1	6						
[A7]	**Vulnerabilidades en software**	**[D]**	0	0	0	0	0	0	1	1	3	Muy Bajo	0,6	Moderada	1,8	**Bajo**
		[I]	0	0	0	0	0	0	1	1						
		[C]	0	0	0	0	0	0	1	1						
[A8]	**Error de mantenimiento**	**[D]**	0	1	0	1	1	0	1	4	8	Bajo	0,8	Alta	6,4	**Alto**
		[I]	0	1	0	1	1	0	1	4						
		[C]	0	0	0	0	0	0	0	0						
[A9]	**Suplantación de identidad**	**[D]**	1	1	0	0	0	0	1	3	9	Moderado	0,8	Alta	7,2	**Alto**
		[I]	1	1	0	0	0	0	1	3						
		[C]	1	1	0	0	0	0	1	3						
[A10]	**Interceptación de información**	**[D]**	0	0	0	0	0	0	0	0	1	Muy Bajo	0,5	Moderada	0,5	**Muy Bajo**
		[I]	0	0	0	0	0	0	0	0						
		[C]	0	1	0	0	0	0	0	1						
[A11]	**Revelación de la información**	**[D]**	0	0	0	0	0	0	0	0	5	Bajo	1	Muy Alta	5	**Moderado**
		[I]	0	0	0	0	0	0	0	0						
		[C]	1	1	0	1	1	0	1	5						

Realizado por: Merino. Katherine, 2022.

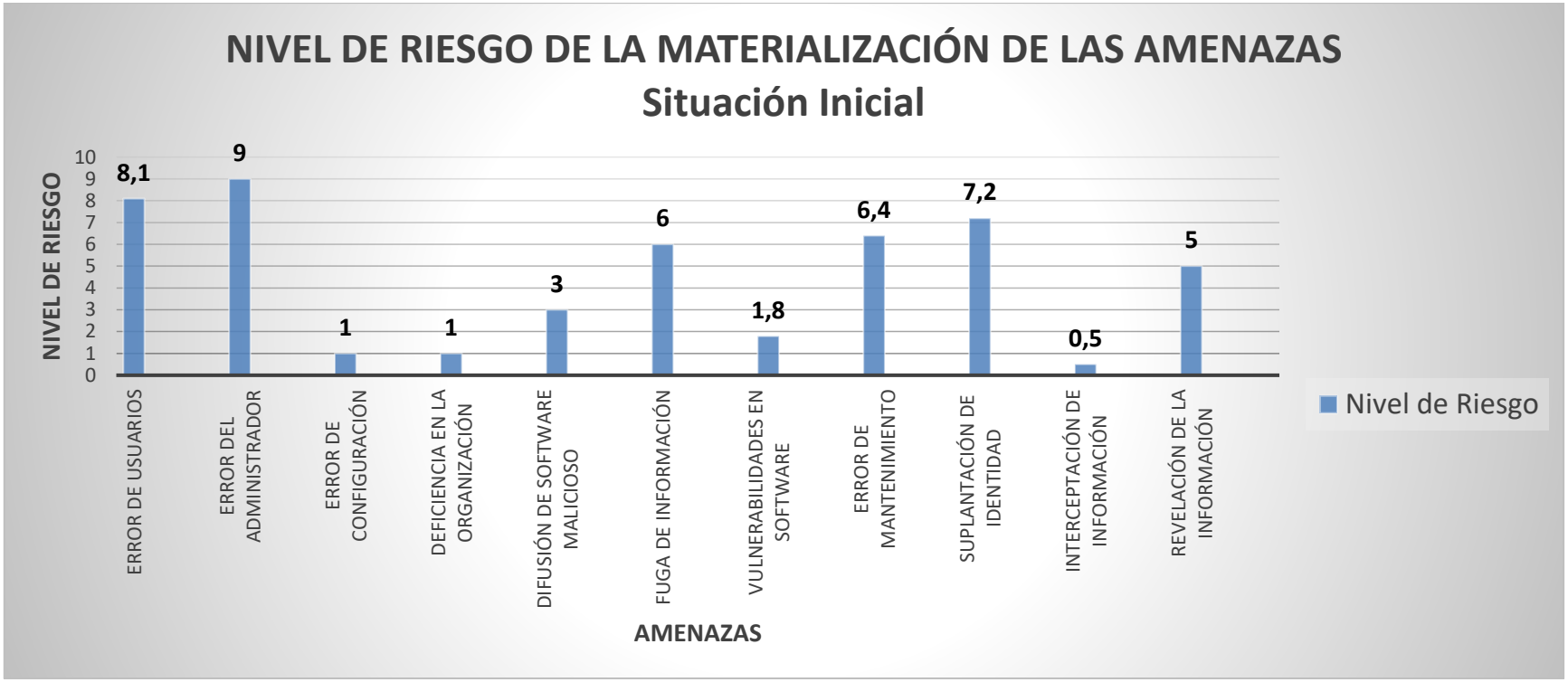


Gráfico 1-4: Nivel de riesgo de materialización de las Amenazas (Situación Inicial)
Realizado por: Merino. Katherine, 2022.

De los datos obtenidos se concluye que las amenazas con mayores riesgos de materializarse son:

- Error de usuario
- Error del administrador
- Fuga de información
- Error de manteniendo
- Suplantación de identidad
- Revelación de la información

Todas estas amenazas con un nivel de riesgo entre alto y moderado. Es decir, afectaría parcialmente el funcionamiento de la empresa y un conjunto de datos personales se verían afectos. Al tener un riesgo moderado también implica que los procesos no están funcionando correctamente de acuerdo con la Tabla 20-3: Valoración de los riesgos y Tabla 23-3: Acciones según la zona de riesgo. Afectando directamente a la disponibilidad, integridad y confidencialidad de los datos.

4.1.2. Análisis de resultados de la situación Post-Implementación

A continuación, se presenta los resultados luego de haber creado los procedimientos basados en la norma ISO 27001, se procede a nuevamente a encuestar y se aplica el mismo procedimiento de análisis que se realizó en la situación inicial, obteniendo los siguientes resultados:

Tabla 4-4: Resultados de la encuesta realizada en la situación Post-Implementación

ID	N°	PREGUNTAS	SI	NO	PORCENTAJE (SI)	PORCENTAJE (NO)	TOTAL	PROMEDIO DE LAS RESPUESTAS DE NO	PROBABILIDAD	CUMPLE SATISFACTORIAMENTE	CUMPLE PARCIALMENTE	NO CUMPLE	EVIDENCIA
[A1]	1	¿Existen procedimientos de seguridad para evitar la pérdida, destrucción o daño accidental?	5		100%	0%	100%	1,00	0,20		x		DP_001 MSPD_001
	2	¿Existen procedimientos que restringa el acceso a los diferentes tipos de datos?	4	1	80%	20%	100%			x			MS_002
[A2]	3	¿Para determinar las medidas a aplicar se tiene en cuenta el alcance, contexto y fines del tratamiento, así como riesgos de probabilidad y los derechos de las personas físicas?	4	1	80%	20%	100%	1,00	0,20		x		MS_007 DP_016 MSPD_001

	4	¿Existe un proceso de verificación, evaluación y valoración regular de la eficacia de las medidas técnicas y organizativas implementadas para garantizar la seguridad del tratamiento?	4	1	80%	20%	100%				x		MS_010 MS_011
[A3]	5	¿Existen procedimientos que indiquen la forma de uso de los sistemas y equipos?	4	1	80%	20%	100%	0,50	0,10		x		DP_012 DP_013 DP_002
	6	¿Existe medidas para asegurar la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico?	5	0	100%	0%	100%			x			MS_009 DP_0010 DP_008
[A4]	7	¿Existen procesos que permitan la continuidad del funcionamiento correcto de la organización?	4	1	80%	20%	100%	1,00	0,20		x		MS_008 MSPD_001
	8	¿Existen medidas técnicas y organizativas apropiadas que garanticen un nivel de seguridad adecuado de protección contra el riesgo?	5		100%	0%	100%			x			MSPD_001
[A5]	9	¿Se ha establecido un procedimiento para identificar y gestionar las brechas de seguridad?	4	1	80%	20%	100%	1,00	0,20	x			MS_006 MS_007 DP_013
	10	¿Existe procesos de verificación, evaluación y valoración de la eficacia de las medidas técnicas y organizativas aplicadas para garantizar la seguridad del tratamiento de datos personales?	4	1	80%	20%	100%				x		MS_011
[A6]	11	¿Se ha establecido procedimientos de eliminación segura de información de dispositivos que haya cumplido con su vida útil?	4	1	80%	20%	100%	0,67	0,13	x			DP_008
	12	¿Se ha establecido procedimientos de protección de datos en ambientes de prueba?	5	0	100%	0%	100%			x			DP_015
	13	¿Se ha establecido procesos que restrinjan el acceso a los datos?	4	1	80%	20%	100%				x		MS_002

[A7]	14	¿Se ha implementado procedimientos para identificar y gestionar las brechas de seguridad?	5	0	100%	0%	100%	0,50	0,10	x			MS_003
	15	¿Existe procedimientos que se identifiquen procedimientos para salvaguardar los aplicativos?	4	1	80%	20%	100%				x		DP_012 MS_006
[A8]	16	¿Existe documentación que registre las medidas técnicas y organizativas apropiadas al riesgo de los tratamientos?	5	0	100%	0%	100%	0,50	0,10		x		MS_007
	17	¿Se han establecido medidas para asegurar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento?	4	1	80%	20%	100%				x		MS_009 MS_006 DP_0010
[A9]	18	¿Existen procedimientos de accesos a los sistemas solo por personal autorizado?	4	1	80%	20%	100%	1,00	0,20	x			DP_005 DP_006 MS_001
	19	¿Existen procedimientos de restricción de acceso a la información?	4	1	80%	20%	100%			x			MS_002
[A10]	20	¿Existen procesos de seguridad en las redes de datos de la organización?	5	0	100%	0%	100%	0,50	0,10		x		MS_004 DP_013
	21	¿Existe procesos de documentación de brechas de seguridad que afecten a la información?	4	1	80%	20%	100%				x		MS_003 MS_007
[A11]	22	¿Existe procedimientos que las personas autorizadas para tratar datos personales se comprometen a respetar la confidencialidad o están sujetas a una obligación de confidencialidad de naturaleza legal?	4	1	80%	20%	100%	1,00	0,20		x		MS_005 MS_005
	23	¿Existen procedimientos para la transferencia de información?	4	1	80%	20%	100%			x			DP_014
	24	¿Existe cláusulas que indique que se requiere autorización del propietario de los datos personales para realizar un tratamiento?	4	1	80%	20%	100%			x			MS_005 DP_016

Realizado por: Merino. Katherine, 2022.

Tabla 5-4: Nivel de riesgo de la materialización de las amenazas (Post-Implementación)

ID	AMENAZA		[D]	[COM]	[HW]	[L]	[Media]	[P]	[SW]	IMPACTO	IMPACTO		PROBABILIDAD GENERAL		PONDERANCIA (Riesgo)	
[A1]	Error de usuarios	[D]	1	0	0	0	1	0	1	3	9	Moderado	0,20	Muy Baja	1,80	**Bajo**
		[I]	1	0	0	0	1	0	1	3						
		[C]	1	0	0	0	1	0	1	3						
[A2]	Error del Administrador	[D]	1	1	1	0	1	0	1	5	15	Alto	0,20	Muy Baja	3,00	**Bajo**
		[I]	1	1	1	0	1	0	1	5						
		[C]	1	1	1	0	1	0	1	5						
[A3]	Error de configuración	[D]	0	0	0	0	0	0	0	0	1	Muy Bajo	0,10	Muy Baja	0,10	**Muy Bajo**
		[I]	1	0	0	0	0	0	0	1						
		[C]	0	0	0	0	0	0	0	0						
[A4]	Deficiencia en la organización	[D]	0	0	0	0	0	1	0	1	1	Muy Bajo	0,20	Muy Baja	0,20	**Muy Bajo**
		[I]	0	0	0	0	0	0	0	0						
		[C]	0	0	0	0	0	0	0	0						
[A5]	Difusión de software malicioso	[D]	0	0	0	0	0	0	1	1	3	Muy Bajo	0,20	Muy Baja	0,60	**Muy Bajo**
		[I]	0	0	0	0	0	0	1	1						
		[C]	0	0	0	0	0	0	1	1						
[A6]	Fuga de información	[D]	0	0	0	0	0	0	0	0	6	Bajo	0,13	Muy Baja	0,80	**Muy Bajo**
		[I]	0	0	0	0	0	0	0	0						
		[C]	1	1	0	1	1	1	1	6						
[A7]	Vulnerabilidades en software	[D]	0	0	0	0	0	0	1	1	3	Muy Bajo	0,10	Muy Baja	0,30	**Muy Bajo**
		[I]	0	0	0	0	0	0	1	1						
		[C]	0	0	0	0	0	0	1	1						
[A8]	Error de mantenimiento	[D]	0	1	0	1	1	0	1	4	8	Bajo	0,10	Muy Baja	0,80	**Muy Bajo**
		[I]	0	1	0	1	1	0	1	4						
		[C]	0	0	0	0	0	0	0	0						
[A9]	Suplantación de identidad	[D]	1	1	0	0	0	0	1	3	9	Moderado	0,20	Muy Baja	1,80	**Bajo**
		[I]	1	1	0	0	0	0	1	3						
		[C]	1	1	0	0	0	0	1	3						
[A10]	Interceptación de información	[D]	0	0	0	0	0	0	0	0	1	Muy Bajo	0,10	Muy Baja	0,10	**Muy Bajo**
		[I]	0	0	0	0	0	0	0	0						

		[C]	0	1	0	0	0	0	0	1						
[A11]	Revelación de la información	[D]	0	0	0	0	0	0	0	0	5	Bajo	0,20	Muy Baja	1,00	**Muy Bajo**
		[I]	0	0	0	0	0	0	0	0						
		[C]	1	1	0	1	1	0	1	5						

Realizado por: Merino. Katherine, 2022.

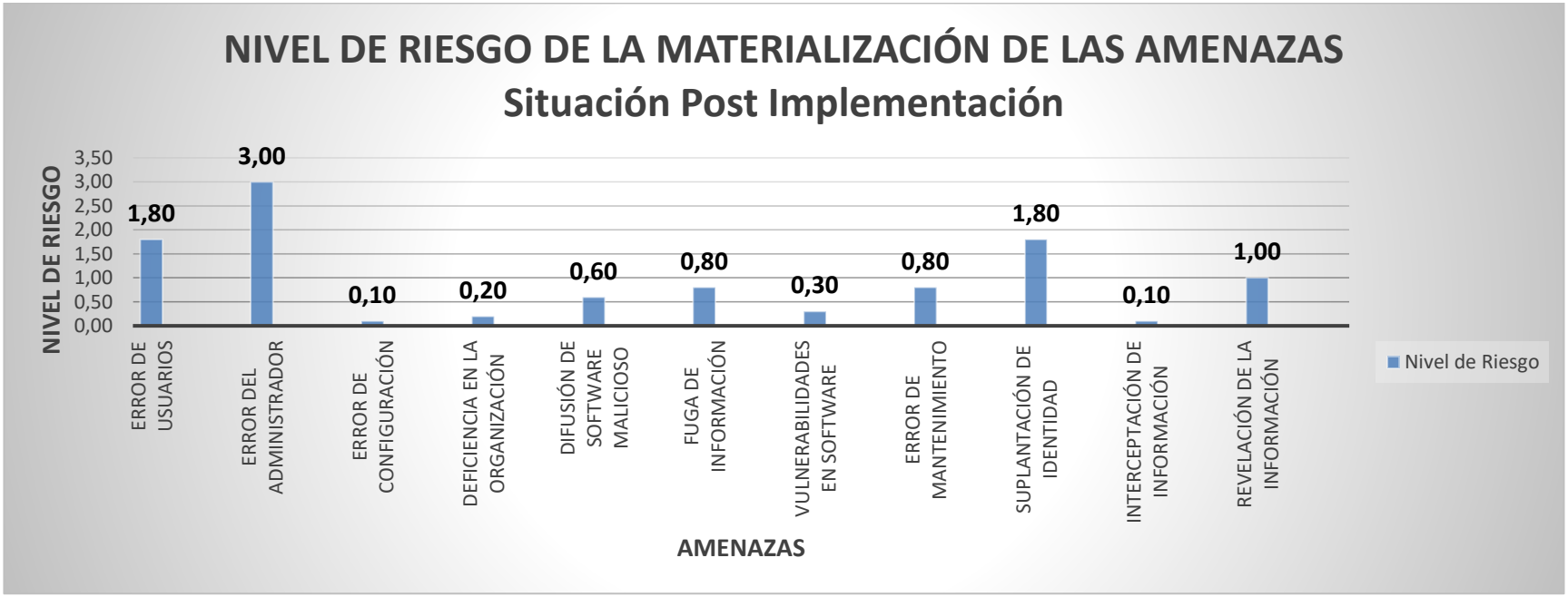


Gráfico 2-4: Nivel de riesgo de materialización de las Amenazas (Situación Post-Implementación)
Realizado por: Merino. Katherine, 2022.

De los resultados obtenidos se puede concluir que los niveles de riesgo han bajado considerablemente con respecto a la situación inicial de la empresa, tal como se muestra en la siguiente tabla de comparación.

Tabla 6-4: Nivel de riesgos Situación inicial- Post-Implementación

ID	AMENAZA	PONDERANCIA INICIAL (Riesgo)		PONDERANCIA POST-IMPLEMENTACIÓN (Riesgo)	
[A1]	Error de usuarios	8,10	Alto	1,80	Bajo
[A2]	Error del Administrador	9,00	Alto	3,00	Bajo
[A3]	Error de configuración	1,00	Muy Bajo	0,10	Muy Bajo
[A4]	Deficiencia en la organización	1,00	Muy Bajo	0,20	Muy Bajo
[A5]	Difusión de software malicioso	3,00	Bajo	0,60	Muy Bajo
[A6]	Fuga de información	6,00	Moderado	0,80	Muy Bajo
[A7]	Vulnerabilidades en software	1,80	Bajo	0,30	Muy Bajo
[A8]	Error de mantenimiento	6,40	Alto	0,80	Muy Bajo
[A9]	Suplantación de identidad	7,20	Alto	1,80	Bajo
[A10]	Interceptación de información	0,50	Muy Bajo	0,10	Muy Bajo
[A11]	Revelación de la información	5,00	Moderado	1,00	Muy Bajo

Realizado por: Merino. Katherine, 2022.

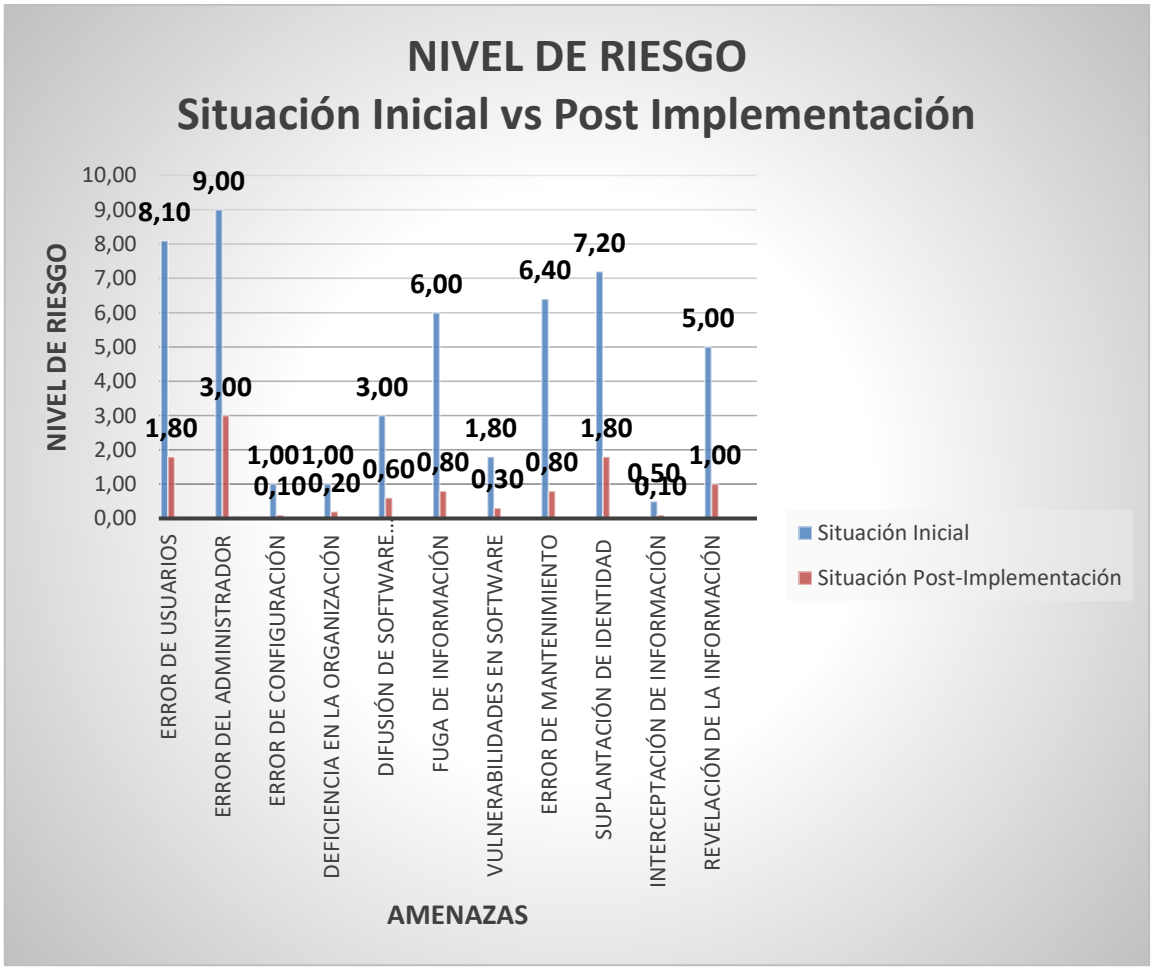


Gráfico 3-4: Niveles de riesgos Situación inicial- Post-Implementación

Realizado por: Merino. Katherine, 2022.

A continuación, se presenta el nivel del riesgo en porcentaje en la situación inicial y en la Post-Implementación, además el porcentaje de reducción del riesgo.

Tabla 7-4: Riesgo expresado en porcentaje

ID	AMENAZA	PONDERANCIA INICIAL (Riesgo)	PONDERANCIA POST-IMPLEMENTACIÓN (Riesgo)	PORCENTAJE DE REDUCCION DE RIESGO
[A1]	**Error de usuarios**	38,57%	8,57%	30,00%
[A2]	**Error del Administrador**	42,86%	14,29%	28,57%
[A3]	**Error de configuración**	4,76%	0,48%	4,29%
[A4]	**Deficiencia en la organización**	4,76%	0,95%	3,81%
[A5]	**Difusión de software malicioso**	14,29%	2,86%	11,43%
[A6]	**Fuga de información**	28,57%	3,81%	24,76%
[A7]	**Vulnerabilidades en software**	8,57%	1,43%	7,14%
[A8]	**Error de mantenimiento**	30,48%	3,81%	26,67%
[A9]	**Suplantación de identidad**	34,29%	8,57%	25,71%
[A10]	**Interceptación de información**	2,38%	0,48%	1,90%
[A11]	**Revelación de la información**	23,81%	4,76%	19,05%

Realizado por: Merino. Katherine, 2022.

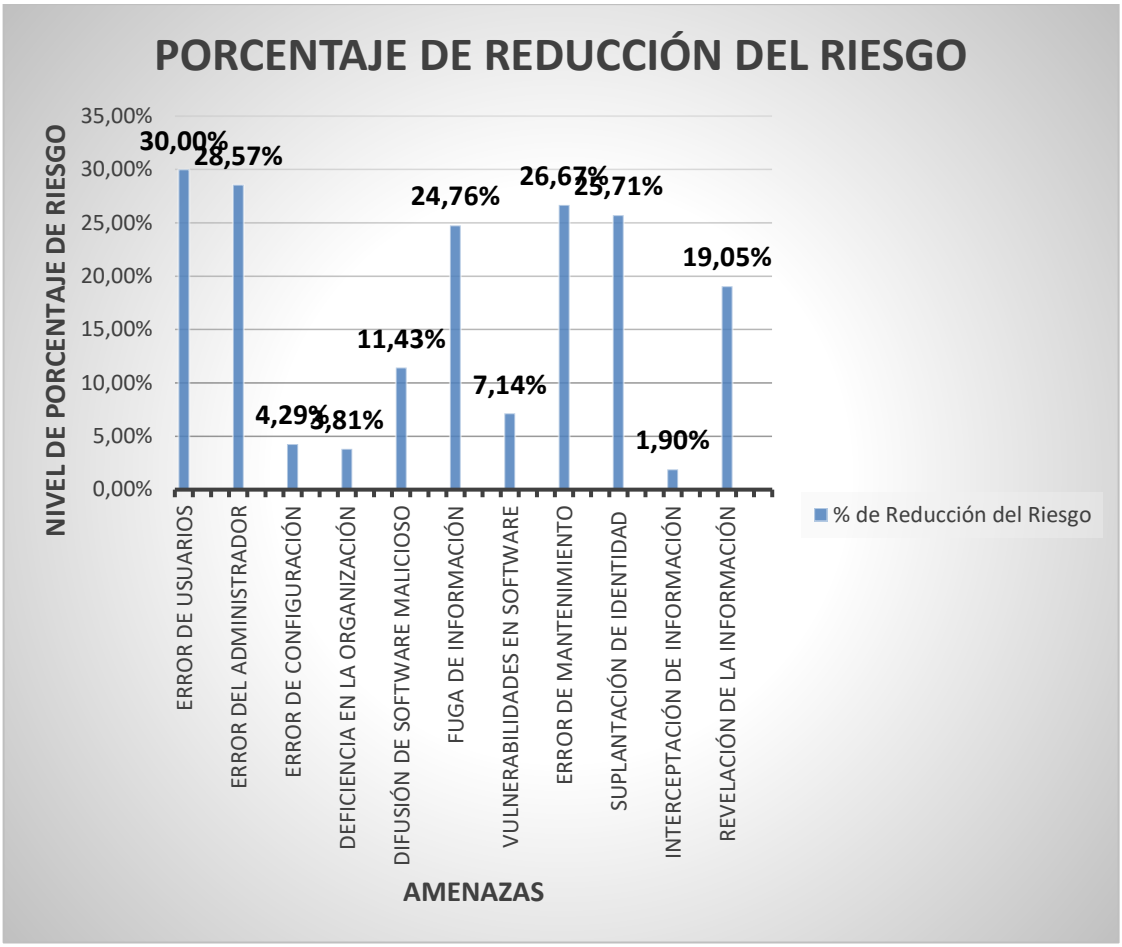


Gráfico 4-4: Porcentaje de reducción de riesgo

Realizado por: Merino. Katherine, 2022.

Como se puede observar la reducción de los niveles de riesgos en análisis inicial y en la post-implementación son significantes como para cambiar el estado del nivel de riesgo.

4.2. Comprobación de la Hipótesis

Para la presente investigación se aplica la prueba T-Student, la cual consiste en comprobar si la hipótesis es nula. Se la aplica cuando la población posee una distribución normal y la muestra es demasiado pequeña, utiliza la una estimación de desviación típica en lugar de un valor real.

4.2.1. Planteamiento de la Hipótesis

Hipótesis de investigación Hi: Al elaborar e implementar un marco referencial de seguridad utilizando ISO 27001 reducirá riesgos en el tratamiento de datos personales en empresas prestadoras de servicios de acceso a internet.

Hipótesis de Nula H_0: Al elaborar e implementar un marco referencial de seguridad utilizando ISO 27001 no reducirá riesgos en el tratamiento de datos personales en empresas prestadoras de servicios de acceso a internet.

$$H_o: \mu_{\bar{d}} = 0$$

Hipótesis Alternativa H_1: Al elaborar e implementar un marco referencial de seguridad utilizando ISO 27001 reducirá riesgos en el tratamiento de datos personales en empresas prestadoras de servicios de acceso a internet.

$$H_1: \mu_{\bar{d}} \neq 0$$

Donde $\mu_{\bar{d}}$ es la media de las medidas.

4.2.2. Nivel de significancia

Para la presente investigación se establece un nivel de significancia del 0,05, este valor permite juzgar si los resultados obtenidos son estadísticamente significativos y también determina la probabilidad de error.

Para esta investigación el nivel de significancia se lo representa como α (Alpha). Al establecer el valor de 0,05 nos indica un riesgo de error del 5%

$$\alpha=0,05$$

4.2.3. Estadístico de prueba

Para los datos obtenidos en los análisis de la situación inicial y en la Post-Implementación se utiliza la distribución T de Student que emplea las siguientes fórmulas matemáticas:

$$tc = \frac{\bar{d}}{\frac{S_d}{\sqrt{n}}}$$

$$S_d = \sqrt{\frac{\sum_{i=1}^{n}(d - \bar{d})^2}{n-1}}$$

Dónde:

t_c = Valor estadístico del procedimiento calculado.

$\bar{d}$ = Valor promedio o media aritmética de las diferencias entre los momentos antes y después.

S_d = Desviación estándar de las diferencias entre los momentos antes y después.

n = Tamaño de la muestra

4.2.4. Regla de decisión

Para identificar si se rechaza la hipótesis nula se consideran dos casos:

Caso 1: $t_c > t_\alpha$, *rechaza la hipotesis nula* $H0$

Caso 2: $Valor\ p < \alpha$, *se rechaza la hipotesis nula* $H0$

4.2.5. Conclusiones

Los datos obtenidos en la presente investigación fueron evaluados en la herramienta Análisis de Datos de Microsoft Excel, para el análisis de datos se selecciona la función T-Student.

Para la prueba de normalidad que permite aceptar la hipótesis y consideran todas las categorías de riesgo obtenidos en los análisis de la situación inicial y en la Post-Implementación tal como se muestra en la siguiente tabla:

Tabla 8-4: Datos inicial y Post-Implementación

ID	AMENAZA	PONDERANCIA INICIAL (Riesgo)	PONDERANCIA POST-IMPLEMENTACIÓN (Riesgo)
[A1]	**Error de usuarios**	8,10	1,80
[A2]	**Error del Administrador**	9,00	3,00
[A3]	**Error de configuración**	1,00	0,10
[A4]	**Deficiencia en la organización**	1,00	0,20
[A5]	**Difusión de software malicioso**	3,00	0,60
[A6]	**Fuga de información**	6,00	0,80
[A7]	**Vulnerabilidades en software**	1,80	0,30
[A8]	**Error de mantenimiento**	6,40	0,80
[A9]	**Suplantación de identidad**	7,20	1,80
[A10]	**Interceptación de información**	0,50	0,10
[A11]	**Revelación de la información**	5,00	1,00

Realizado por: Merino. Katherine, 2022.

Tabla 9-4: Resultados de la prueba T-Student

	Variable 1	Variable 2
Media	4,4545	0,9545
Varianza	9,6627	0,8247
Observaciones	11,0000	11,0000
Coeficiente de correlación de Pearson	0,8990	
Diferencia hipotética de las medias	0,0000	
Grados de libertad	10,0000	
Estadístico t	4,9898	
P(T<=t) una cola	0,0003	
Valor crítico de t (una cola)	1,8125	
P(T<=t) dos colas	0,0005	
Valor crítico de t (dos colas)	2,2281	

Realizado por: Merino. Katherine, 2022.

De la tabla anterior se puede apreciar que el promedio de riesgo de amenazas en la situación inicial es de 4,4545 mientras que en la Post-Implementación se reduce al 0,9545 obteniendo una diferencia de 3,5.

Para determinar si las acciones implementadas han reducido el nivel del riesgo se debe considerar el valor de P para dos colas para esta investigación se obtiene el valor de 0,0005, el cual es menor que α=0,05 lo cual indica que la hipótesis nula H_0 es rechazada **y** la hipótesis alternativa H_1 se acepta.

Por lo que se puede concluir que al elaborar e implementar un marco referencial de seguridad utilizando ISO 27001 reduce riesgos en el tratamiento de datos personales en empresas prestadoras de servicios de acceso a internet con un nivel de confianza del 95%.

4.2.6. Análisis de Controles necesarios para crear el Marco referencial de Seguridad

El presente análisis identifica los controles necesarios para cumplir con la Ley Orgánica de Telecomunicaciones, considerando también los documentos obligatorios para la ISO 27001:2013 y diversas recomendaciones.

Con respecto a la Ley Orgánica de Telecomunicaciones los valores serán:

Obligatorio: Si la Ley Orgánica de Telecomunicaciones obliga su cumplimiento.

No obligatorio: Si la Ley Orgánica de Telecomunicaciones no obliga su cumplimiento.

Los valores para la ISO 27001:2013 serán:

Obligatorio: Si la aplicación del control permite crear información documentada.

No obligatorio: Si la aplicación del control no permite crear información documentada.

Los prestadores de servicios de acceso a internet tendrán la posibilidad de indicar los controles a ser aplicados, debido a que no necesariamente tienen que aplicar, para lo cual deberán realizar la declaración de aplicabilidad indicando las razones.

Tabla 10-4: Dirección de gestión para la seguridad de la información

5.1 Dirección de gestión para la seguridad de la información		
Proporciona dirección de gestión y soporte para la seguridad de la información de acuerdo con los requisitos de negocio, leyes y regulaciones relevantes.		
Control	**LOT**	**ISO27001**
5.1.1	Obligatorio	Obligatorio
5.1.2	Obligatorio	Obligatorio

Realizado por: Merino. Katherine, 2022.

Análisis:

Este control es responsabilidad de la alta dirección debido a que es quien establece las políticas de seguridad que la organización aplicará de acuerdo con los requisitos y las legislaciones vigentes. Esta política debe periódicamente revisada para un correcto funcionamiento.

Recomendaciones:

- Aplicar ciclo de vida de revisión de contenido de las políticas de seguridad, considerando las siguientes etapas: creación, discusión, aprobación, difusión y consolidación.
- Crear la política según compatibles con el contexto y dirección estratégica de la organización.
- La dirección debe aprobar dichas políticas, además comprometerse a cumplirla en todo momento.
- Revisar periódicamente la política implementada.

Tabla 11-4: Organización interna

6.1 Organización interna		
Es necesario crear un marco de trabajo para la implementación y la operación de la seguridad de la información.		
Control	**LOT**	**ISO27001**
6.1.1	Obligatorio	No obligatorio
6.1.2	No obligatorio	No obligatorio
6.1.3	No obligatorio	No obligatorio
6.1.4	No obligatorio	No obligatorio
6.1.5	No obligatorio	No obligatorio

Realizado por: Merino. Katherine, 2022.

Análisis:

En este control la organización define los roles de los responsables de la información, los cuales se recogerán en un documento. Es necesario asignar un responsable de la seguridad, quien se encargará de la coordinación y control de todas las medidas de seguridad.

Recomendaciones:

- Asignar un responsable a cada proceso identificado.
- El responsable de la seguridad debe conocer los objetivos de negocio y encargarse de la asignación de los activos.

Tabla 12-4: Dispositivos móviles y teletrabajo

6.2 Dispositivos móviles y teletrabajo		
Asegurar la seguridad del teletrabajo y el uso de los aparatos móviles.		
Control	**LOT**	**ISO27001**
6.2.1	No obligatorio	No obligatorio
6.2.2	No obligatorio	No obligatorio

Realizado por: Merino. Katherine, 2022.

Análisis: Para la presente investigación no se considera este control, pero si recomendable en el caso de utilizar los dispositivos móviles como herramienta de trabajo

Recomendaciones:

- Identificar los dispositivos móviles que tendrán acceso a las aplicaciones corporativas.
- Limitar el acceso e impedir la instalación de aplicaciones sin la aprobación del administrador.

Tabla 13-4: Previo al empleo

7.1 Previo al empleo		
Los empleados y los contratistas deben comprender sus responsabilidades para los que son considerados.		
Control	**LOT**	**ISO27001**
7.1.1	No obligatorio	No obligatorio
7.1.2	No obligatorio	Obligatorio

Realizado por: Merino. Katherine, 2022.

Análisis:

Para la presente investigación no se considera este control.

Tabla 14-4: Durante el empleo

7.2 Durante el empleo		
Los empleados y contratistas deben conocer y cumplir con sus responsabilidades.		
Control	**LOT**	**ISO27001**
7.2.1	No obligatorio	No obligatorio
7.2.2	No obligatorio	No obligatorio
7.2.3	No obligatorio	No obligatorio

Realizado por: Merino. Katherine, 2022.

Análisis:

- Este control no se considera necesario para este caso de estudio.

Tabla 15-4: Terminación o cambio de empleo

7.3 Terminación o cambio de empleo		
Se debe proteger los intereses de la organización cuando se finaliza la relación laboral con un empleado.		
Control	**LOT**	**ISO27001**
7.3.1	No obligatorio	No obligatorio

Realizado por: Merino. Katherine, 2022.

Análisis:

Este control no se considera necesario para este caso de estudio.

Tabla 16-4: Responsabilidad por los activos

8.1 Responsabilidad por los activos		
Identificar activos organizativos y definir responsabilidades de protección apropiadas.		
Control	**LOT**	**ISO27001**
8.1.1	No obligatorio	Obligatorio
8.1.2	No obligatorio	No obligatorio

8.1.3	No obligatorio	Obligatorio
8.1.4	No obligatorio	No obligatorio

Realizado por: Merino. Katherine, 2022.

Análisis:

Este control no se considera necesario, pero sí recomendable ya que identificar todos los activos permite asignar a un propietario, en caso de rescisión de contrato, el empleado tendrá que devolver los activos.

Recomendaciones:

- Incluir cláusulas que indiquen que los activos deberán se inventariados, sus responsables y ser devueltos a la finalización de sus contratos.

Tabla 17-4: Clasificación de la información

8.2 Clasificación de la información		
La información debe recibir un nivel apropiado de protección de acuerdo con su importancia.		
Control	**LOT**	**ISO27001**
8.2.1	No obligatorio	No obligatorio
8.2.2	No obligatorio	No obligatorio
8.2.3	No obligatorio	No obligatorio

Realizado por: Merino. Katherine, 2022.

Análisis:

Este control no se considera necesario, pero sí recomendable ya que la información debe ser clasificada según la política de seguridad definida por la organización, para el uso de los activos se seguirá los procedimientos adoptados y dependerá de las restricciones de acceso.

Recomendaciones:

- Establecer una clasificación de acuerdo con el tipo de datos recolectado por la empresa.
- Disponer un registro histórico de los propietarios de los activos.

Tabla 18-4: Manipulación de media

8.3 Manipulación de media		
Prevenir la divulgación, modificación, eliminación o destrucción no autorizada de la información almacenada en los medios.		
Control	**LOT**	**ISO27001**
8.3.1	No obligatorio	No obligatorio
8.3.2	No obligatorio	No obligatorio
8.3.3	No obligatorio	No obligatorio

Realizado por: Merino. Katherine, 2022.

Análisis:

Este control no se considera necesario, pero sí recomendable. La organización debe establecer procedimientos para manipular los medios según la clasificación de los activos. De ser necesario

el traslado de medios físicos, se debe establecer una protección mediante servicios de mensajería confiables.

Recomendaciones:

- Los medios móviles deberían almacenarse de forma segura.
- Aplicar sistemas de encriptación para la transmisión de información a través de medios móviles y realizar copias de seguridad de la información.
- Crear registros de los medios que se han dejado de utilizar, identificando los datos sensibles que contenían.
- Para transferencia de medios físicos contratar servicios de mensajería confiables.

Tabla 19-4: Requisitos de negocio para el control de acceso

9.1 Requisitos de negocio para el control de acceso		
Limitar el acceso a la información y las instalaciones donde se procesan la información.		
Control	**LOT**	**ISO27001**
9.1.1	Obligatorio	Obligatorio
9.1.2	Obligatorio	Obligatorio

Realizado por: Merino. Katherine, 2022.

Análisis:

La organización debe establecer una política de control de acceso para usuarios autorizados. Los servicios de red deberán ser monitoreados y se deberá establecer procedimientos de conexión.

Recomendaciones:

- Tomar en cuenta los requisitos de seguridad definidos en la política de seguridad de la organización.
- Revisar periódicamente los derechos de acceso de los usuarios.
- Realizar seguimiento de los servicios de red de la organización.

Tabla 20-4: Gestión de acceso de usuarios

9.2 Gestión de acceso de usuarios		
Asegurar el acceso de personal autorizado y prevenir el acceso no autorizado a los sistemas y servicios.		
Control	**LOT**	**ISO27001**
9.2.1	No obligatorio	No obligatorio
9.2.2	No obligatorio	No obligatorio
9.2.3	No obligatorio	No obligatorio
9.2.4	No obligatorio	No obligatorio
9.2.5	No obligatorio	No obligatorio
9.2.6	No obligatorio	No obligatorio

Realizado por: Merino. Katherine, 2022.

Análisis:

Este control no se considera necesario para este estudio.

Tabla 21-4: Responsabilidades de los usuarios

9.3 Responsabilidades de los usuarios		
Asegurar la responsabilidad que tiene los usuarios para salvaguardas la información		
Control	**LOT**	**ISO27001**
9.3.1	No obligatorio	No obligatorio

Realizado por: Merino. Katherine, 2022.

Análisis:

Este control no se considera necesario para este caso de estudio.

Tabla 22-4: Control de acceso a sistemas y aplicaciones

9.4 Control de acceso a sistemas y aplicaciones		
Prevenir el acceso no autorizado.		
Control	**LOT**	**ISO27001**
9.4.1	Obligatorio	No obligatorio
9.4.2	No obligatorio	No obligatorio
9.4.3	No obligatorio	No obligatorio
9.4.4	No obligatorio	No obligatorio
9.4.5	No obligatorio	No obligatorio

Realizado por: Merino. Katherine, 2022.

Análisis:

El acceso a la información debe restringirse según la política de seguridad de la organización y evitar el acceso al código fuente de los programas informáticos para prevenir la introducción de código malintencionado.

Recomendaciones:

- Limitar cantidad de intentos de acceso a los sistemas.
- Ocultar los campos de contraseñas con símbolos.
- En caso de detectar un acceso no autorizado generar un evento de seguridad que informe al responsable de seguridad de la información.
- Cerrar la sesión de los sistemas luego de un período de inactividad.
- Obligar al usuario a cambiar su contraseña.

Tabla 23-4: Controles criptográficos

10.1 Controles criptográficos		
Asegurar el uso apropiado y efectivo de la criptografía para proteger la confidencialidad, autenticación y/o la integridad de la información.		
Control	**LOT**	**ISO27001**
10.1.1	No obligatorio	No obligatorio
10.1.2	No obligatorio	No obligatorio

Realizado por: Merino. Katherine, 2022.

Análisis: Este control no se considera necesario para este caso de estudio, pero si recomendable. La organización debe aplicar una política de encriptación que proteja la confidencialidad,

autenticación e integridad y deberá utilizar para la generación, almacenamiento y destrucción de claves.

Recomendaciones:

- La dirección debe utilizar comunicaciones encriptadas para evitar el acceso no deseado a información sensible.
- La encriptación debe ser acorde con la información sensible tratada.

Tabla 24-4: Áreas seguras

11.1 Áreas seguras		
Prevenir el acceso físico no autorizado, daños e interferencias a las instalaciones de procesamiento de información e información de la organización.		
Control	**LOT**	**ISO27001**
11.1.1	No obligatorio	No obligatorio
11.1.2	No obligatorio	No obligatorio
11.1.3	No obligatorio	No obligatorio
11.1.4	No obligatorio	No obligatorio
11.1.5	No obligatorio	No obligatorio
11.1.6	No obligatorio	No obligatorio

Realizado por: Merino. Katherine, 2022.

Análisis:

Este control no se considera necesario para este caso de estudio

Tabla 25-4: Equipos

11.2 Equipos		
Prevenir la pérdida, el daño, el robo de los activos y la interrupción de las operaciones corporativas		
Control	**LOT**	**ISO27001**
11.2.1	No obligatorio	No obligatorio
11.2.2	No obligatorio	No obligatorio
11.2.3	No obligatorio	No obligatorio
11.2.4	No obligatorio	No obligatorio
11.2.5	No obligatorio	No obligatorio
11.2.6	No obligatorio	No obligatorio
11.2.7	Obligatorio	No obligatorio
11.2.8	No obligatorio	No obligatorio
11.2.9	Obligatorio	No obligatorio

Realizado por: Merino. Katherine, 2022.

Análisis:

La organización debe proteger los equipos ante cualquier amenaza y tomar en cuenta las consecuencias ante fallos de las empresas de servicios públicos. Además, proteger el cableado de transmisión de datos, realizar mantenimiento de los equipos, gestionar los equipos que están fuera de las instalaciones.

Recomendaciones:

- Los servicios públicos contratados deben ser monitoreados para asegurar el buen funcionamiento.
- Realizar el mantenimiento de los equipos considerando los manuales de uso y las recomendaciones de los fabricantes.
- Identificar y registrar todos los activos.
- Utilizar salvapantallas automáticos cuando el equipo no sea utilizado en un período de tiempo determinado.

Tabla 26-4: Procedimientos operacionales y responsabilidades

12.1 Procedimientos operacionales y responsabilidades		
Asegurar que las operaciones sean correctas y seguras de las instalaciones de procesado de la información.		
Control	**LOT**	**ISO27001**
12.1.1	No obligatorio	Obligatorio
12.1.2	No obligatorio	No obligatorio
12.1.3	No obligatorio	No obligatorio
12.1.4	No obligatorio	No obligatorio

Realizado por: Merino. Katherine, 2022.

Análisis:

Este control no se considera necesario para este caso de estudio.

Tabla 27-4: Protección contra códigos maliciosos

12.2 Protección contra códigos maliciosos		
Asegurar que las instalaciones de aplicaciones estén protegidas contra los códigos maliciosos.		
Control	**LOT**	**ISO27001**
12.2.1	No obligatorio	No obligatorio

Realizado por: Merino. Katherine, 2022.

Análisis:

Este control no se considera necesario para este caso de estudio.

Tabla 28-4: Copias de respaldo

12.3 Copias de respaldo		
Protección contra la pérdida de datos.		
Control	**LOT**	**ISO27001**
12.3.1	Obligatorio	No obligatorio

Realizado por: Merino. Katherine, 2022.

Análisis:

Siempre se debe realizar copias de respaldo para evitar posible pérdida de información.

Recomendaciones:

- Crear un método de respaldo en el que se indique cuando realizar las copias de seguridad, la periodicidad y qué información almacenar.
- Verifica periódicamente los datos de respaldo.

Tabla 29-4: Registro y monitorización

12.4 Registro y monitorización		
Registrar eventos y generar evidencias.		
Control	**LOT**	**ISO27001**
12.4.1	No obligatorio	Obligatorio
12.4.2	No obligatorio	No obligatorio
12.4.3	No obligatorio	Obligatorio
12.4.4	No obligatorio	No obligatorio

Realizado por: Merino. Katherine, 2022.

Análisis:

Este control no se considera necesario para este caso de estudio, pero si recomendable. Se debe monitorear todos los eventos de la seguridad de la información, los datos recogidos deben estar protegidos para garantizar la integridad de información.

Recomendaciones:

- Recoger la identidad de los usuarios, actividades, privilegios utilizados, ficheros y acceso a bases de datos.
- Recoger las direcciones de red accedidas, los intentos y denegaciones de acceso a los sistemas.
- Recoger los cambios de configuración y evitar que los registros puedan ser alterados.

Tabla 30-4: Control de software operacional

12.5 Control de software operacional		
Asegurar la integridad de los sistemas operacionales.		
Control	**LOT**	**ISO27001**
12.5.1	No obligatorio	No obligatorio

Realizado por: Merino. Katherine, 2022.

Análisis:

Este control no se considera necesario para este caso de estudio, pero si recomendable. Se debe desarrollar un procedimiento para asegurar que el software que se va a instalar no tenga código malicioso o aplicaciones que puedan afectar al rendimiento de las aplicaciones.

Recomendaciones:

- La instalación del software la debería realizar solamente el administrador.
- Las aplicaciones deben ser aprobadas por la dirección.
- Debe existir un registro de todas las aplicaciones instaladas o eliminadas.

Tabla 31-4: Gestión de la vulnerabilidad técnica

12.6 Gestión de la vulnerabilidad técnica		
Prevenir las vulnerabilidades técnicas.		
Control	**LOT**	**ISO27001**
12.6.1	No obligatorio	No obligatorio
12.6.2	No obligatorio	No obligatorio

Realizado por: Merino. Katherine, 2022.

Análisis:

Este control no se considera necesario para este caso de estudio, pero si recomendable. En caso de identificarse una vulnerabilidad, la organización debe indicar el riesgo al que va a ser sometido para que las personas encargadas puedan tratarlas de acuerdo con sus roles y responsabilidades.

Recomendaciones:

- Definir roles y responsabilidades del personal encargado de la gestión de vulnerabilidades.
- Definir un tiempo de reacción ante una vulnerabilidad.
- Revisar de manera regular el proceso de la gestión de las vulnerabilidades.

Tabla 32-4: Consideraciones sobre auditorias de sistemas de información

12.7 Consideraciones sobre auditorias de sistemas de información		
Minimizar el impacto de las actividades de auditoría en los sistemas operacionales.		
Control	**LOT**	**ISO27001**
12.7.1	No obligatorio	Obligatorio

Realizado por: Merino. Katherine, 2022.

Análisis:

Este control no se considera necesario para este caso de estudio.

Tabla 33-4: Gestión de seguridad de las redes

13.1 Gestión de seguridad de las redes		
Asegurar la información que se transmite en las redes.		
Control	**LOT**	**ISO27001**
13.1.1	No obligatorio	No obligatorio
13.1.2	Obligatorio	No obligatorio
13.1.3	No obligatorio	No obligatorio

Realizado por: Merino. Katherine, 2022.

Análisis:

Se debe realizar un control de las redes para impedir el acceso no autorizado a los datos, además se debería establecer acuerdos de servicio con los proveedores (SLA).

Recomendaciones:

- Definir procedimientos de gestión de los equipos de red.

- En el caso que la organización disponga de varias áreas, es necesario dividir en distintos dominios de red.
- Monitorear el servicio ofrecido.

Tabla 34-4: Transferencia de información

13.2 Transferencia de información		
Mantener la seguridad de información transferida dentro de la organización y fuera de la organización		
Control	**LOT**	**ISO27001**
13.2.1	Obligatorio	No obligatorio
13.2.2	Obligatorio	No obligatorio
13.2.3	No obligatorio	No obligatorio
13.2.4	Obligatorio	Obligatorio

Realizado por: Katherine Merino. 2020

Análisis:

La transferencia de información debe estar sujeta a controles de seguridad para impedir que la información sea distribuida más allá del ámbito del acuerdo entre la organización y las entidades externas.

Recomendaciones:

- Definir procedimientos para proteger los datos y utilizar criptografía para proteger todo tipo de información.
- Concienciar la necesidad de no revelar datos confidenciales.

Tabla 35-4: Requisitos de seguridad de los sistemas de información

14.1 Requisitos de seguridad de los sistemas de información		
Asegurar los requisitos de los sistemas de información dentro de las redes públicas.		
Control	**LOT**	**ISO27001**
14.1.1	Obligatorio	Obligatorio
14.1.2	No obligatorio	No obligatorio
14.1.3	No obligatorio	No obligatorio

Realizado por: Merino. Katherine, 2022.

Análisis:

Los requisitos de la seguridad de la información se deben aplicar para todos los sistemas que se desarrollen sean nuevos o para mejorar los existentes.

Recomendaciones:

- Preservar la confidencialidad, integridad y disponibilidad de los servicios donde implique transferencias de información en redes públicas.
- Aplicar encriptación en la transmisión de la información.
- Almacenar la información en entornos de la organización de los datos de transacciones.

Tabla 36-4: Seguridad en los procesos de desarrollo y soporte

14.2 Seguridad en los procesos de desarrollo y soporte		
Asegurar que la seguridad de la información dentro del desarrollo de los sistemas de información		
Control	**LOT**	**ISO27001**
14.2.1	No obligatorio	No obligatorio
14.2.2	No obligatorio	No obligatorio
14.2.3	No obligatorio	No obligatorio
14.2.4	No obligatorio	No obligatorio
14.2.5	No obligatorio	Obligatorio
14.2.6	No obligatorio	No obligatorio
14.2.7	No obligatorio	No obligatorio
14.2.8	No obligatorio	No obligatorio
14.2.9	No obligatorio	No obligatorio

Realizado por: Merino. Katherine, 2022.

Análisis:

Este control no se considera necesario para este caso de estudio.

Tabla 37-4: Datos de prueba

14.3 Datos de prueba		
Asegurar la protección de datos en ambientes de pruebas.		
Control	**LOT**	**ISO27001**
14.3.1	Obligatorio	No obligatorio

Realizado por: Merino. Katherine, 2022.

Análisis:

Todos los datos de pruebas deben ser protegidos para evitar la divulgación de la información.

Recomendaciones:

- No utilizar datos que permitan identificar a la persona.
- Eliminar los datos de prueba una vez utilizados.
- Monitorear la información que se utiliza para las pruebas.

Tabla 38-4: Seguridad de la información en las relaciones con los proveedores

15.1 Seguridad de la información en las relaciones con los proveedores		
Asegurar la protección de los activos de la organización que son accesibles por los proveedores.		
Control	**LOT**	**ISO27001**
15.1.1	No obligatorio	Obligatorio
15.1.2	No obligatorio	No obligatorio
15.1.3	No obligatorio	No obligatorio

Realizado por: Merino. Katherine, 2022.

Análisis:

Este control no se considera necesario para este caso de estudio.

Tabla 39-4: Gestión de la prestación de servicios con los proveedores

15.2 Gestión de la prestación de servicios con los proveedores		
Mantener un nivel de seguridad de la información con los proveedores		
Control	**LOT**	**ISO27001**
15.2.1	No obligatorio	Obligatorio
15.2.2	No obligatorio	No obligatorio

Realizado por: Merino. Katherine, 2022.

Análisis:

Este control no se considera necesario para este caso de estudio.

Tabla 40-4: Gestión de incidentes y mejoras de seguridad de la información

16.1 Gestión de incidentes y mejoras de seguridad de la información		
Asegurar la gestión de los incidentes de seguridad de la información, incluyendo los eventos y debilidades de seguridad.		
Control	**LOT**	**ISO27001**
16.1.1	No obligatorio	No obligatorio
16.1.2	No obligatorio	Obligatorio
16.1.3	No obligatorio	Obligatorio
16.1.4	No obligatorio	Obligatorio
16.1.5	No obligatorio	Obligatorio
16.1.6	No obligatorio	No obligatorio
16.1.7	No obligatorio	No obligatorio

Realizado por: Merino. Katherine, 2022.

Análisis:

Este control no se considera necesario para este caso de estudio, pero si recomendable. Las responsabilidades y procedimientos deben generar una respuesta rápida a los incidentes de seguridad. Los eventos producidos deben ser clasificados y recogidos, se definirán como incidentes, en función de su consideración.

Recomendaciones:

- Segmentar las responsabilidades y procedimientos para la gestión de incidentes de seguridad.
- Los empleados deben notificar cualquier evento que sospechen que se trata de un incidente.
- Recoger la información y proceder a un análisis forense para determinar las causas y su tratamiento.

Tabla 41-4: Continuidad de seguridad de la información

17.1 Continuidad de seguridad de la información		
La continuidad de la seguridad de la información debe integrarse a la continuidad del negocio de la organización.		
Control	**LOT**	**ISO27001**
17.1.1	No obligatorio	No obligatorio
17.1.2	Obligatorio	Obligatorio
17.1.3	No obligatorio	No obligatorio

Realizado por: Merino. Katherine, 2022.

Análisis:

La continuidad de la seguridad de la información debe formar parte de la continuidad del negocio para asegurar que la organización está preparada para eventos adversos.

Recomendaciones:

- Cuando se planifique la continuidad del negocio también se debe considerar los requisitos de continuidad para la seguridad de la información.
- Planificar el procedimiento cuando se produzca un incidente.
- Realizar simulacros para verificar los procedimientos y controles en ambientes controlados.

Tabla 42-4: Redundancias

17.2 Redundancias		
Asegurar la disponibilidad de la información.		
Control	**LOT**	**ISO27001**
17.2.1	Obligatorio	No obligatorio

Realizado por: Merino. Katherine, 2022.

Análisis:

Se debe asegurar que exista disponibilidad de procesado de la información.

Recomendaciones:

- Aplicar sistemas redundantes para asegurar continuidad del servicio.
- Realizar respaldos de seguridad de la información.
- Realizar simulaciones controladas para verificar la disponibilidad de los sistemas y corregir errores.

Tabla 43-4: Cumplimiento con los requisitos legales y contractuales

18.1 Cumplimiento con los requisitos legales y contractuales		
Asegurar el cumplimiento de obligaciones legales relacionadas con la seguridad de la información y con cualquier requisito de seguridad.		
Control	**LOT**	**ISO27001**
18.1.1	Obligatorio	Obligatorio
18.1.2	No obligatorio	No obligatorio
18.1.3	No obligatorio	No obligatorio
18.1.4	Obligatorio	No obligatorio
18.1.5	No obligatorio	No obligatorio

Realizado por: Merino. Katherine, 2022.

Análisis:

La organización debe cumplir con los requisitos de la seguridad de la información, debe identificarlos y documentarlos.

Recomendaciones:

- Identificar y aplicar las normativas vigentes a las que está sujeta la organización.

Tabla 44-4: Revisiones de seguridad de la información

18.2 Revisiones de seguridad de la información		
Asegurar que los procedimientos de seguridad de la información operan de acuerdo con las políticas y procedimientos de la organización.		
Control	**LOT**	**ISO27001**
18.2.1	Obligatorio	Obligatorio
18.2.2	Obligatorio	Obligatorio
18.2.3	Obligatorio	Obligatorio

Realizado por: Merino. Katherine, 2022.

Análisis:

La organización debe cumplir con las políticas y estándares de seguridad, el cumplimiento técnico debe revisarse en función de la política de seguridad de la organización.

Recomendaciones:

- Revisar la política de seguridad por personas no involucradas en su desarrollo.
- La información obtenida debe ser documentada.
- Las revisiones deberán ser planificadas de forma periódica.

Del análisis anterior se obtiene la siguiente tabla con el resumen de los controles necesarios para ser aplicados.

Tabla 45-4:: Controles ISO 27001

NOMBRE DOMINIOS DE CONTROL	APLICA / NO APLICA	CONTROLES PARA APLICAR
DOMINIO 5 - POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Aplica	5.1.1 5.1.2
DOMINIO 6 - ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	Aplica	6.1.1 6.2.1 (No obligatorio)
DOMINIO 7 - SEGURIDAD DE LOS RECURSOS HUMANOS	No Aplica	No Aplica
DOMINIO 8 - GESTIÓN DE ACTIVOS	No Aplica	8.1.1 (No obligatorio) 8.1.2 (No obligatorio) 8.1.4 (No obligatorio) 8.8.2 (No obligatorio) 8.3.1 (No obligatorio)
DOMINIO 9 - CONTROL DE ACCESO	Aplica	9.1.1 9.1.2 9.2.4 9.4.1
DOMINIO 10 - CRIPTOGRAFÍA	No Aplica	10.1.1 (No obligatorio)
DOMINIO 11 - SEGURIDAD FÍSICA Y DEL ENTORNO	Aplica	11.2.7 11.2.9
DOMINIO 12 - SEGURIDAD DE LAS OPERACIONES	Aplica	12.3.1 12.4.1 (No obligatorio)

		12.5.1 (No obligatorio) 12.6.1 (No obligatorio)
DOMINIO 13 - SEGURIDAD DE LAS COMUNICACIONES	Aplica	13.1.2 13.2.1 13.2.2
DOMINIO 14 - ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	Aplica	14.1.2 14.3.1
DOMINIO 15 - RELACIÓN CON LOS PROVEEDORES	No Aplica	No Aplica
DOMINIO 16 - GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	No Aplica	16.1.3 (No obligatorio)
DOMINIO 17 - ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO	Aplica	17.1.2 17.2.1
DOMINIO 18 - CUMPLIMIENTO	Aplica	18.1.1 18.1.4 18.2

Realizado por: Merino. Katherine, 2022.

CAPÍTULO V

5. PROPUESTA

5.1. Marco Referencial de Seguridad basado en la Norma ISO 27001

El marco referencial de seguridad está basado en la norma ISO 27001 y en el ciclo continuo PDCA que se encuentra implícito dentro de la norma que permite su periódica actualización y mejora, con el fin de incrementar la seguridad y mejorar los procesos y procedimientos para que las organizaciones lleguen a un estado de madurez con respecto a la implementación de procesos seguros, tal como se muestra a continuación:

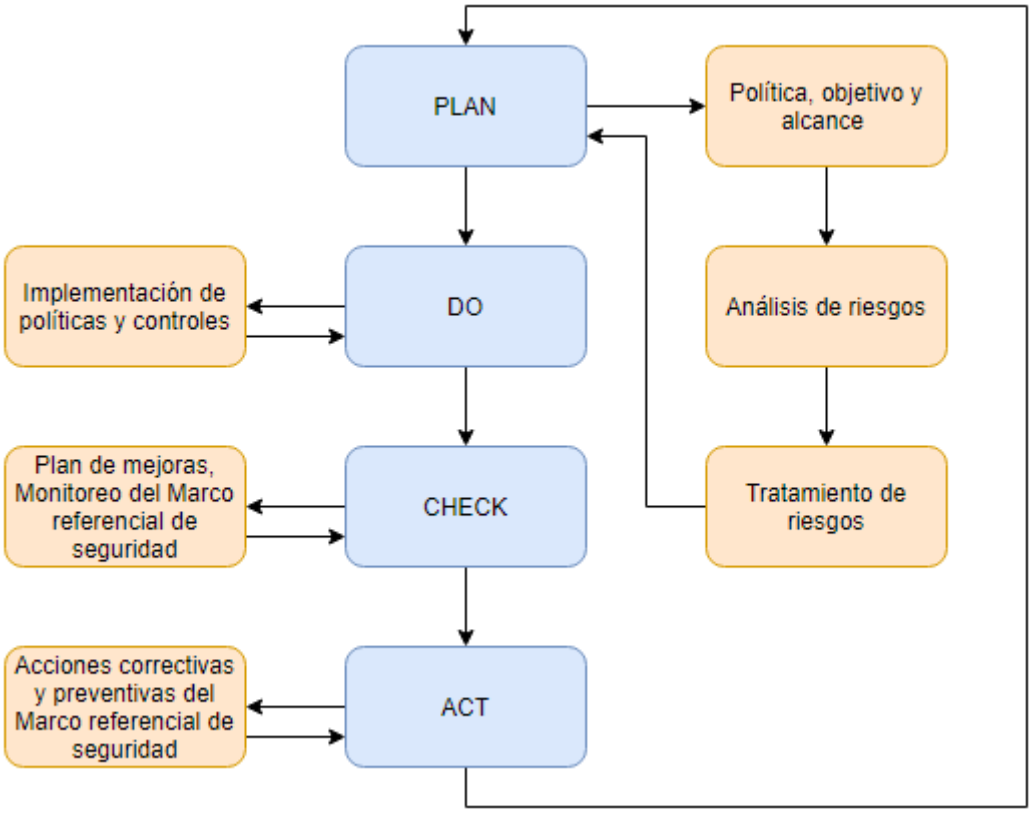


Gráfico 1-5: Ciclo PDCA del Marco Referencial de Seguridad propuesto.

Realizado por: Merino. Katherine, 2022.

Para el desarrollo de este Marco Referencial de Seguridad se aplicaron diversas metodologías y normas ISO debido a que no existe una metodología explicita para tratar los datos personales con lo solicitado en la Ley Orgánica de Telecomunicaciones, por lo que se procedió con las siguientes acciones.

- Se identificó los requerimientos de la Ley Orgánica de Telecomunicaciones para garantizar la protección de los datos personales y posteriormente se comparó con la norma ISO 27001:2013 para identificar los dominios y controles necesario que cumplan con lo solicitado en la LOT, obteniendo que el Marco Referencial de Seguridad debe abarcar 13 dominios y 31 controles establecidos en la Norma ISO 27001:2013.

- Para identificar y categorizar los tipos de datos personales que se están tratando dentro de estas organizaciones que consideró la clasificación establecida por la Agencia Española de Protección de Datos, ya que ISO 27001:2013 no establece ninguna clasificación con respecto a los datos personales.
- Para categorizar los activos y determinar el impacto de la amenaza se tomó como referencia a la metodología MAGERIT Versión 3, ya que esta metodología fue creada en base a la norma ISO 27001 y permite calcular en impacto en función de la confidencialidad, integridad y disponibilidad de los datos.
- La determinación de amenazas se realizó en base a lo estipulado en la Ley Orgánica de Telecomunicaciones y adicional de un análisis FODA de la organización y se procedió a relacionarlas con el listado de amenazas de ISO27001 que es similar al catálogo de amenazas que presenta MAGERIT Versión 3.
- Para determinar la probabilidad del Riesgo se realizó una encuesta en función a las amenazas tomando como referencias preguntas del listado de cumplimiento normativo del Reglamento General de protección de datos que estén vinculadas a las amenazas identificadas.
- Para la valoración del riesgo se consideraron recomendaciones de IS0 31000:2018 e ISO 31010:2019, estableciendo como criterio el impacto del riesgo sobre el negocio. No se consideró MAGERIT Versión 3 para esta actividad debido a que las ponderaciones calculadas no coincidían con las recomendaciones de la metodología MAGERIT.

Por lo que el presente marco referencial de seguridad es un hibrido de varias metodologías y normas que mejor se adaptan a la protección de los datos personales que son tratados por los prestadores de servicios de acceso a internet y que son compatibles con la norma ISO 27001:2013, las cuales permiten dar cumplimiento con lo solicitado en la Ley Orgánica de Telecomunicaciones.

Adicional a este marco referencial de seguridad se creó una guía de Implementación de la Información Documentada, ya que es de suma importancia para la Norma ISO 27001:2013 la información documenta de todas las acciones que se creen dentro de las organizaciones, además que sirven de respaldo para una auditoría. Cabe mencionar que la Ley Orgánica de Telecomunicaciones estipula que los prestadores de servicios de Telecomunicaciones deben someterse a una auditoría.

5.1.1. Alcance del Marco Referencial de Seguridad

El Marco de seguridad está diseñado para los proveedores de servicios de internet quienes están sujetos al cumplimiento de la Ley Orgánica de Telecomunicaciones y tratan datos personales de sus abonados, clientes o usuarios.

El presente marco de seguridad contiene acciones a seguir para dar cumplimiento con lo estipulado en la Ley Orgánica de Telecomunicaciones considerando las recomendaciones y controles de la Norma ISO 27001 para salvaguardar los datos personales en las acciones de que involucran el tratamiento de datos, tomando como caso de análisis el proveedor de servicios de internet MUNDOTRONIC.

5.1.2. Objetivos del Marco Referencial de Seguridad

- Establecer procedimientos para asegurar los datos personales de abonados, clientes o usuarios de los proveedores de internet.
- Documentar las acciones empleadas para asegurar los datos personales de abonados, clientes o usuarios de los proveedores de internet.
- Prevenir amenazas potenciales que pongan en riesgo los datos personales de abonados, clientes o usuarios de los proveedores de internet.

5.1.3. Documentos de referencia empleados en el Marco Referencial de Seguridad

- Norma ISO/IEC 27001:2013
- Ley Orgánica de Telecomunicaciones
- Recomendaciones de la Agencia Española de Protección de datos.
- Documentación interna
- Regulaciones, normas y leyes aplicables a la organización

5.1.4. Partes Interesadas

Para determinar las partes interesadas se considera a todos los involucrados con los tratamientos de los datos personales considerando los siguientes aspectos:

- Dueños de los datos personales: Abonados, clientes o usuarios.
- Procesadores de datos: Personal que forman parte de la organización.
- Creadores de procesos de gestión de los datos personales: Alta dirección.
- Controladores del correcto tratamiento de los datos personales: Entes reguladores.

Luego de identificar a las partes interesadas relevantes que están involucrados con los datos personales se procede a identificar las necesidad y expectativas de cada uno de ellos:

Tabla 1-5: Partes Interesadas

Partes interesadas	Necesidades y expectativas
Abonados, clientes o usuarios.	Los datos personales deben ser confidenciales, estar disponibles y mantenerse íntegros
Personal	Deben conocer sus responsabilidades con especto al tratamiento de los datos personales para mantener su integridad, confidencialidad y disponibilidad de estos.
Alta dirección	Mantener la gestión, confidencialidad disponibilidad e integridad de los datos personales
Entes reguladores	Garantizar el cumplimiento de las leyes y normativas referentes a protección de datos personales.

Realizado por: Merino. Katherine, 2022.

5.1.5. Resolución de contenidos del Marco referencial de Seguridad

- Considerando que en Ecuador la protección de datos se garantiza mediante El Art. 66 de la Constitución de la República, donde "…Se reconoce y garantizará a las personas: 19. "El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos de información requerirán la autorización del titular y el mandato de la ley" (Const., 2008, art. 66)
- Dada a que la Ley Orgánica de Telecomunicaciones estipula en sus artículos: Art. 22, Art. 23, Art. 24, Art. 76, Art. 77, Art. 78 y Art. 81 la necesidad y obligación de los presentadores de servicios de telecomunicaciones a implementar medidas para salvaguardar los datos de carácter personal.
- Dado al análisis entre la Ley Orgánica de Telecomunicaciones y Norma ISO/IEC 27001:2013 como herramienta de cumplimiento de esta.

Se concluye que los prestadores de servicios de telecomunicaciones deben implementar 13 aspectos recomendados por la norma ISO 27001 para dar cumplimiento a lo estipulado en la Ley Orgánica de Telecomunicaciones.

A continuación, se presentan los (13) ítems por los que está compuesto el Marco Referencial de Seguridad, cabe indicar que sigue el mismo orden de análisis de la Norma ISO/IEC 27001:2013, por lo que se recomienda que para su ejecución se siga el orden presentado, además que se debe considerar que el primer punto a tratar evalúa la situación inicial que servirá como punto de partida y de comparación con la Port-Implementación.

Determinada la situación inicial se procederá a identificar políticas y procesos necesarios para salvaguardar o mejorar la seguridad de la protección de los datos personales con el fin de reducir la probabilidad de la materialización de la amenaza.

Figura 1-5: Contenido del Marco referencial de Seguridad.

Realizado por: Merino. Katherine, 2022.

1. Análisis de Riesgos

Figura 2-5: Análisis de Riesgos

Realizado por: Merino. Katherine, 2022.

El análisis de riesgos presenta la situación de la empresa e identifica los activos que se requiere proteger en base a los siguientes aspectos:

Disponibilidad: Es cuando los recursos, sistemas e información deben estar disponibles cuando el usuario lo requiera.

Integridad: Es cuando la información no cambia.

Confidencialidad: Esta información debe ser accesible solo por personal autorizado.

Para realizar el análisis de riesgo es necesario considerar lo que se desea proteger, contra quien se va a proteger y como se lo va a proteger. Para lo cual es necesario estas tres actividades:

1) **Identificación de amenazas. -**Para realizar la identificación de amenazas se deben realizar las siguientes acciones:

- Realizar un inventario de activos
- Catalogar los activos según los siguientes tipos de activos.

Tabla 2-5: Tipos de Activos del Marco Referencial de Seguridad.

IDENTIFICADOR	TIPO DE ACTIVO
[D]	DATOS/INFORMACIÓN
[HW]	HARDWARE
[MEDIA]	SOPORTES
[SW]	SOFTWARE
[COM]	REDES Y COMUNICACIONES
[L]	INSTALACIONES
[P]	PERSONAL

Realizado por: Merino. Katherine, 2022.

- Identificar y categorizar los tipos de datos almacenados. - Para esta actividad catalogar los datos en función del siguiente listado:
  - Aspectos personales. - Nombres, apellidos, nacionalidad, actividades económicas

- Identificadores únicos. - Números de teléfonos, número de cédula, IP, dirección MAC.
- Datos de localización. - Direcciones domiciliaria, Coordenadas
- Preferencias de consumo. - Servicios de consumo
- Metadatos. - Tráfico de red
- Estado financiero. - Estados financieros
- Datos de medios de pago. - Método de pago del cliente
- Documentos personales. - Documentos que servicios básicos, copias de documentos personales.

- Identificar para cada activo las amenazas y vulnerabilidades a los que se encuentran expuestos, considerar el siguiente listado de amenazas y su impacto

Tabla 3-5: Amenazas e Impacto para el Marco Referencial de Seguridad.

ID	AMENAZA	DESCRIPCIÓN	IMPACTO	
[A1]	Error de usuarios	Equivocaciones de las personas cuando utilizan los datos o servicios	9	Moderado
[A2]	Error del Administrador	Fallas por parte del personal responsable en la realización de los procesos.	15	Alto
[A3]	Error de configuración	Fallas en la realización de las configuraciones.	1	Muy Bajo
[A4]	Deficiencia en la organización	Fallas en la segregación de funciones.	1	Muy Bajo
[A5]	Difusión de software malicioso	Propagación de software que altere el correcto funcionamiento de los sistemas (virus, troyano, gusano, etc.)	3	Muy Bajo
[A6]	Fuga de información	Revelación de datos personales de la organización.	6	Bajo
[A7]	Vulnerabilidades en software	Fallas en código fuente de los programas, aplicaciones, sistemas operativos	3	Muy Bajo
[A8]	Error de mantenimiento	Fallas de personas en la realización de los procedimientos de control y monitoreo de los sistemas	8	Bajo
[A9]	Suplantación de identidad	Fallas del personal al momento de utilizar los activos	9	Moderado

[A10]	Interceptación de información	Acceso a la información (se mantiene en escucha)	1	Muy Bajo
[A11]	Revelación de la información	Revelación de la información de los clientes, usuario o abonados	5	Bajo

Realizado por: Merino. Katherine, 2022.

- Para obtener la medida cualitativa del impacto se puede usar también la siguiente tabla:

Tabla 4-5: Impacto de Riesgo del Marco Referencial de Seguridad.

NIVEL	CONCEPTO	DESCRIPCIÓN (En caso de presentarse el hecho)	SEGURIDAD DE LA INFORMACIÓN
1-3	**Muy Bajo**	No afecta el funcionamiento de la empresa	Afecta a una actividad del proceso.
4-8	**Bajo**	Afecta a ciertos departamentos de la empresa	Afecta a una persona, grupo de personas
9-13	**Moderado**	Puede afectar parcialmente el funcionamiento a de la empresa	Afecta a un conjunto de datos personales o en la realización de proceso.
14-18	**Alto**	Pone en riesgo el funcionamiento a la empresa	Afecta a varios de datos personales o a uno o varios procesos de la organización.
19-21	**Muy Alto**	Cese de funciones de la empresa	Afecta toda la organización. Sanciones legales.

Realizado por: Merino. Katherine, 2022.

- Para calcular la probabilidad aplicar el siguiente cuestionario a todo el personal de la organización.

Tabla 5-5: Encuesta para la probabilidad para el Marco Referencial de Seguridad.

ID	AMENAZAS	N°	PREGUNTAS
[A1]	Error de usuarios	1	¿Existen procedimientos de seguridad para evitar la pérdida, destrucción o daño accidental?
		2	¿Existen procedimientos que restringa el acceso a los diferentes tipos de datos?
[A2]	Error del Administrador	3	¿Para determinar las medidas a aplicar se tiene en cuenta el alcance, contexto y fines del tratamiento, así como riesgos de probabilidad y los derechos de las personas físicas?
		4	¿Existe un proceso de verificación, evaluación y valoración regular de la eficacia de las medidas técnicas y organizativas implementadas para garantizar la seguridad del tratamiento?
[A3]	Error de configuración	5	¿Existen procedimientos que indiquen la forma de uso de los sistemas y equipos?
		6	¿Existe medidas para asegurar la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico?

[A4]	Deficiencia en la organización	7	¿Existen procesos que permitan la continuidad del funcionamiento correcto de la organización?
		8	¿Existen medidas técnicas y organizativas apropiadas que garanticen un nivel de seguridad adecuado de protección contra el riesgo?
[A5]	Difusión de software malicioso	9	¿Se ha establecido un procedimiento para identificar y gestionar las brechas de seguridad?
		10	¿Existe procesos de verificación, evaluación y valoración de la eficacia de las medidas técnicas y organizativas aplicadas para garantizar la seguridad del tratamiento de datos personales?
[A6]	Fuga de información	11	¿Se ha establecido procedimientos de eliminación segura de información de dispositivos que haya cumplido con su vida útil?
		12	¿Se ha establecido procedimientos de protección de datos en ambientes de prueba?
		13	¿Se ha establecido procesos que restrinjan el acceso a los datos?
[A7]	Vulnerabilidades en software	14	¿Se ha implementado procedimientos para identificar y gestionar las brechas de seguridad?
		15	¿Existe procedimientos que se identifiquen procedimientos para salvaguardar los aplicativos?
[A8]	Error de mantenimiento	16	¿Existe documentación que registre las medidas técnicas y organizativas apropiadas al riesgo de los tratamientos?
		17	¿Se han establecido medidas para asegurar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento?
[A9]	Suplantación de identidad	18	¿Existen procedimientos de accesos a los sistemas solo por personal autorizado?
		19	¿Existen procedimientos de restricción de acceso a la información?
[A10]	Interceptación de información	20	¿Existen procesos de seguridad en las redes de datos de la organización?
		21	¿Existe procesos de documentación de brechas de seguridad que afecten a la información?
[A11]	Revelación de la información	22	¿Existe procedimientos que las personas autorizadas para tratar datos personales se comprometen a respetar la confidencialidad o están sujetas a una obligación de confidencialidad de naturaleza legal?
		23	¿Existen procedimientos para la transferencia de información?
		24	¿Existe cláusulas que indique que se requiere autorización del propietario de los datos personales para realizar un tratamiento?

Realizado por: Merino. Katherine, 2022.

Posteriormente se debe identificar la cantidad de encuestados, sacar el promedio de respuestas negativas por cada amenaza y por cada amenaza aplicar la siguiente fórmula:

$$Probabilidad = \frac{Promedio\ de\ respuestas\ negativas}{Total\ de\ la\ Población\ encuestada}$$

Al aplicar la fórmula anterior se obtiene la probabilidad de cada amenaza, para obtener su medida cualitativa deben aplicar la siguiente tabla:

Tabla 6-5: Probabilidad del riesgo

NIVELES DE PROBABILIDAD DE OCURRENCIA		DESCRIPCIÓN
0,9-1	**Muy alta**	Riesgo de materialización es recurrente (Más de tres veces por semana) (Casi seguro).
0,7-0,8	**Alta**	Riesgo que puede materializarse de manera habitual (Más de ocho veces al mes) (Probable).
0,5-0,6	**Moderada**	Riesgo que se presenta de forma casual o accidental (Menos de cuatro veces al mes) (Posible).
0,3-0,4	**Baja**	Riesgo que puede presentarse de manera eventual (Menos de doce veces al año) (Raro).
<0,2	**Muy baja**	Riesgo cuya probabilidad de materializarse es mínima (Menos de seis veces al año) (Improbable).

Realizado por: Merino. Katherine, 2022.

- Calcular el riesgo

Para calcular el riesgo de cada amenaza se de aplicar la siguiente fórmula:

$$Riesgo = Impacto\ x\ Probabilidad$$

Para esta actividad se debe listar las amenazas, colocar su impacto y su probabilidad para luego aplicar la fórmula anterior y encontrar el nivel de riesgo por cada amenaza. Para dimensionar el riesgo se debe aplicar la siguiente tabla considerando el valor obtenido de la multiplicación.

Tabla 7-5: Valoración del Riesgo para el Marco Referencial de Seguridad.

DIMENSIÓN DEL RIESGO	RANGO ASIGNADO	ACCIÓN REQUERIDA
Riesgo Extremo	12,01-21	Evitar el riesgo aplicando controles que reduzcan el nivel de probabilidad, reducir el riesgo empleando controles orientados a minimizar el impacto.
Riesgo Alto	6,1-12	Evitar o mitigar el riesgo aplicando medidas adecuadas y aprobadas, para trasladarlo a la zona de riesgo moderado o a su vez compartir y/o transferir el riesgo.
Riesgo Moderado	3,1-6	Evitar o mitigar el riesgo aplicando prontamente medidas que permitan reducir o compartir el riesgo.
Riesgo Bajo	1,1-3	Asumir el riesgo. Mitigar el riesgo con acciones detectivas y preventivas.
Riesgo Muy Bajo	0,1-1	Asumir el riesgo. Mitigar el riesgo con acciones administrativas.

Realizado por: Merino. Katherine, 2022.

- Decidir las acciones para mitigar el riesgo

Para identificar qué es lo que se va a realizar con los riesgos, se debe considerar las zonas de riesgos, tal como se presenta en la siguiente tabla.

Tabla 8-5: Acciones según la zona de riesgo para el Marco Referencial de Seguridad.

ZONA	ACCIÓN REQUERIDA
Zona de Riesgo Mínimo	**Asumir el Riesgo:** Cuando el nivel de exposición del riesgo es adecuado y por lo tanto se acepta.
Zona de Riesgo Aceptable	**Asumir el Riesgo:** Cuando el nivel de exposición del riesgo es adecuado y por lo tanto se acepta.
Zona de Riesgo Moderado	**Mitigar o Evitar el Riesgo:** Cuando se requiere fortalecer los controles existentes y/o agregar nuevos controles.
Zona de Riesgo Importante	**Mitigar o Evitar el Riesgo: Se debe** Implementar controles adicionales fortaleciendo los actuales.
Zona de Riesgo Inaceptable	**Evitar el Riesgo:** Implementar acciones inmediatas que para reducir la probabilidad y el impacto de materialización.

Realizado por: Merino. Katherine, 2022.

2) **Medidas de Protección. -** Por cada amenaza detectada identificar las acciones de mitigación. Realizar las siguientes acciones:

- Identificar los riesgos con más alto nivel ya que estos deben ser priorizados para implementar las acciones de mitigación.
- Analizar las acciones de mitigación en función al costo beneficio que tendrá sobre la organización.

3) **Estrategias de respuestas. -** Para establecer las estrategias de respuesta se debe considerar los siguiente:

Proteger y procesar: Estas acciones se aplican cuando la organización es demasiado vulnerable y se la debe proteger inmediatamente.

Perseguir y procesar: Se aplica estas acciones cuando el riesgo es controlable.

Una vez identificado las estrategias de respuestas se debe realizar un presupuesto y cronograma de implementación de las acciones de mitigación.

2. Políticas de Seguridad

Los proveedores de servicios de acceso a internet deben crear una política de seguridad de los datos personales y ser documentada, socializada y actualizada periódicamente. Esta debería ser creada y aprobada por la alta dirección con la asesoría de las áreas técnicas de la organización.

En el caso existir cambios significativos será responsabilidad de la alta dirección la aprobación de ajustes, cambios y actualizaciones.

Para crear la política de seguridad se debe considerar los siguientes aspectos:

- **Organización de la seguridad:** Donde se indica como se va a administrar la seguridad dentro de la organización.
- **Clasificación y control de activos:** Permite gestionar los activos.

- **Cumplimiento:** La alta dirección deberá establecer los métodos para garantizar el cumplimiento.

3. Organización de la Seguridad

Los proveedores de servicios de acceso a internet deben formar un comité de seguridad de los datos personales y deberán convocarse a reuniones ordinarias y extraordinarias documentando las siguientes acciones:

1) **Compromiso de la alta gerencia con la seguridad de los datos personales:** Las acciones a implementar son:

- Establecer los roles y responsabilidades del personal relativas a la seguridad de la información.
- Establecer metodologías y procesos para implementar la seguridad de la información.

Estas acciones se deben realizar con la finalidad de establecer correctamente los roles y responsabilidades de las áreas funcionales existentes en las empresas prestadoras de servicios de acceso a internet.

2) **Nombrar un responsable del tratamiento de los datos personales:** La persona responsable del tratamiento de datos personales debe ser una persona con conocimiento sobre seguridad de la información
3) **Asignar las responsabilidades del responsable del tratamiento de los datos personales:** Sus responsabilidades mínimas deben ser:

- Velar por los procesos de seguridad
- Planificar, evaluar y coordinar la implementación y mejora de los procesos y políticas de seguridad
- Promover la difusión de las políticas

4) **Identificar las partes interesadas:** Se debe identificar:

- Actores internos de la empresa
- Actores externos a la empresa
- Identificar las expectativas de las partes interesadas con respecto a la organización.

5) **Identificación de los riesgos que corren los datos de las partes interesadas:** Identificar activos y sus riesgos.
6) **Establecer políticas de dispositivos móviles:** Se aplica cuando se empleen dispositivos móviles como herramientas de trabajo.

4. Gestión de Activos

Los proveedores de servicios de acceso a internet deben considerar como activo principal los datos y documentos personales de los abonados, clientes o usuarios y los activos que los contienen. Por lo que deben realizar las siguientes actividades.

1) **Inventario de activos:** Se debe inventariar todos los activos existentes en la organización. El inventario debe contener.

- Identificador
- Tipo de activo
- Modelo o categorización

2) Establecer los propietarios de los activos: En base al cargo dentro de la empresa, el personal debe ser propietario de los activos que utilizará para desempeñar su trabajo.

3) **Política de devolución de los activos:** Se debe identificar los motivos de devolución de los activos, que acciones se van a realizar con estos y establecer las responsabilidades del responsable de las devoluciones de los activos.

4) **Clasificar la información**: Se debe considerar los siguientes criterios:

7) Política de uso de medios removibles: Se debe realizar las siguientes acciones:

- Identificar los medios removibles permitidos dentro de la organización.
- La seguridad a implementarse para salvaguardar la información contenida en estos medios removibles.
- Formas de uso permitido por terceros
- Procesos de almacenamiento y de desecho.

5. Control de Acceso a la Red

Los proveedores de servicios de acceso a internet deben establecer los procesos de control de acceso a los datos personales de los abonados, clientes o usuarios que involucren los siguientes aspectos:

1) Uso de los servicios de red. - Se debe identificar las redes que forman parte de la red corporativa para lo cual se debe realizar las siguientes acciones:

- Identificar los servicios que están presentes en la red corporativa
- Identificar los tipos de privilegios
- Establecer acciones para determinar las personas a las cuales se les va a otorgar los accesos.
- Otorgar privilegios a los diferentes tipos de usuarios.

2) Gestión de información de autenticación secreta. -Se deben realizar las siguientes acciones:

- Identificar la herramienta de autenticación
- Realizar un registro de los usuarios que accederán por autenticación.
- Establecer procedimientos de revocación de accesos por desvinculación de personal o cambio de puesto de trabajo.

3) Restricción de acceso a la información. - Se debe aplicar las siguientes acciones:

- Establecer reglas de acceso a los usuarios.
- Implementar medios dedicados para establecer las comunicaciones, como por ejemplo VPN.

4) **Procedimiento de ingreso seguro. -**Aplicarlas siguientes acciones:

- Establecer las responsabilidades que tiene el personal con respecto al cuidado de los usuarios y contraseñas que se les asignó.
- Limitar el número de intentos de accesos.
- Limitar el tiempo de accesos de acuerdo con el tipo de usuario.

6. Criptografía

Los proveedores de servicios de acceso a internet deben establecer una política de uso de controles criptográficos, los cuales pueden emplearse en:

- Protección de claves de accesos
- Transmisión de información confidencial

7. Seguridad Física y del Entorno

Los proveedores de servicios de acceso a internet deben establecer:

1) **Política de eliminación segura o reutilización de equipos que identifique los procedimientos y métodos de destrucción de la información. –** Los elementos a ser almacenados o eliminados son:

- Documentos físicos
- Grabaciones
- Discos duros externo e internos
- Softwares
- Documentos del sistema.

Las acciones para implementarse son:

- Generar un registro por cada equipo a ser eliminado o reutilizado el cual debe contener:
  - Id del equipo
  - Propietario
  - Nuevo propietario (De ser el caso)
  - Motivos de por los cuales va a ser eliminado o reutilizado
  - Fecha en la que el equipo que va a ser eliminado o reutilizado
  - Información contenida dentro equipo que a ser eliminado o reutilizado
- Sacar respaldos de la información contenida en los dispositivos a ser eliminados o reutilizados.
- Llevar un registro de la información respaldada
- Establecer temporalidad que se almacenará la información respaldada.
- Establecer métodos de eliminación.
- Mantener un registro de los dispositivos y documentos eliminados.

2) **Política de escritorio y pantalla limpios por ausencia del personal de su sitio de trabajo. -** Las acciones recomendadas son:

- Identificar lugares lógicos y físicos seguros de almacenamiento dentro de las estaciones de trabajo.
- Almacenar en sitios seguros los documentos y medios de almacenamiento en gabinetes u otros lugares con protección física.
- Desconectar los equipos que no se estén usando de la red de datos.
- Crear procedimiento para que el personal no mantenga documentos sensibles de la organización en sus estaciones de trabajo.
- Crear procedimientos para que el personal realice un correcto uso de sus pausas activas y no abandonen sus estaciones de trabajo por largos periodos de tiempo.
- Establecer como procedimiento de estricto cumplimiento que al alejarse de sus estaciones de trabajo los equipos deben ser bloqueados.
- Establecer procedimiento de bloqueos automáticos dentro de los equipos y sistemas.

8. Seguridad de las Operaciones

Los proveedores de servicios de acceso a internet deben establecer las siguientes políticas y procedimientos:

1) **Política para respaldos de la información. -** Se debe detallar las acciones a implementarse para respaldar la información contenida dentro de las organizaciones. Ya sea de sistemas, softwares o unidades extraíbles, para lo cual es necesario identificar:

- Lugares lógicos y físicos seguros de almacenamiento.
- Aplicativo gestor de respaldos de información
- De acuerdo con el tipo de información la periodicidad en la que necesita ser respaldada la información.
- Las horas del día en la que se va a respaldar la información para que no interfiriera con la jornada laboral del personal de la organización
- La periodicidad del almacenamiento de la información

Además, se debe llevar un registro de la información respaldada y establecer las funciones del responsable de generar los respaldos de la información.

2) **Política de registro de eventos. -** Debe contener:

- Identificación de usuario
- Fecha y hora de inicio y finalización del incidente
- Ubicación del incidente
- Registro de incidentes solucionados exitosamente y los más impactantes.

3) **Políticas de instalación de software en sistemas operativos. -** Se debe considerar

- Identificar personal autorizado de ejecutar software.
- Llevar un registro de aplicaciones utilizadas dentro de la organización.
- Utilizar software libre o software con licencia.

4) **Procesos de gestión de las vulnerabilidades. -** Se debe aplicar técnicas con procedimientos a seguir para identificar activos, amenazas y establecer acciones de mitigación. Se recomienda realizar:

- Testing de software para identificar defectos en los softwares utilizados en la organización.
- Realizar auditorías en el software utilizando herramientas como: OWASP.
- Aplicar supervisores de red como: PRTG

Como acciones a mitigar se recomienda en uso de:

- Utilizar software de gestión de riesgos y compliance.

9. Seguridad de las comunicaciones

Los proveedores de servicios de acceso a internet deben establecer:

1) **Procesos de seguridad de los servicios de red. -** Las acciones a implementarse es.

- Identificar las redes y servicios de la organización.
- Identificar la ubicación de cada elemento de res y los riesgos a los que está expuesto.
- Establecer procedimientos de acceso a las conexiones de red.
- Establecer procedimientos de vinculación de nuevos equipos.
- Crear procedimiento de pruebas de conectividad.
- Segmentar la red de acuerdo con el tipo de usuario que va a acceder.
- Establecer medios de comunicación dedicados para transportar información confidencial.

2) **Política de seguridad de red. -**Para establecer la política de seguridad de red se debe identificar:

- Sistemas y equipos de información
- Proveedores de servicios
- Propietarios de activos e información
- Usuario de la información.
- Herramientas de seguridad.
- Procedimientos hardening
- Herramientas de monitoreo
- Personal capacitado en seguridad.

3) **Trasferencia de información. -** Los proveedores de servicios de acceso a internet deben establecer:

- Procedimientos de transferencia de los datos personales dentro y fuera de la organización. Por ejemplo, cláusulas de confidencialidad en la cual el proveedor se obliga a que tanto este como sus empleados guardarán y protegerán como confidencial en los términos de las leyes aplicables en la materia, la información conferida a ellos por parte de los abonados, clientes o usuario y comprometerse que ni este ni sus empleados o subcontratistas divulgarán a tercero alguno la información confidencial recibida.

- Establecer política de la transferencia de los datos personales dentro y fuera de la organización.
- Establecer acuerdos de confidencialidad o de no divulgación entre las personas que contienen los datos personales y los receptores de los datos.

10. Adquisición, desarrollo y mantenimiento de sistemas

Los proveedores de servicios de acceso a internet deben establecer los procedimientos de seguridad que serán implementados en la red de datos y procedimientos de protección de datos para cuando sea necesario realizar pruebas con los equipos de la red de datos, tomando las siguientes consideraciones:

- Definir procedimientos en las etapas de análisis y diseño en los procedimientos de procesamiento de aplicaciones
- Evaluar requerimientos de seguridad los controles a aplicar para mitigar para salvaguardar la red.
- Establecer procedimiento de creación de ambientes de prueba seguros.
- Procedimientos de respaldos de la información de los equipos que se utilizaran en los ambientes de prueba.
- Procedimientos para regresar a su función normal a los equipos utilizados en los ambientes de prueba.

11. Gestión de incidentes de seguridad de la información

Los proveedores de servicios de acceso a internet deben establecer procedimientos de elaboración de reportes de eventos e incidentes de seguridad sobre:

- Debilidades detectadas de seguridad
- Procedimiento de seguridad implementados
- Recolección de evidencias.

Además, se debe llevar un registro de incidentes y los procedimientos que se llevaron a cabo para solventarlos.

12. Aspectos de seguridad de la información de la gestión de continuidad de negocio

Los proveedores de servicios de acceso a internet deben asegurar la disponibilidad de los sistemas que contienen datos personales de los abonados, clientes o usuarios, previamente de deberá contar con una evaluación de riesgos para implementar planes de continuidad de los servicios o planes de contingencia. Además, se debe establecer las acciones de redundancia para garantizar la disponibilidad de los datos personales, para lo cual es necesario implementar:

- Cronograma de pruebas periódicas de las acciones implementadas
- Coordinar mejoras de las acciones implementadas.
- Proponer mejoras de las acciones implementadas.
- Probar y actualizar acciones implementadas.

13. Cumplimiento

Es de cumplimiento obligatorio que todos los proveedores de servicios de acceso a internet cumplan con lo estipulado en la Ley Orgánica de Telecomunicaciones que asegura la protección de datos personales de los abonados, clientes o usuarios que garantizan la integridad, confidencialidad y disponibilidad de estos. Los artículos por cumplir son: Art. 22, Art. 23, Art. 24, Art. 76, Art. 77, Art. 78 y Art. 81. Para esto es necesario cumplir con políticas y normas de seguridad de datos personales y verificar su cumplimiento.

14. Esquema aplicativo del Marco Referencial de Seguridad

Como resultado del trabajo realizado, en el cual, previamente se analizó los requerimientos establecidos por la Ley Orgánica de Telecomunicaciones sobre el tratamiento de los datos personales e identificados los controles de la Norma ISO 27001 que solventan dichos requerimientos y del análisis de riesgos sobre los activos utilizando la metodología Magerit V3, se presenta un esquema resumen y el orden de las actividades que debe realizar el prestador de servicios de acceso a internet para cumplir con lo solicitado en la Ley Orgánica de Telecomunicaciones y proteger la información.

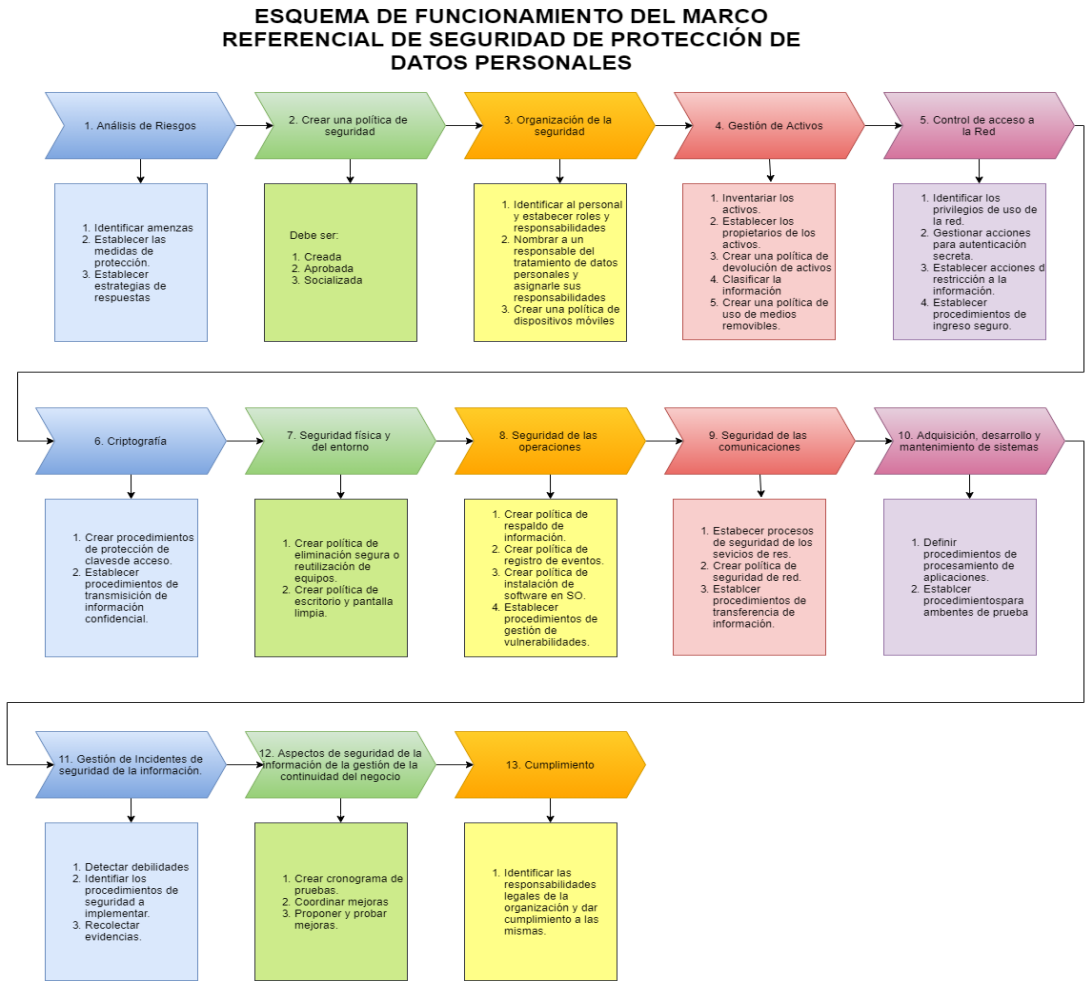


Figura 3-5: Esquema aplicativo del Marco Referencial de Seguridad.

Realizado por: Merino. Katherine, 2022.

5.2. Marco Referencial de Seguridad de MUNDOTRONIC.

A continuación, se presenta un esquema de funcionamiento de la prestadora de Servicio de Acceso a Internet Mundotronic y demás datos generales:

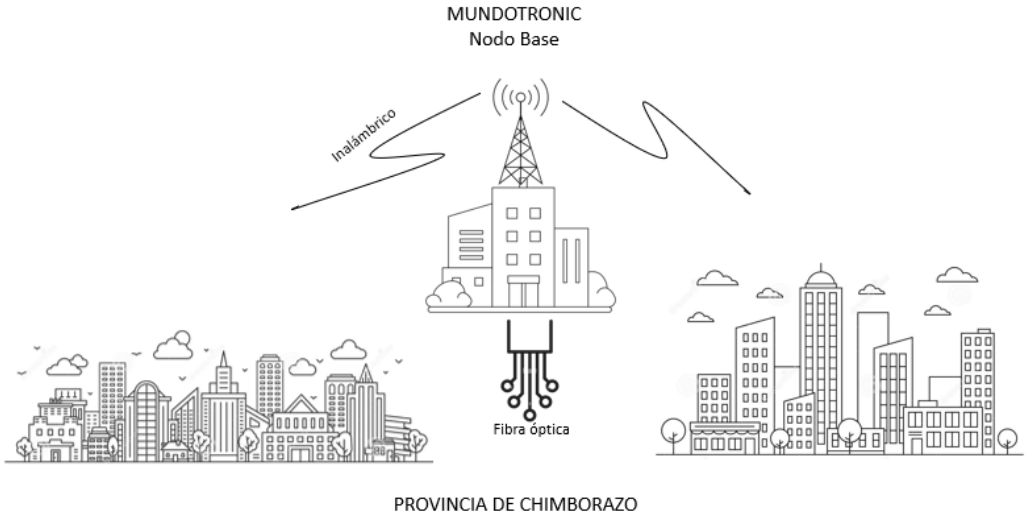


Figura 4-5: Diagrama operacional de Red de Mundotronic

Realizado por: Merino. Katherine, 2022.

La cobertura operacional de Red Mundotronic presenta la siguiente información:

Servicio: Prestadora de Servicios de Acceso a Internet

Nombre comercial: MUNDOTRONIC

Medio de provisión de servicio: Por antena y fibra óptica

Área de cobertura: Chimborazo

Nodo Base: Riobamba

Mundotronic al poseer un título habilitante de registro de servicio de acceso a internet y concesión de uso y explotación de frecuencia de espectro radioeléctrico otorgado por la Agencia de Regulación y Control de las Telecomunicaciones debe prestar el servicio en conformidad de la Ley organiza de Telecomunicaciones y cumplir con las obligaciones generales suscritos en dicho título siendo uno de estos la protección de los datos personales de sus abonados, clientes o usuarios.

Para dar cumplimiento a dicha obligación implementa el marco de Seguridad el cual consta de una Guía de Implementación. **Ver Anexo A.** Y en su puesta en marcha se identifican las siguientes

amenazas a los que están expuestos los datos personales que son tratadas dentro de MUNDOTRONIC.

Tabla 9-5: Amenazas y vulnerabilidades detectadas en MUNDOTRONIC

ID	AMENAZA	DESCRIPCIÓN	VULNERABILIDADES
[A1]	Error de usuarios	Equivocaciones de las personas cuando utilizan los datos o servicios	Equivocaciones de las personas cuando utilizan los datos o servicios
[A2]	Error del Administrador	Fallas por parte del personal responsable en la realización de los procesos.	Falta de capacitación
[A3]	Error de configuración	Fallas en la realización de las configuraciones.	El usuario no registrado en el sistema. Direcciones IP duplicadas. Diseño de red erróneo.
[A4]	Deficiencia en la organización	Fallas en la segregación de funciones.	Tardanza en realizar las actividades. No cumplimiento con las actividades que establece el contrato.
[A5]	Difusión de software malicioso	Propagación de software que altere el correcto funcionamiento de los sistemas (virus, troyano, gusano, etc.)	Falta de políticas de uso de software
[A6]	Fuga de información	Revelación de datos personales de la organización.	Divulgación de información sensible de clientes, usuario o abonados
[A7]	Vulnerabilidades en software	Fallas en código fuente de los programas, aplicaciones, sistemas operativos	Mal funcionamiento de los sistemas
[A8]	Error de mantenimiento	Fallas de personas en la realización de los procedimientos de control y monitoreo de los sistemas	Desactualización de los sistemas Mal funcionamiento de los sistemas.
[A9]	Suplantación de identidad	Fallas del personal al momento de utilizar los activos	Suplantación de identidad del personal de la empresa.
[A10]	Interceptación de información	Acceso a la información (se mantiene en escucha)	Falta de procedimientos de seguridad en canales de comunicación
[A11]	Revelación de la información	Revelación de la información de los clientes, usuario o abonados	Mala aplicación o redacción de procedimiento o accesos

Realizado por: Merino. Katherine, 2022.

Luego de los análisis realizados se procede a crear el Marco de Seguridad adaptado a las necesidades de MUNDOTRONIC y los requisitos para dar cumplimiento con lo estipulado en la Ley Orgánica de Telecomunicaciones. **Ver Anexo B.** Además, se utilizan las plantillas de registro de información requeridas por MUNDOTRONIC que se encuentran el **Anexo C.**

A continuación, se presenta una tabla con los controles, los documentos de políticas y procedimientos implementados necesarios para dar cumplimientos a los controles. De la misma tabla se puede concluir que para salvaguardar correctamente los datos personales se han implementado (31) controles.

Tabla 10-5: Controles aplicados en MUNDOTRONIC

NOMBRE DOMINIOS DE CONTROL	APLICA / NO APLICA	CONTROLES PARA APLICAR	ID DOCUMENTO	DOCUMENTOS	CONTROLES QUE APLICAN
DOMINIO 5 - POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Aplica	5.1.1 5.1.2	DP_001	Política de seguridad de la información	2
DOMINIO 6 - ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	Aplica	6.1.1 6.2.1 (No obligatorio)	MSPD_001 DP_002	Marco de Seguridad de protección de Datos de MUNDOTRONIC (sección Roles y responsabilidades) Política para dispositivos móviles	2
DOMINIO 7 - SEGURIDAD DE LOS RECURSOS HUMANOS	No Aplica	No Aplica	No Aplica	No Aplica	0
DOMINIO 8 - GESTIÓN DE ACTIVOS	No Aplica	8.1.1 (No obligatorio) 8.1.2 (No obligatorio) 8.1.4 (No obligatorio) 8.8.2 (No obligatorio) 8.3.1 (No obligatorio)	MSPD_001 DP_003 DP_004	Marco de Seguridad de protección de Datos de MUNDOTRONIC (Secciones: Gestión de activos) Política de devolución de activos Política de uso de medios removibles.	5
DOMINIO 9 - CONTROL DE ACCESO	Aplica	9.1.1 9.1.2 9.2.4 9.4.1	DP_005 DP_006 MS_001 MS_002	Política de control de acceso Política sobre el uso de los servicios de red Procesos de Acceso a la red Procesos de Restricción de acceso a la información	4
DOMINIO 10 - CRIPTOGRAFÍA	No Aplica	10.1.1 (No obligatorio)	DP_007	Política sobre el uso de controles criptográficos	1
DOMINIO 11 - SEGURIDAD FÍSICA Y DEL ENTORNO	Aplica	11.2.7 11.2.9	DP_008 DP_009	Política de eliminación segura o reutilización de equipos Política de escritorio y pantalla limpia	2
DOMINIO 12 - SEGURIDAD DE LAS OPERACIONES	Aplica	12.3.1 12.4.1 (No obligatorio) 12.5.1 (No obligatorio) 12.6.1 (No obligatorio)	DP_0010 DP_011 DP_012 MS_003	Política para respaldos de la información Política de registros de eventos Política de instalación de software Procesos de gestión de las vulnerabilidades técnicas	4

DOMINIO 13 - SEGURIDAD DE LAS COMUNICACIONES	Aplica	13.1.2 13.2.1 13.2.2	MS_004 MS_005 DP_013 DP_014	Procesos de seguridad de las comunicaciones Cláusulas de transferencias de información Política de procedimientos de seguridad de las redes Política de transferencia de información	3
DOMINIO 14 - ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	Aplica	14.1.2 14.3.1	MS_006 DP_015	Procedimientos de especificación de requisitos de seguridad de la información Política de procedimientos de protección de datos en ambientes de prueba.	2
DOMINIO 15 - RELACIÓN CON LOS PROVEEDORES	No Aplica	No Aplica	No Aplica	No Aplica	0
DOMINIO 16 - GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	No Aplica	16.1.3 (No obligatorio)	MS_007	Proceso de gestión de Incidentes	1
DOMINIO 17 - ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO	Aplica	17.1.2 17.2.1	MS_008 MS_009	Proceso de continuidad de negocio Proceso para disponibilidad de instalaciones de procesamiento de información	2
DOMINIO 18 - CUMPLIMIENTO	Aplica	18.1.1 18.1.4 18.2	MS_010 DP_016 MS_011	Procedimiento de cumplimiento legales Política de privacidad y protección de datos personales Procedimiento de revisiones de seguridad de la información	3
TOTAL DE CONTROLES APLICADOS					**31**

Realizado por: Katherine Merino. 2020

5.3. Guía de Implementación de la Información Documentada

5.3.1 Objetivos de la guía de implementación

Describir las acciones a realizarse con los requisitos mínimos que debería contener la información documentada solicitada en el marco referencial de seguridad.

5.3.2 Alcance de la guía de implementación

La presente guía de implementación contiene los requisitos mínimos que debería contener la información documentada solicitadas en el marco referencia de seguridad los cuales brindaran un adecuado nivel de protección en el tratamiento de los datos personales de los abonados, clientes o usuarios.

5.3.3 Contenido de la guía de implementación

1. **El marco de seguridad deberá contener:**

- El número de revisión
- Apellidos y nombres de quienes lo realizaron, lo aprobaron y revisaron, cargo, fecha y firma
- Número de páginas contenidas en el plan.

2. **Políticas de Seguridad**

Debe ser:

- Creada
- Documentada
- Identificada
- Definir su estado
- Comunicada a todo el personal
- Revisada y actualizada periódicamente
- Aprobada

3. **Organización de la Seguridad**

Debe contener:

- Organigrama de la empresa.
- Establecer un comité directivo, comité de riesgos y el responsable del tratamiento de los datos personales.
- Establecer los objetivos y funciones del comité directivo y del comité de riesgos
- Establecer las funciones del responsable del tratamiento de los datos personales.

- Crear política de uso de dispositivos móviles la cual debe tener el alcance y los objetivos de esta, y debe ser:
  - Creada
  - Documentada
  - Identificada
  - Definir su estado
  - Comunicada a todo el personal
  - Revisada y actualizada periódicamente
  - Aprobada

4. Gestión de Activos

- Realizar un inventario de activos que estén relacionados con el tratamiento de datos personales e identificar a su propietario en función al organigrama
- Identificar y clasificar los datos personales en función a los siguientes aspectos:
  - **Aspectos personales**. - Nombres, apellidos, nacionalidad, actividades económicas
  - **Identificadores únicos.** - Números de teléfonos, número de cédula, IP, dirección MAC.
  - **Datos de localización. -** Direcciones domiciliaria, Coordenadas
  - **Preferencias de consumo.** - Servicios de consumo
  - **Metadatos. -** Tráfico de red
  - **Estado financiero.** - Estados financieros
  - **Datos de medios de pago.** - Método de pago del cliente
  - **Documentos personales. -** Documentos que servicios básicos, copias de documentos personales.
- Crear políticas de devolución de los activos y de uso de medios removibles las cuales deben tener el alcance y los objetivos de esta, y debe ser:
  - Creada
  - Documentada
  - Identificada
  - Definir su estado
  - Comunicada a todo el personal
  - Revisada y actualizada periódicamente
  - Aprobada

5. Control de Acceso a la red

- Identificar y establecer los procesos de control de acceso, y debe ser:
  - Creado
  - Documentado
  - Identificado
  - Definir su estado

- Comunicada a todo el personal
- Revisada y actualizada periódicamente
- Aprobado

6. Criptografía

Crear políticas de sobre el uso de controles criptográficos la cual debe tener el alcance y los objetivos de esta, y debe ser:

- Creada
- Documentada
- Identificada
- Definir su estado
- Comunicada a todo el personal
- Revisada y actualizada periódicamente
- Aprobada

7. Seguridad física y del entorno

Crear políticas de eliminación segura o reutilización de equipos y de escritorio y pantalla limpios, estas deben contener el alcance y los objetivos, y deben ser:

- Creadas
- Documentadas
- Identificadas
- Definir su estado
- Comunicadas a todo el personal
- Revisadas y actualizadas periódicamente
- Aprobadas

8. Seguridad de las operaciones

Crear políticas de respaldos de la información, registro de eventos e instalación de software en sistemas operativos, estas deben contener el alcance y los objetivos, y deben ser:

- Creadas
- Documentadas
- Identificadas
- Definir su estado
- Comunicadas a todo el personal
- Revisadas y actualizadas periódicamente
- Aprobadas

En el proceso de gestión de las vulnerabilidades técnicas se debe identificar el responsable y detallar las actividades, este debe ser:

- Creado
- Documentado

- Identificado
- Definir su estado

9. Seguridad de las comunicaciones

Crear proceso de Seguridad de las comunicaciones, se debe identificar el responsable y detallar las actividades, este debe ser:

- Creado
- Documentado
- Identificado
- Definir su estado

Crear cláusulas de transferencias de información, se debe identificar el responsable y detallar las actividades, este debe ser:

- Creado
- Documentado
- Identificado
- Definir su estado

10. Adquisición, desarrolla y mantenimiento de sistemas

Crear procedimientos de especificación de requisitos de seguridad de la información, se debe identificar el responsable y detallar las actividades, este debe ser:

- Creado
- Documentado
- Identificado
- Definir su estado
- Definir actividades y acciones

11. Gestión de incidentes de seguridad de la información

Crear proceso de gestión de incidentes se debe identificar el responsable, detallar las actividades y acciones, este debe ser:

- Creado
- Documentado
- Identificado
- Definir su estado
- Aprobado
- Revisado

12. Gestión de continuidad de negocio

Crear un proceso de gestión para disponibilidad de instalaciones de procesamiento de información, se debe identificar el responsable y detallar las actividades, este debe ser:

- Creado
- Documentado

- Identificado
- Definir su estado

13. Cumplimiento

Crear un procedimiento de cumplimiento legales, se debe identificar el responsable y detallar las actividades, este debe ser:

- Creado
- Documentado
- Identificado
- Definir su estado

Crear un procedimiento de revisiones de seguridad de la información, se debe identificar el responsable y detallar las actividades, este debe ser:

- Creado
- Documentado
- Identificado
- Definir su estado

CONCLUSIONES

- En base al estudio se elaboró e implementó la propuesta del Marco Referencial de Seguridad en la prestadora de servicio de acceso a internet MUNDOTRONIC con sede en Riobamba, con: 16 políticas y 11 procesos para cubrir con los 13 dominios y 31 controles de la Norma ISO 27001:2013, convirtiéndose en una herramienta dinámica ya que cumple con el ciclo PDCA de mejora continua, es decir, que cada vez que se la gestione va a ir mejorando sus procesos y políticas permitiendo que las organizaciones vayan madurando en temas de seguridad de protección de datos personales.
- Debido a que la Ley Orgánica de Telecomunicaciones es quien directamente solicita a los prestadores de servicios de acceso a internet establecer procedimientos que garanticen la seguridad de los datos se procedió a identificar los requerimientos de esta ley y se realizó una comparativa con la Norma internacional ISO 27001, determinando que el Marco Referencial de Seguridad debe abarcar 13 dominios y 31 controles establecidos en la Norma ISO 27001:2013. Además, en la Constitución del Ecuador se estipula como un derecho de los ecuatorianos la protección de datos personales, también en el Código Orgánico Integral se establece ciertas sanciones por tratamientos no autorizados de este tipo de datos, pero es la Ley Orgánica de Telecomunicaciones quién regula a los prestadores de servicios de acceso a internet y establece pautas que se deben implementar para proteger los datos personales de los clientes, abonados y usuarios de este piso de servicios, en base a la revisión realizada se determina que esta ley no establece metodologías o normas específicas de como garantizar la protección.
- De la investigación realizada se identificó que la Norma internacional ISO 27001 mediante la aplicación de Sistemas de Gestión de Seguridad de la Información gestiona todo tipo de información que pueda existir en las organizaciones y se centra en la protección de los activos. Mientras que el Reglamento General de Protección de Datos que rige a toda la Unión Europea ya categoriza a los tipos de datos personales y establece procedimientos no profundos para proteger estos datos, al no ser tan específicos dichos procedimientos la Norma internacional ISO 27001 se convierte en herramienta para dar cumplimiento a dicho Reglamento.
- La evaluación de la implementación del Marco Referencial de seguridad propuesto se realizó en base a la encuesta fundamentada en el listado de cumplimiento normativo del RGPD en función de las amenazas detectadas, ejecutándola antes y después de la aplicación para identificar la reducción del nivel de riesgo. Se aplicó el método estadístico T- Student con el 5% de tolerancia, comprobándose la hipótesis. Siendo necesario para el desarrollo del Marco Referencial de Seguridad la complementación de métodos, metodologías y normas internacionales compatibles con la Norma ISO 27001:2013 que evalúen en función de la

confidencialidad, integridad y disponibilidad de los datos, debido a que no existe procedimientos específicos para tratar adecuadamente los datos personales, generando un Marco Referencial de Seguridad híbrido adaptado a las necesidades de la Ley Orgánica de Telecomunicaciones.

- Producto de la investigación del Marco Referencial de Seguridad se generó una Guía de Implementación de la Información Documentada, ya que representa un capital intelectual de la empresa y además permite llevar un control documental identificable, estándar, revisado y aprobado que debe ser almacenado y preservado para futuros controles de cambios, sirviendo también como evidencia del cumplimiento de la guía cuando se presente una auditoría y de lo establecido en la Norma ISO 27001:2013.

RECOMENDACIONES

- Se debe aplicar la totalidad del Marco Referencial de Seguridad propuesto, pues los procesos y procedimientos mitigan y controlan los riesgos en el tratamiento de datos personales a los que están expuestos los activos de las organizaciones y garantizan un adecuado nivel de confidencialidad, disponibilidad e integridad de los datos.
- Se debe identificar los activos de las organizaciones y definir el propietario de cada uno, además de segregar responsabilidades dentro de la organización, ya que el Marco Referencial de Seguridad no solo depende de la alta dirección sino de toda la empresa, por lo que se recomienda al encargado de la implementación, que todo el personal de la empresa sea partícipe de la creación e implementación y se pueda crear una cultura de seguridad.
- Se recomienda aprovechar el diseño PDCA del Marco Referencial de Seguridad para reducir riesgos en el tratamiento de datos personales y evaluarlo periódicamente para determinar si los procedimientos y políticas están dando los resultados esperados y de ser el caso mejorarlos, eliminarlos o crear otros procedimientos o políticas con el fin de robustecer al Marco Referencial de Seguridad y aumentar el control sobre las amenazas.
- Es importante la correcta gestión de la información documentada ya que la Norma ISO 27001 establece ciertos aspectos necesarios que deben contener y realizarse con los documentos y aunque la Ley Orgánica de Telecomunicaciones no establece la periodicidad de dichas auditorías si la menciona, por lo que es responsabilidad de los prestadores de servicios a internet cumplir con lo que solicita le ley, estar preparados cuando llegue el momento de la auditoría y utilizar como instrumentos y evidencias la información documentada.
- Se recomienda que los prestadores de servicios de acceso a internet implementen el Marco Referencial de Seguridad para reducir riesgos en el tratamiento de datos personales propuesto, ya que presenta las acciones a realizarse de una forma ordenada y acorde con lo solicitado por la Ley Orgánica de Telecomunicaciones planteando solo los dominios y controles de la Norma ISO 27001 necesarios para garantizar un adecuado nivel de disponibilidad, confidencialidad e integridad de este tipo de datos. Además, tomando en consideración la demostración de la hipótesis planteada, la presente propuesta permite mitigar vulnerabilidades y amenazas a los que están expuestos los activos de las empresas prestadoras de servicios de acceso a internet.

GLOSARIO

ARCOTEL	Agencia de Regulación y Control de Telecomunicaciones
DINARDAP	Dirección Nacional de Registro de Datos Públicos
FODA	Fortalezas, Oportunidades, Debilidades y Amenazas
GPS	Global Positioning System - Sistema de Posicionamiento Global
IDS	Intrusion Detection System- Sistema de Detección de Intrusiones
IP	Protocolo de Internet
ISO	Internacional Organization for Standardization- Organización Internacional de Normalización
ISP	Proveedor de Servicios de Internet
LOT	Ley Orgánica de Telecomunicaciones.
MAC	Media Access Control - Control de Acceso a Medios
MINTEL	Ministerio de Telecomunicaciones
PDCA	Planear, hacer, revisar y actuar
RGPD	Reglamento General de Protección de Datos
RUC	Registro Único de Contribuyentes
SAI	Servicio de acceso a internet
TIC	Tecnologías de Información y Comunicación

BIBLIOGRAFÍA

Agencia de Regulación y Control de las Telecomunicaciones. (2016). *Reglamento para la prestación de servicios de Teleomunicaciones y Servicios de Radiodifusión por suscripción.* Quito: Resolución 05-03-ARCOTEL-2016 .

Agencia Española de Protección de Datos. (Mayo de 2018). Listado de cumplimiento normativo. España.

Agencia Española de Protección de Datos. (s.f.). *Guia Práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD.*

Agencybcn. (2018). *Una guía rápida y concisa para saber cómo afecta a empresas y autónomos el nuevo Reglamento General de Protección de Datos (RGPD)*. Obtenido de https://www.agencybcn.com/guia-rapida-del-rgpd-para-empresas-y-autonomos-2018/#Que_se_entiende_como_un_dato_de_caracter_personal

ARCOTEL. (2016). *REGLAMENTO PARA LA PRESTACIÓN DE SERVICIOS DE TELECOMUNICACIONES Y SERVICIOS DE RADIODIFUSIÓN POR SUSCRIPCIÓN*. RESOLUCIÓN 05-03.

ARCOTEL. (2019). Servivio de acceso a internet. *Boletín estadístico mayo 20019*, 12.

Barragán, C. (Octubre de 2017). ADAPTACIÓN DE LAS NORMAS ISO 27001 E HIPPA PARA LA REDUCCIÓN DE RIESGOS EN LA SEGURIDAD EN HOSPITALES NIVEL I DEL IESS. Riobamba, Chimborazo, Ecuador.

Benavides, D. (2014). *Informe de la MIPYMES en la Contratación Pública 2013-2014*. Ecuador: DNEI-INI-0107.

Brian, A. (2018). La protección de datos personales en América Latina: entre la Unión Europea y los Estados Unidos de Norteamérica. *Seminario Internacional de Protección de Datos Personales 2018 en conmemoración del Día Internacional de Protección de Datos Personales del INFODF*. México: Recuperado de http://www.infodf.org.mx/seminariodatos2018/presentaciones/Ana_Brian.pdf.

Bustamante, G., & Osorio, J. (4 de Agosto de 2014). Metodología de la seguridad de la información como medida de protección en pequeñas empresas. Medellin, Colombia.

Código Orgánico Integral Penal [COIP]. (2016). *Artículo 229 [Título VII]*. Registro Oficial No. 899.

Código Orgánico Integral Penal [COIP]. (2016). Registro Oficial No. 899.

Comisión Europea. (2018). *Reforma de 2018 de las normas de protección de datos de la UE*. Recuperado de https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_es.

Comisión Europea. (2018). *RGPD: nuevas oportunidades, nuevas obligaciones.* Luxemburgo: Bietlot in Belgium. Recuperado de https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-sme-obligations_es.pdf.

Consejo Europeo, & Consejo de la Unión Europea. (25 de 10 de 2018). *Consilium*. Obtenido de https://www.consilium.europa.eu/es/policies/data-protection-reform/data-protection-regulation/

Constitución de la Republica del Ecuador [Const]. (2008). *Artículo 66 [Título II]*. Decreto Legislativo 0.

Cordero, G. (2015). Estudio comparativo entre metodologías MAGERIT y CRAMM, utilizadas para Análisis y Gestión de Riesgos de Seguridad de la Información. Cuenca, Azuay, Ecuador.

Dirección Nacional de Registro de Datos Públicos. (24 de julio de 2018). Lorena Naranjo: "Ecuador necesita una Ley de Protección de Datos que favorezca el flujo de datos en beneficio económico y social". Recuperado de http://www.datospublicos.gob.ec/lorena-naranjo-ecuador-necesita-una-ley-de-proteccion-de-datos-que-favorezca-el-flujo-de-datos-en-beneficio-economico-y-social/.

Dirección Nacional de Registro de Datos Públicos. (15 de marzo de 2018). Mintel y la Dinardap trabajan en una estrategia para la protección de los datos personales. Recuperado de http://www.datospublicos.gob.ec/mintel-y-la-dinardap-trabajan-en-una-estrategia-para-la-proteccion-de-los-datos-personales/.

Escuela Europea de Excelencia. (s.f.). Cómo realizar la evaluación de riesgos según ISO 31000:2018. Córdoba, España.

Escuela Europea de Excelencia. (s.f.). Listado de amenazas y vulnerabilidades en ISO 27001. Córdoba, España.

Garrigues. (2014). Mario Costeja vs. Google ¿Cómo pueden coexistir libertad de expresión, protección de datos y gestión de la reputación? . *d+i LLORENTE & CUENCA*, 1-3.

ISO 27001. (s.f.). FASE 9 REVISIÓN POR LA DIRECCIÓN SEGÚN ISO 27001. España.

legaltech. (28 de junio de 2018). Hacia una adecuada protección de los datos personales en Ecuador. Recuperado de https://legaltech.com.ec/hacia-una-adecuada-proteccion-de-los-datos-personales-en-ecuador/.

Ley Orgánica. (2015). *De Telecomuniaciones.* Quito: Registro Oficial Nº 439.

Manuel, D. (29 de Octubre de 2009). Análisis de Riesgos: ISO 27005 vs MAGERIT y otras metodologías. Madrid, España: Audea.

Martínez, D. (2018). Unificación de la protección de datos personales en la Unión Europea: Desafíos e implicaciones. *El Profesional de la Información*, Volumen 27, 198.

MINTEL. (2018). Seguridad de la Información y Protección de Datos Personales. En *Libro Blanco de la Sociedad de la Información y del Conocimiento* (pág. 45). Quito.

Ortiz, F., Candelas, F., Pomares, J., Gil, P., & Crespo, L. (2002). Prácticas de Redes. En F. Ortiz, F. Candelas, J. Pomares, P. Gil, & L. Crespo, *Prácticas de Redes* (págs. 28-32). Cottolengo: Club Universitario.

Reglamento General. (2016). *De Protección de Datos.* Directiva 95/46/CE.

Ron, M. (2018). Protección de Datos Personales. Recuperado de https://www.derechoecuador.com/proteccion-de-datos-personales.

Sánchez, G., & Rojas, I. (2012). Leyes de Protección de Datos Personales en el mundo y la Protección de Datos Biométricos – Parte I. *Revista Seguridad*. Recuperado de https://revista.seguridad.unam.mx/numero-13/leyes-de-protecci%C3%B3n-de-datos-personales-en-el-mundo-y-la-protecci%C3%B3n-de-datos-biom%C3%A9tricos-%E2%80%93.

UNAM. (s.f.). Metodología para realizar la gestión de riesgos. México.

ANEXOS

ANEXO A: CERTIFICADO DE MUNDOTRONIC

mundo Tronic
SOLUCIONES TECNOLÓGICAS

Riobamba, 28 de noviembre de 2019

Ingeniero

Oswaldo Martínez MSc.

COORDINADOR DE LA MAESTRIA DE SEGURIDAD TELEMÁTICA DE LA ESCUELA SUPERIOR POLITÉCNIA DE CHIMBORAZO

Presente

Tengo el agrado de dirigirme a Usted, con la finalidad de hacer de su conocimiento quela Srta. Katherine Adriana Merino Villa, con Cédula de Identidad N° 0605764109, maestrante de la Maestría de Seguridad Telemática desarrolló he implementó un Marco Referencial de Seguridad para Reducir Riesgos en el Tratamiento de Datos Personales para la empresa MUNDOTRONIC.

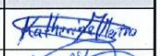
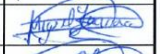
Atentamente,

Ing. Miguel Huaraca
Gerente General
MUNDOTRONIC

Mundo TRONIC ESPECIALISTAS EN SEGURIDAD
RUC.: 0603579897001
TELF.: 032608247 CEL.: 0995638678 - 0979219445

ANEXO B: MARCO REFERENCIAL DE SEGURIDAD DE MUNDOTRONIC

MARCO DE SEGURIDAD DE PROTECCIÓN DE DATOS DE MUNDOTRONIC

REV. 1	Nombre y Apellidos	Cargo	Fecha	Firma
Confeccionado	Katherine Merino	Maestrante	2019-11-25	
Aprobado	Miguel Huaraca	Gerente	2019-11-25	
Revisado	Miguel Huaraca	Gerente	2019-11-25	
Código: MSPD_001				

Contenido

Introducción

El prestador de servicio de acceso a internet MUNDOTRONIC que tiene como sede la ciudad de Riobamba y brinda sus servicios por medios inalámbricos a la población de la provincia de Chimborazo y su afán por dar cumplimiento a lo estipulado en la Ley Orgánica de Telecomunicaciones y con el afán de dar seguridad a sus clientes, usuarios y abonados pone a disposición su Marco de Seguridad de Protección de Datos Personales.

Objetivo del Marco de Seguridad de Protección de Datos Personales de MUNDOTRONIC

Brindar protección en el tratamiento de datos personales de los clientes, usuarios y abonados que consumen el servicio ofertado por MUNDOTRONIC.

Alcance del Marco de Seguridad de Protección de Datos Personales de MUNDOTRONIC

El Marco de Seguridad de Protección de Datos Personales de MUNDOTRONIC contiene los procedimientos a aplicarse para dar cumplimiento a lo estipulado en la Ley Orgánica de Telecomunicaciones y salvaguardar los datos personales que han sido confiados a MUNDOTRONIC por parte de sus clientes, usuarios y abonados.

1. Políticas de Seguridad de la Información

Título del documento	Política de seguridad de la información
ID Documento	DP_001
Estado:	Vigente
Versión:	1.0

Historial de cambios			
Versión	Fecha	Descripción	Páginas
1.0	2019-11-25	Creación del documento	Todas

REV. 1	**Nombre y Apellidos**	**Cargo**	**Fecha**	**Firma**
Confeccionado	Katherine Merino	Maestrante	2019-11-25	
Aprobado	Miguel Huaraca	Gerente	2019-11-25	
Revisado	Miguel Huaraca	Gerente	2019-11-25	

Definición de la Política

En conformidad con el Plan Estratégico Empresarial, la entidad establece la siguiente política:

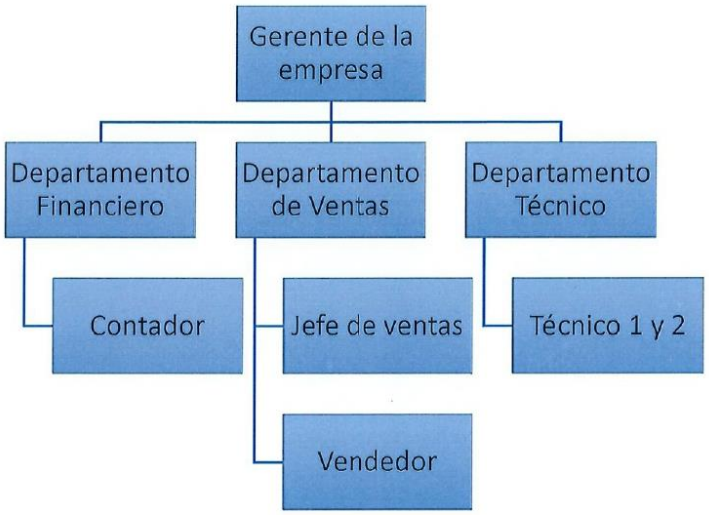
La información entregada en MUNDOTRONIC es considerada como datos importantes para obtener los objetivos propuestos:

- Crecer de forma sólida, estable y segura mediante el fortalecimiento
- Expandir la empresa de forma local, distrital y nacional dentro del mercado de las telecomunicaciones
- Desarrollar proyectos trascendentales dentro del mercado de las telecomunicaciones

A través de la prevención, vigilancia y control de las situaciones de vulnerabilidad, nuestra entidad predispone todos los recursos tanto físicos, tecnológicos, cognitivos y humanos para dirigir y fortalecer la seguridad de la información mediante la instauración, implementación y desarrollo continuo del Marco Referencial de Seguridad de Protección de Datos Personales cuyo propósito es la protección de la privacidad, integridad y disponibilidad de la información mediante la gestión y procedimiento adecuado de la información dentro de los requisitos de la entidad con sus servicios y clientes comprometidos a colaborar activamente en el crecimiento de la educación de seguridad de la información.

2. Organización de la Seguridad

MUNDOTRONIC posee una estructura organizacional vertical, la cual permite establecer quien llevará el liderazgo de la aplicación del Marco de Seguridad de Protección de Datos personales e identificar los roles y responsabilidades que ejercerán dentro del Marco de Seguridad.



Organigrama de MUNDOTRONIC

2.1. Roles y responsabilidades

Comité Directivo

Tiene como objetivo determinar la dirección estratégica de MUNDOTRONIC estableciendo prioridades y políticas de acuerdo con los objetivos de la empresa.

Funciones

- Revisar el seguimiento de prioridades y políticas estratégicas de la organización
- Revisar temas organizacionales y de funcionamiento
- Revisar temas relevantes de los departamentos de MUNDOTRONIC

Comité de Riesgos

Tiene como objetivo desarrollar estrategias que permitan evitar, reducir o transferir los riesgos identificados dentro de MUNDOTRONIC.

Funciones

- Identificar los riesgos a los que están expuesto los datos personales que trata MUNDOTRONIC
- Diseñar estrategias, políticas y procedimientos que permitan mitigar los riesgos
- Asegurarse de la implementación de las estrategias, políticas y procedimientos que permitan mitigar los riesgos
- Diseñar, analizar y aprobar planes de contingencia
- Revisar periódicamente las estrategias, políticas y procedimientos implementados
- Corregir, actualizar las estrategias, políticas y procedimientos implementados

Responsable del tratamiento de los datos personales

Tiene como responsabilidad:

- Clasificar los datos
- Definir su uso
- Definir su ciclo de vida
- Delimitar los privilegios de acceso

Usuarios de la información

Es cualquier persona que no es propietario de los datos y requiere hacer uso de los datos que se almacena en MUNDOTRONIC

Tiene como responsabilidad:

- Conocer y aplicar la política de seguridad de los datos personales
- Ejercer actividades que no afecten los datos personales
- Comunicar al Comité de Riesgos sobre incidentes de seguridad detectados
- Aplicar mejores prácticas recomendadas por la empresa
- Cumplir y hacer cumplir las cláusulas de confidencialidad

Segregación de funciones

Personal	Actividad
Gerente de la empresa	Miembro del comité directivo / Responsable del tratamiento de los datos personales
Jefes de departamentos	Miembros del comité directivo
Jefes de departamentos	Miembros del comité de riesgos

3. Gestión de Activos

En MUNDOTRONIC se ha identificado los siguientes activos que trata datos personales de los usuarios, clientes o abonados.

IDENTIFICADOR	TIPO DE ACTIVO	ACTIVO/RESPONSABLE	TIPOS DE DATOS QUE ADMINISTRAN
[D]	DATOS / INFORMACIÓN	DATOS DEL CLIENTE / JEFE DE VENTAS	Aspectos personales
			Identificadores únicos
			Datos de localización
			Identificadores únicos
		DATOS DE UBICACIÓN DEL SERVICIO / JEFE TÉCNICO	Datos de localización
			Identificadores únicos
			Aspectos personales
		DATOS DE SERVICIOS CONTRATADOS / JEFE DE VENTAS	Preferencias de consumo
			Metadatos
			Estado financiero
			Datos de medios de pago
		DOCUMENTOS DEL CLIENTE / JEFE DE VENTAS	Documentos personales
		DATOS DE LOS EQUIPOS / JEFE TÉCNICO	Identificadores únicos
			Metadatos
[P]	PROCESOS DEL NEGOCIO	PROCESOS DE FACTURACIÓN / JEFE DE VENTAS	Aspectos personales
			Identificadores únicos
			Datos de medios de pago
		PROCESO DE CONTRATACIÓN /	Aspectos personales
			Identificadores únicos
			Datos de localización

		GERENTE DE LA EMPRESA	Identificadores únicos
[HW]	HARDWARE	COMPUTADORA CENTRAL / JEFE TÉCNICO	Identificadores únicos
			Datos de localización
			Preferencias de consumo
			Metadatos
			Estado financiero
			Datos de medios de pago
			Documentos personales
		DISPOSITIVOS MÓVILES / JEFE TÉCNICO	Identificadores únicos
			Datos de localización
[MEDIA]	SOPORTES	DISCOS EXTERNOS / JEFE TÉCNICO	Metadatos
		DISPOSITIVOS USB / JEFE TÉCNICO	Metadatos
[SW]	SOFTWARE	WINDOWS 10 / JEFE TÉCNICO	Aspectos personales
			Identificadores únicos
			Datos de localización
			Preferencias de consumo
			Metadatos
			Estado financiero
			Datos de medios de pago
			Documentos personales
		CCLEANER / JEFE TÉCNICO	Metadatos
		SISTEMA DE FACTURACIÓN / JEFE DE VENTAS	Aspectos personales
			Identificadores únicos
			Datos de medios de pago
[COM]	REDES Y COMUNICACIONES	FIREWALL / JEFE TÉCNICO	Identificadores únicos
			Metadatos
		ROUTERS / JEFE TÉCNICO	Identificadores únicos
			Metadatos
		SWITCH / JEFE TÉCNICO	Metadatos
		MODEMS / JEFE TÉCNICO	Metadatos
[L]	INSTALACIONES	ANTENA TX 1 / JEFE TÉCNICO	Identificadores únicos
			Metadatos
		ANTENA TX 2 / JEFE TÉCNICO	Identificadores únicos
			Metadatos
		ANTENA TX 3 / JEFE TÉCNICO	Identificadores únicos
			Metadatos
[P]	PERSONAL	GERENTE / GERENTE	Aspectos personales
			Identificadores únicos
			Datos de localización
			Preferencias de consumo
			Metadatos
			Estado financiero
			Datos de medios de pago
			Documentos personales
		ADMINISTRADOR / JEFES DE DEPARTAMENTOS	Aspectos personales
			Identificadores únicos
			Datos de medios de pago
		PERSONAL TÉCNICO / TÉCNICOS	Identificadores únicos
			Metadatos

MUNDOTRONIC trata los siguientes tipos de datos:

Los datos que maneja MUNDOTRONIC son los siguientes:

- **Datos del cliente**: Estos se recopilan cuando se establece el contrato con el cliente.

DATOS DEL CLIENTE	TIPO DE DATOS
Nombre del cliente	Aspectos personales
Nacionalidad	Aspectos personales
Sexo	Aspectos personales
Número de Cédula	Identificadores únicos
RUC	Identificadores únicos
Representante legal	Aspectos personales
Razón Social	Aspectos personales
Actividad Económica	Aspectos personales
Dirección del domicilio	Datos de localización
Referencia	Datos de localización
Ciudad	Datos de localización
Parroquia	Datos de localización
Barrio	Datos de localización
Coordenada latitud	Datos de localización
Coordenada longitud	Datos de localización
Tipo de edificación	Datos de localización
Número convencional	Identificadores únicos
Número celular	Identificadores únicos
Correo electrónico	Aspectos personales
Nombre Referencia familiar	Identificadores únicos
Número telefónico Referencia familiar	Identificadores únicos

Tabla 1: Datos del cliente

- **Datos de ubicación del servicio:** Estos datos son receptados al inicio del contrato y se los conserva para realizar las instalaciones y los mantenimientos, forman parte del diseño de red física.

DATOS DE UBICACIÓN DEL SERVICIO	TIPO DE DATOS
Dirección de instalación	Datos de localización
Coordenada latitud	Datos de localización
Coordenada longitud	Datos de localización
Referencia	Datos de localización
Ciudad	Datos de localización
Parroquia	Datos de localización
Tipo de edificación	Datos de localización
Teléfono del sitio	Identificadores únicos
Persona para contactar	Aspectos personales

Tabla 2: Datos de ubicación del servicio

- **Datos del servicio contratado**: Estos se recopilan cuando se establece el contrato con el cliente y se los mantiene para la provisión del servicio y se lo utiliza para clasificar el servicio y el tipo de cliente y estimar el ingreso por cliente.

SERVICIOS CONTRATADOS		TIPO DE DATOS
Características del plan	Tipo de plan (home, corporativo)	Preferencias de consumo
	Medio (FTTH, DSL, otro)	Preferencias de consumo
	Compartición	Preferencias de consumo
	Tasa máxima de bajada (Mbps)	Metadatos
	Tasa mínima de bajada (Mbps)	Metadatos
	Tasa máxima de subida (Mbps)	Metadatos
	Tasa mínima de subida (Mbps)	Metadatos
Servicios y tarifas	Tipo de Servicio	Preferencias de consumo
	Costo de instalación	Estado financiero
	Pago mensual	Estado financiero
	Promociones	Estado financiero
	Productos o servicios adicionales	Estado financiero
	Descuentos	Estado financiero
	Tipo de pago	Datos de medios de pago

Tabla 3: Datos del servicio contratado

- **Documento**: Estos documentos se receptan al inicio del contrato como respaldo de la veracidad de los datos entregados y para ubicar lugar de residencia. Además, se almacenan documentos como copias de las facturas para dar cumplimiento al sistema legal que rigen a las empresas como es el Servicio de Rentas Internas.

DOCUMENTOS	TIPO DE DATOS
Copia de cédula de identidad o pasaporte	Documentos personales
Copia de factura de un servicio básico que demuestre la residencia del solicitante para acceder al servicio	Documentos personales
Copia del RUC	Documentos personales
Copia de cédula o pasaporte de representante legal	Documentos personales
Nombramiento de representante legal	Documentos personales
Facturas de consumo	Documentos personales
Correos electrónicos	Documentos personales

Tabla 4: Documentos receptados y almacenados por MUNDOTRONIC

- **Datos de Equipos**: Los datos identificadores de los equipos se los registra en el diseño lógico de la red para accesos remotos, los datos de monitoreo se los almacena periódicamente.

DATOS DE EQUIPOS	TIPO DE DATOS
IP del equipo del cliente	Identificadores únicos
MAC del equipo del cliente	Identificadores únicos
Datos de monitoreo de comunicaciones	Metadatos
ID de los equipos	Metadatos
Tipos de equipos	Metadatos

Tabla 5: Datos de los equipos de MUNDOTRONIC

4. Control de Acceso a la red

Título del documento	Procesos de Acceso a la red
ID Documento	MS_001
Estado:	Vigente
Versión:	1.0

Historial de cambios			
Versión	Fecha	Descripción	Páginas
1.0	2019-11-25	Creación del documento, versión inicial	Todas

REV. 1	Nombre y Apellidos	Cargo	Fecha	Firma
Confeccionado	Katherine Merino	Maestrante	2019-11-25	
Aprobado.	Miguel Huaraca	Gerente	2019-11-25	
Revisado.	Miguel Huaraca	Gerente	2019-11-25	

Las acciones a realizarse para el control de accesos tienen como fin mitigar, reforzar las acciones de accesos sobre los datos personales.

Responsables y responsabilidades

- **Gerente General:** Supervisar la ejecución de las acciones a realizarse
- **Jefe Técnico:** Responsable de ejecutar las actividades de control de acceso a los sistemas

Actividades

Actividades	Documentos de registro
Acciones entre el ISP y la red corporativa • Reglas ACL • Políticas de Firewall • Reglas NAT • Reglas de Rutas	Catálogo de servicios del ISP
Seguridad en la red corporativa • Deshabilitación de puertos no utilizados • Activación de protocolos a nivel lógico para proteger los puertos de intrusos	Manual Hardening
Máquinas virtuales Protege contra intrusos por medio del firewall principal y firewall del sistema operativo.	
Redes virtuales Crear VLANs como buenas prácticas de seguridades para aislar de otros clientes activos.	Instructivo de creación de VLAN

Observaciones:

Las actividades detalladas anteriormente han sido identificadas como necesarias para ser implementadas, para lo cual se requiere realizar presupuesto y reestructuración de la red corporativa, por lo que estas acciones requieren tiempo y la realización del presupuesto de coste de implementación de las acciones antes mencionadas. Por lo que actualmente solo está documentado. Cabe anotar que MUNDOTRONC si cuenta con acciones de control de acceso a su red.

Título del documento	Procesos de Restricción de acceso a la información
ID Documento	MS_002
Estado:	Vigente
Versión:	1.0

Historial de cambios			
Versión	Fecha	Descripción	Páginas
1.0	2019-11-25	Creación del documento	Todas

REV. 1	Nombre y Apellidos	Cargo	Fecha	Firma
Confeccionado	Katherine Merino	Maestrante	2019-11-25	
Aprobado	Miguel Huaraca	Gerente	2019-11-25	
Revisado	Miguel Huaraca	Gerente	2019-11-25	

Las acciones detalladas en este proceso permiten restringir el acceso y manejo de la información y son de estricto cumplimiento y aplicación a los sistemas y equipos de MUNDOTRONIC

Responsable

Gerente

Jefe técnico

Comité de riesgos

Actividades

1. Todas las aplicaciones y sistemas deben contar con un control de acceso.
2. Las funciones e información confidencial deben ser ocultadas de usuarios de bajos privilegios.
3. Se debe identificar y determinar los datos que deben ser accesibles y disponibles para cada tipo de usuario.
4. La información debe ser restringida de forma selectiva para otorgar permisos de lectura, escritura, borrado, modificado.
5. Establecer restricciones físicas y lógicas para información altamente confidencial.

5. Criptografía

El uso de la criptografía se debe aplicar a dispositivos removibles, equipos de cómputo portátiles, claves de accesos a sistemas, datos, servicios y sobre los correos electrónicos. Por lo que MUNDOTRONIC aplica la política de uso de controles criptográficos.

6. Seguridad física y del entorno

MUNDOTRONIC identificando las razones de ausencia de su personal de las estaciones de trabajo y alejamiento de sus equipos de trabajo asignados crea las siguientes políticas:

- Política de eliminación segura o reutilización de equipos que identifique los procedimientos y métodos de destrucción de la información

- Política de escritorio y pantalla limpia por ausencia del personal de su sitio de trabajo

7. Seguridad de operaciones

MUNDOTRONIC constantemente identifica cambios en sus sistemas por lo que se entiende como evento cualquier cambio importante en la gestión de un elemento o servicio, se crea las siguientes políticas y prendimientos.

- Política para respaldos de la información
- Política de registro de evento
- Políticas de instalación de software en sistemas operativos
- Procesos de gestión de las vulnerabilidades técnicas

Para el registro de eventos se considera que las herramientas deben monitorear el procesamiento de la información, y generar, mantener y revisar registros de las actividades de los usuarios; excepciones, faltas y eventos de seguridad. Los registros de eventos deberían contener:

- ID de usuarios
- Actividades registradas dentro de los sistemas
- Fecha, hora y detalles de los eventos, es decir, el inicio y finalización de la sesión
- Los registros de los intentos exitosos y rechazados de acceso al sistema
- Las direcciones y protocolos de redes

Título del documento	Procesos de gestión de las vulnerabilidades técnicas
ID Documento	MS_003
Estado:	Vigente
Versión:	1.0

Historial de cambios			
Versión	Fecha	Descripción	Páginas
1.0	2019-11-25	Creación del documento, versión inicial	Todas

REV. 1	Nombre y Apellidos	Cargo	Fecha	Firma
Confeccionado	Katherine Merino	Maestrante	2019-11-25	
Aprobado	Miguel Huaraca	Gerente	2019-11-25	
Revisado	Miguel Huaraca	Gerente	2019-11-25	

Las acciones para realizarse en la gestión de vulnerabilidades tienen como objetivo identificar, analizar, priorizar y establecer acciones de mitigación de riesgos.

Responsables:

Comité de Riesgos

Actividades	Descripción de las actividades
Planeación	• Identificar los activos • Identificar los tipos de datos • Identificar sus propietarios • Identificar las amenazas
Ejecución	• Escanear las vulnerabilidades a la que están expuestos los datos personales • Establecer un inicio y fin de pruebas de los sistemas

	• Realizar pruebas de penetración al sistema
Análisis y reportes	• Analizar el nivel de criticidad de los activos • Identificar falsos positivos • Identificar los activos con más nivel de riesgos • Realizar recomendaciones de acciones para mitigar los riesgos • Realizar informe de entrega de resultados a las partes interesadas
Remediación	• Ejecutar las acciones de mitigación por parte de los responsables

8. Seguridad de las comunicaciones

Título del documento	Procesos de seguridad de las comunicaciones
ID Documento	MS_004
Estado:	Vigente
Versión:	1.0

Historial de cambios			
Versión	Fecha	Descripción	Páginas
1.0	2019-11-25	Creación del documento, versión inicial	Todas

REV. 1	**Nombre y Apellidos**	**Cargo**	**Fecha**	**Firma**
Confeccionado	Katherine Merino	Maestrante	2019-11-25	
Aprobado	Miguel Huaraca	Gerente	2019-11-25	
Revisado	Miguel Huaraca	Gerente	2019-11-25	

Las acciones para realizarse en el proceso de seguridad de las comunicaciones tienen como fin implementar acciones de hardening en la red de MUNDOTRONIC.

Responsables:

Gerente

Jefe técnico

Comité de riesgos

Actividades	**Descripción de las actividades**
Instalar solo lo necesario	Se debe identificar los equipos que realmente se necesita para que el diseño de red sea óptima, robusta y segura.
Configurar Grupos y permisos	Se debe identificar el tipo de usuario que tendrá acceso al sistema y a los equipos ya que cada usuario tiene diferentes requerimientos.
Implementar controles de seguridad	Se debe identificar los equipos y los riesgos a los que están expuestos e implementar acciones de mitigación como: firewall, sistemas de detección y prevención de intrusos, antivirus, sacar copias de respaldos de la información, realizar pruebas de seguridad, actualizar los softwares e instalar parches.
Planes de recuperación	Se debe crear acciones de contingencia en el caso de materializarse una amenaza.
Concientización	El personal debe tomar conciencia de la necesidad de la seguridad en la red, esta actividad debe estar a cargo del comité de riesgos.

Observaciones:

Esta actividad quedará documentada ya que la empresa no cuenta con el presupuesto para la realización de este proceso.

Título del documento	Cláusulas de transferencias de información
ID Documento	MS_005
Estado:	Vigente
Versión:	1.0

Historial de cambios			
Versión	Fecha	Descripción	Páginas
1.0	2019-11-25	Creación del documento, versión inicial	Todas

REV. 1	Nombre y Apellidos	Cargo	Fecha	Firma
Confeccionado	Katherine Merino	Maestrante	2019-11-25	
Aprobado	Miguel Huaraca	Gerente	2019-11-25	
Revisado	Miguel Huaraca	Gerente	2019-11-25	

Para la transferencia de información MUNDOTRONIC crea:

- Cláusulas de transferencia de información
- Polítticas de transferencia de información

Este documento tiene como objetivo establecer las cláusulas a cumplirse entre las partes involucradas en la transferencia de información.

Responsables:

Gerente general

Comité de riesgos

Partes interesadas:

MUNDOTRONIC

Clientes, usuarios o abonados.

Acciones:

Aplicar cláusulas de transferencia de información.

CLAÚSULAS

Confidencialidad

- MUNDOTRONIC obliga en forma irrevocable a no revelar, divulgar o facilitar bajo cualquier forma a persona alguna sea natural o jurídica, pública o privada, o de cualquier otra naturaleza, y a no utilizar para su propio beneficio o de un tercero, toda la información generada durante la vigencia del contrato establecido con sus clientes. Solo se revelará la información en el caso de existir una orden judicial o que exista una autorización por escrito por parte de los clientes.

Datos personales

- MUNDOTRONIC llevará a cabo el tratamiento de datos por personal calificado, autorizado y capacitado para ello, estableciendo niveles de acceso y claves, quienes cumplirán con el deber de confidencialidad, seguridad y protección de la información personal, suscribiendo convenios a tales fines. Estos usuarios dependientes de MUNDOTRONIC deberán recibir adecuado entrenamiento en la materia de protección de datos personales y privacidad. A su vez, deberá notificar al cliente de cualquier cambio. Sólo se notificará el cambio de estado, sin identificar las razones de este, de manera tal de que no se vulnere la legislación laboral aplicable.
- MUNDOTRONIC deberá notificar inmediatamente al cliente sobre:
    - Cualquier solicitud de una autoridad de aplicación jurídicamente vinculante que tuviere como objeto la divulgación de los datos personales a los que tuviera acceso a menos que la ley lo prohíba.
    - Cualquier incidente de seguridad que afecte la información de carácter personal, como por ejemplo, un acceso no autorizado o accidental.
- MUNDOTRONIC deberá efectuar la comunicación inicial con el cliente incluyendo en dicha comunicación cualquier información que pudiera ser relevante para resolver la solicitud o la queja.
- Suprimir inmediatamente la información personal en cualquiera de los siguientes casos, salvo que exista algún impedimento legal para ello:
    - Cuando haya terminado la relación jurídica con el cliente
    - Por instrucciones expresas y por escrito del cliente

  En cualquier caso, previamente a la eliminación de la información personal, MUNDOTRONIC deberá haber hecho entrega de esta al cliente. Asimismo, MUNDOTRONIC utilizará un borrado seguro y permanente, y le proporcionará al cliente una certificación por escrito de lo anterior mencionado, dicha certificación estará firmada por un representante autorizado MUNDOTRONIC.
- Para cualquier transferencia de información personal, las partes suscribirán adicionalmente un Acuerdo de Transferencia de Datos.

9. Adquisición, desarrollo y mantenimiento de sistemas

Para dar cumplimiento con la protección de la información en ambientes de prueba, MUNDOTRONIC crea la política de transferencia de información siendo su responsable el departamento técnico.

Título del documento	Procedimientos de especificación de requisitos de seguridad de la información
ID Documento	MS_006
Estado:	Vigente
Versión:	1.0

Historial de cambios			
Versión	Fecha	Descripción	Páginas
1.0	2019-11-25	Creación del documento, versión inicial	Todas

REV. 1	**Nombre y Apellidos**	**Cargo**	**Fecha**	**Firma**
Confeccionado	Katherine Merino	Maestrante	2019-11-25	
Aprobado	Miguel Huaraca	Gerente	2019-11-25	
Revisado	Miguel Huaraca	Gerente	2019-11-25	

Este documento tiene como objetivo establecer los procedimientos de análisis y especificación de requisitos de seguridad de la información

Responsables:

Gerente general

Comité de riesgos

Actividades

- Los sistemas operativos de los equipos deben estar parchados en el caso que se requiera actualizaciones manuales, caso contrario deberá estar activa las actualizaciones automáticas.
- Los servicios de red solo deben tener activos los servicios necesarios y los servicios que no se requieran deberán estar desactivados.
- Los servicios de red deben ser monitoreados para resolver fallas de seguridad en el servicio.
- Los sistemas deben tener contraseñas seguras y ser almacenadas con claves ssh.
- Los sistemas operativos deben tener antivirus y firewall activos.
- Los antivirus deben tener las actualizaciones automáticas.

Acciones:

Aplicar medidas y políticas establecidas en el Marco de Seguridad.

10. Gestión de incidentes de seguridad de la información

Título del documento	Proceso de gestión de Incidentes
ID Documento	MS_007
Estado:	Vigente
Versión:	1.0

Historial de cambios			
Versión	Fecha	Descripción	Páginas
1.0	2019-11-25	Creación del documento, versión inicial	Todas

REV. 1	Nombre y Apellidos	Cargo	Fecha	Firma
Confeccionado	Katherine Merino	Maestrante	2019-11-25	
Aprobado	Miguel Huaraca	Gerente	2019-11-25	
Revisado	Miguel Huaraca	Gerente	2019-11-25	

Este documento tiene como objetivo establecer como herramienta de trabajo el análisis de riesgos para asegurar los datos que procesa MUNDOTRONIC.

Responsables:

Gerente general

Comité de riesgos

Actividades

- Realizar la evaluación de riesgos e identificar su impacto
- Realizar la estimación del riesgo y su importancia
- Priorizar el riesgo
- Establecer criterios de aceptación y transferencia del riesgo
- Identificación de acciones de mitigación
- Priorizar los riesgos
- Aplicar medidas de seguridad
- Generar informes de los riesgos

Acciones:

Aplicar medidas y políticas establecidas en el Marco de Seguridad

11. Aspectos de seguridad de la información de la gestión de continuidad de negocio

Título del documento	Proceso para disponibilidad de instalaciones de procesamiento de información
ID Documento	MS_009
Estado:	Vigente
Versión:	1.0

Historial de cambios			
Versión	Fecha	Descripción	Páginas
1.0	2019-11-25	Creación del documento, versión inicial	Todas

REV. 1	Nombre y Apellidos	Cargo	Fecha	Firma
Confeccionado	Katherine Merino	Maestrante	2019-11-25	
Aprobado	Miguel Huaraca	Gerente	2019-11-25	
Revisado	Miguel Huaraca	Gerente	2019-11-25	

Este documento tiene como objetivo establecer los procesos para mantener la disponibilidad de las instalaciones que procesan información.

Responsables:

Gerente general

Comité de riesgos

Departamento técnico

Actividades

- Inventariar los equipos existentes dentro de MUNDOTRONIC
- Identificar el responsable de cada elemento que forme parte de las instalaciones de MUNDOTRONIC
- Revisar periódicamente las instalaciones y cumplir con los requerimientos normativos
- Identificar un lugar alterno para instalaciones alternas
- Monitorear el funcionamiento de las instalaciones alternas

12. Cumplimiento

Título del documento	Procedimiento de cumplimiento legales
ID Documento	MS_010
Estado:	Vigente
Versión:	1.0

Historial de cambios			
Versión	Fecha	Descripción	Páginas
1.0	2019-11-25	Creación del documento, versión inicial	Todas

REV. 1	Nombre y Apellidos	Cargo	Fecha	Firma
Confeccionado	Katherine Merino	Maestrante	2019-11-25	
Aprobado	Miguel Huaraca	Gerente	2019-11-25	
Revisado	Miguel Huaraca	Gerente	2019-11-25	

Este documento tiene como objetivo detectar el nivel de seguridad que debe cumplir en el entorno legal.

Actividades

- Es responsabilidad del Gerente administrar las actividades legales que debe cumplir la empresa.

- Es responsabilidad del Gerente salvaguardar las evidencias del cumplimiento legal.
- Es responsabilidad del Gerente identificar las medidas y procedimientos exigidos por las entidades de regulación.

Actividades a dar cumplimiento:

- Cumplir con: Art. 22, Art. 23, Art. 24, Art. 76, Art. 77, Art. 78 y Art. 81 estipulados en la Ley Orgánica de Telecomunicaciones
- Establecer cláusulas de confidencialidad
- Identificar derechos y responsabilidades de los usuarios, clientes y abonados

Título del documento	Procedimiento de revisiones de seguridad de la información
ID Documento	MS_011
Estado:	Vigente
Versión:	1.0

Historial de cambios			
Versión	Fecha	Descripción	Páginas
1.0	2019-11-25	Creación del documento, versión inicial	Todas

REV. 1	**Nombre y Apellidos**	**Cargo**	**Fecha**	**Firma**
Confeccionado	Katherine Merino	Maestrante	2019-11-25	
Aprobado	Miguel Huaraca	Gerente	2019-11-25	
Revisado	Miguel Huaraca	Gerente	2019-11-25	

Este documento tiene como objetivo establecer los procedimientos a seguir para realizar las revisiones de seguridad de la información.

Actividades

- Es responsabilidad del comité de riesgos realizar las revisiones de seguridad.
- Identificar las políticas, procedimientos y normativas que MUNDOTRONIC debe cumplir.
- Realizar un cronograma de verificación de cumplimiento de políticas, procedimientos y normativas que se debe cumplir.
- Identificar los responsables de las políticas, procedimientos y normativas que se den cumplir.
- Verificar el cumplimiento de las políticas, procedimientos y normativas que se den cumplir.
- Realizar mejorar en los procesos de cumplimiento de las políticas, procedimientos y normativas que se den cumplir.

13. Políticas

13.1. Política de uso de dispositivos móviles

Título del documento	Política de uso de dispositivos móviles
ID Documento	DP_002
Estado:	Vigente
Versión:	1.0

Historial de cambios			
Versión	Fecha	Descripción	Páginas
1.0	2019-11-25	Creación del documento	Todas

REV. 1	Nombre y Apellidos	Cargo	Fecha	Firma
Confeccionado	Katherine Merino	Maestrante	2019-11-25	
Aprobado	Miguel Huaraca	Gerente	2019-11-25	
Revisado	Miguel Huaraca	Gerente	2019-11-25	

Debido a que ciertos trabajos deben realizar en sitios externos a la empresa, MUNDOTRONIC permite a los empleados usar sus propios dispositivos, y considerando que pueden conectarse a cualquier red, que cualquier persona puede hacer uso o se pueden perder, ha decidido crear unas polfticas para asegurar las aplicaciones contenidas dentro de estos dispositivos.

Polftica de uso de dispositivos móviles

Objetivo:

La política de uso de dispositivos móviles tiene como objetivo tener el control sobre la información a la que van a acceder sus empleados a través de los dispositivos personales, los cuales serán capaces de almacenar, transferir y gestionar información de MUNDOTRONIC.

Alcance:

Aplica para todo el personal de MUNDOTRONIC que maneje cartera de clientes y realicen actividades externas a la empresa.

Política de la empresa:

MUNDOTRONIC se reserva el derecho sobre control y propiedad de los datos gestionados en los dispositivos móvil y faculta solo a personal autorizado el almacenamiento, transferencia y gestión de información desde este.

Personal que tiene acceso:

Será responsabilidad de Talento Humano decidir aquellas personas que requieren hacer uso de dispositivos móviles y generar una lista del personal y las aplicaciones que necesiten para cumplir con su trabajo.

El responsable del tratamiento de los datos personales será el encargado de enrolar y monitorizar al usuario con los sistemas de MUNDOTRONIC, además de generar una lista negra de las aplicaciones prohibidas.

Dispositivos permitidos:

El responsable del tratamiento de los datos personales aprobará, gestionará y monitorizará la lista de dispositivos admitidos, además de realizar las configuraciones previas para la vinculación a los sistemas de MUNDOTRONIC.

Será obligatorio que los dispositivos aprobados tengan las siguientes características:

- Firewall recomendado por el responsable de TI
- Sistema de copias de seguridad cada 24 horas mediante Active Directory
- Bloqueo de pantallas
- Doble autenticación por patrón y mediante huella digital
- Antivirus instalado
- Software de prevención de intrusos
- Acceso a VPN cuando hagan uso de los sistemas de MUNDOTRONIC

Responsabilidad del dueño del dispositivo móvil

- Debe asegurarse que el dispositivo esté vinculado al Active Directory para que se realicen las copias de seguridad en el horario establecido.
- Asegurarse que se encuentren instaladas las aplicaciones de seguridad.
- Ingresar a los sistemas de MUNDOTRONIC mediante VPN.
- Activar la doble autenticación para acceder al dispositivo.
- No compartir la información de MUNDOTRONIC por redes inalámbricas WIFI, solo por la red de datos (red celular).
- Permitir actualizaciones.
- Notificar al responsable del tratamiento de los datos personales en caso de perder, vender, dañar o entregar a terceros los dispositivos móviles.
- No instalar aplicaciones que estén en la lista negra.
- No instalar software sin licencia.
- Cumplir con un acuerdo de responsabilidad y cumplimiento de políticas.

Derechos de MUNDOTRONIC

MUNDOTRONIC tiene el derecho sobre la propiedad de los datos contenidos en un BYOD previamente autorizado. Es decir, tiene el derecho a ver, editar, eliminar, monitorizar, gestionar los datos que se encuentran en un dispositivo móvil.

Seguridad

Todos los incidentes de seguridad deberán ser reportados al comité de riesgos.

Capacitación y concientización

Todos los empleados que harán uso de un dispositivo móvil deberán ser previamente capacitados antes de hacer uso de las aplicaciones institucionales instaladas en sus dispositivos.

13.2. Política de devolución de activos

Título del documento	Política de devolución de activos
ID Documento	DP_003
Estado:	Vigente
Versión:	1.0

Historial de cambios			
Versión	Fecha	Descripción	Páginas
1.0	2019-11-25	Creación del documento	Todas

REV. 1	**Nombre y Apellidos**	**Cargo**	**Fecha**	**Firma**
Confeccionado	Katherine Merino	Maestrante	2019-11-25	
Aprobado	Miguel Huaraca	Gerente	2019-11-25	
Revisado	Miguel Huaraca	Gerente	2019-11-25	

Una vez identificados los activos y sus propietarios esos deben ser utilizados para el fin que fueron adquiridos, pero en el caso de que ya no son requeridos se deberá aplicar la presente política.

Objetivo:

Establecer el procedimiento y razones de la recepción de los activos en caso de devoluciones y determinar la disposición final de estos.

Alcance

Estos procedimientos se aplican cuando se considere que los activos ya no requieren ser usados por el personal o departamento al que fue asignado y proceder a fijar la disposición final de estos.

Política de devolución de activos

MUNDOTRONIC se reserva el derecho sobre control y propiedad de los activos y faculta solo a personal autorizado para su reubicación, donación, venta y eliminación de los activos.

Responsable

Es responsabilidad del jefe técnico decidir sobre la disposición final de los activos y gestionar las devoluciones, reubicaciones, baja de activo por donación, venta, daño, robo u otro factor que afecte al activo para ya no estar con su propietario.

Condiciones generales para considerar devolución de activos

- Por vejez, daño y obsolescencia
- Por cambios de tecnología y remodelación
- Por salida de personal o cambio de departamento de trabajo

Acciones por realizarse con los activos revueltos

- Reubicación de activos entre los departamentos
- Donar los activos
- Regalar los activos
- Vender los activos

Eventos para la baja de activos

Por:

- Venta
- Daño
- Donación
- Robo

Responsabilidades del responsable de devoluciones de los activos

- Inventariar los activos existentes en MUNDOTRONIC
- Llevar un registro de los propietarios de los activos
- En caso de devoluciones registrar:
  - Identificador del activo
  - Propietario
  - Motivo de la devolución
  - Estado del activo
  - Acciones para realizarse con el activo
  - Determinar el tipo de dato que gestionaba
- En el caso de reportase una pérdida o robo reportar al comité de riesgos y al responsable de tratamiento de datos

Derechos de MUNDOTRONIC

MUNDOTRONIC tiene el derecho a solicitar la reposición del activo o asignar una penalización a su personal en el caso de ser culpa del propietario del activo la pérdida o daño del activo en cuestión.

MUNDOTRONIC reemplazará y cubrirá con los gastos sobre el activo que se perdió o fue robado si el propietario del activo no fue culpable de las afecciones.

Seguridad

Todos los incidentes de seguridad deberán ser reportados al comité de riesgos.

Capacitación y concientización

Todos los empleados deberán ser previamente notificados y capacitados sobre las devoluciones de los activos.

Plantilla de registro de devolución de activos

ID de activo	
Nombre del activo	
Dueño del activo	
Nombre del que recibe	
Fecha de devolución del activo	
Motivo de devolución	
Estado del activo	
Acción para realizarse luego de la devolución	

13.3. Política de uso de medios removibles

Título del documento	Política de uso de medios removibles.
ID Documento	DP_004
Estado:	Vigente
Versión:	1.0

Historial de cambios			
Versión	Fecha	Descripción	Páginas
1.0	2019-11-25	Creación del documento	Todas

REV. 1	Nombre y Apellidos	Cargo	Fecha	Firma
Confeccionado	Katherine Merino	Maestrante	2019-11-25	
Aprobado	Miguel Huaraca	Gerente	2019-11-25	
Revisado	Miguel Huaraca	Gerente	2019-11-25	

El uso de los medios removibles dentro de MUNDOTRONIC es común por lo que es necesario establecer los procedimientos de seguridad para el uso correcto de los medios removibles.

Objetivo

Delinear las responsabilidades y acciones a tomar sobre el uso de los medios removibles para salvaguardar la información contenida en estos.

Alcance

Esta política se aplica al uso de medios removibles identificados en MUNDOTRONIC y sobre los datos personales que trata.

Política

MUNDOTRONIC se reserva el derecho de especificar las acciones a realizarse sobre los dispositivos removibles que tienen relación con el tratamiento de los datos personales. Considerando las formas de uso, transferencia y almacenamiento de los datos en los medios removibles de forma segura.

Medios removibles permitidos

- Los medios removibles aceptados dentro de la compañía son aquellos que responden a las necesidades de la organización.

- El uso de los medios removibles dentro de la empresa debe ser aprobados por el encargado de activos.

Uso de medios removibles permitidos

- Ningún medio removible que no sea aprobado podrá utilizarse dentro de la organización.
- No se debe utilizar medios removibles en mal estado como: oxidados, mojados o infectados.
- Todos los medios removibles permitidos deben contener antivirus actualizados.

Seguridad de datos en medios removibles permitidos

- Si el contenido del medio removible contiene información sensible como los datos personales deberá ser encriptado.
- Todo software instalado en un medio removible debe ser instalado por personal autorizado dentro de la organización.
- Todo medio removible desde ser almacenado y guardado en un ambiente seguro.

Uso de medios removibles permitidos por terceros

- Si un tercero desea hacer uso de un medio removible requiere un permiso por parte de la empresa.

Desecho de medios removibles

- Si un medio removible deja de ser requerido se lo deberá notificar al encargado de devolución de activos.
- Para evitarse fugas de información estos deben ser limpiados.

Derechos de MUNDOTRONIC

MUNDOTRONIC tiene el derecho a solicitar la reposición del medio removible o una penalización a su personal en el caso de ser culpa del propietario la pérdida o daño del medio removible en cuestión.

MUNDOTRONIC reemplazará y cubrirá con los gastos sobre el a medio removible que se perdió o fue robado si el propietario del activo no fue culpable de las afecciones.

Seguridad

Todos los incidentes de seguridad deberán ser reportados al comité de riesgos.

Capacitación y concientización

Todos los empleados deberán ser previamente notificados y capacitados sobre el uso de medios removibles.

13.4. Política de control de acceso

Título del documento	Política de control de acceso
ID Documento	DP_005
Estado:	Vigente
Versión:	1.0

Historial de cambios			
Versión	Fecha	Descripción	Páginas
1.0	2019-11-25	Creación del documento	Todas

REV. 1	Nombre y Apellidos	Cargo	Fecha	Firma
Confeccionado	Katherine Merino	Maestrante	2019-11-25	
Aprobado	Miguel Huaraca	Gerente	2019-11-25	
Revisado	Miguel Huaraca	Gerente	2019-11-25	

MUNDOTRONIC para salvaguardas la información contenida en sus sistemas crea la política de control de acceso.

Objetivo

Establecer las acciones que protejan los sistemas de MUNDOTRONIC contra accesos no autorizados.

Alcance

Esta política se aplica a todos los procesos y equipos que traten información de carácter personal de MUNDOTRONIC.

Política

MUNDOTRONIC se reserva el derecho de especificar las acciones a implementarse para los accesos a sus sistemas.

Actividades

- Se debe asignar al personal un usuario y contraseña de acceso a los sistemas.
- Para generar los accesos sin ser usuarios registrados se debe contar con un permiso del Gerente General y un responsable de la organización
- En el caso de terminar la relación de dependencia del personal con la empresa, el usuario debe ser dado de baja.
- Se deberá revisar periódicamente las cuentas de usuarios y sus privilegios para verificar que solo personal autorizado tenga acceso a los recursos necesarios.

- Es responsabilidad del personal el uso de usuario y contraseña asignados.
- El personal no debe compartir sus usuarios y contraseñas con personas externas a la empresa.
- Es responsabilidad del área técnica establecer los procedimientos de creación, activación y baja de usuarios y contraseñas.

Derechos de MUNDOTRONIC

MUNDOTRONIC tiene el derecho de establecer las acciones a seguirse para los accesos a los sistemas y sancionar al personal por mal uso de sus usuarios y contraseñas.

Seguridad

Todos los incidentes de seguridad deberán ser reportados al comité de riesgos.

Capacitación y concientización

Todos los empleados deberán ser previamente notificados y capacitados sobre los controles de accesos a los sistemas.

13.5. Política sobre el uso de los servicios de red

Título del documento	Política sobre el uso de los servicios de red
ID Documento	DP_006
Estado:	Vigente
Versión:	1.0

Historial de cambios			
Versión	Fecha	Descripción	Páginas
1.0	2019-11-25	Creación del documento	Todas

REV. 1	Nombre y Apellidos	Cargo	Fecha	Firma
Confeccionado	Katherine Merino	Maestrante	2019-11-25	
Aprobado	Miguel Huaraca	Gerente	2019-11-25	
Revisado	Miguel Huaraca	Gerente	2019-11-25	

MUNDOTRONIC para asegurar los servicios de red y considerando la necesidad de establecer procedimientos de uso de los servicios de red crea la política sobre el uso de los servicios de red.

Objetivo

Establecer las acciones para controlar el uso de la red corporativa de MUNDOTRONIC.

Alcance

Esta política se aplica al personal y usuarios autorizados de acceso a la red de datos de MUNDOTRONIC.

Política

MUNDOTRONIC se reserva el derecho de especificar los procedimientos de uso de la red de datos.

Actividades

- La red interna de MUNDOTRONIC es de uso exclusivo para dar cumplimiento las labores del personal.
- El personal solo podrá acceder a los servicios que le ha sido delegado para gestionar.
- El personal no debe realizar copias no autorizadas de la información contenida dentro de la red de MUNDOTRONIC.
- Para accesos remotos es responsabilidad del área técnica la aplicación de métodos apropiados para la conexión con la red.
- El área técnica deberá crea controles de autenticación para accesos remotos.
- Es responsabilidad del área técnica establecer procedimientos de identificación de equipos.
- Es responsabilidad del área técnica mantener actualizados los registros de los componentes de la red.
- Es responsabilidad del área técnica llevar los registros de errores y fallas de los componentes de la red.
- Es responsabilidad del área técnica identificar y notificar amenazas a los que se encuentran expuestos los equipos de red.

Derechos de MUNDOTRONIC

MUNDOTRONIC tiene el derecho a establecer los procedimientos de uso de red y sancionar al personal en caso de incumplir con estos.

Seguridad

Todos los incidentes de seguridad deberán ser reportados al comité de riesgos.

Capacitación y concientización

Todos los empleados deberán ser previamente notificados y capacitados sobre uso de la red.

13.6. Política sobre el uso de controles criptográficos

Título del documento	Política sobre el uso de controles criptográficos
ID Documento	DP_007
Estado:	Vigente
Versión:	1.0

Historial de cambios			
Versión	Fecha	Descripción	Páginas
1.0	2019-11-25	Creación del documento	Todas

REV. 1	**Nombre y Apellidos**	**Cargo**	**Fecha**	**Firma**
Confeccionado	Katherine Merino	Maestrante	2019-11-25	
Aprobado	Miguel Huaraca	Gerente	2019-11-25	
Revisado	Miguel Huaraca	Gerente	2019-11-25	

MUNDOTRONIC en su afán de proteger la confidencialidad, la autenticidad y la integridad de los datos crea la política sobre el uso de controles criptográficos.

Objetivo

Asegurar el uso apropiado de la criptografía para proteger la confidencialidad, la autenticidad y la integridad de los datos.

Alcance

Esta política presenta las acciones a realizarse sobre los dispositivos y servicios de MUNDOTRONIC que requieran criptografía.

Política

MUNDOTRONIC se reserva el derecho de especificar las acciones sobre el uso de controles criptográficos que tienen relación con el tratamiento de los datos personales, siendo el responsable de esta política el responsable de tratamiento de datos personales.

Activos sobre los que se aplica la política

Se debe implementar sobre:

- Dispositivos de uso removible
- Claves de acceso a sistemas y datos
- Información digital con datos sensibles
- Correos electrónicos del personal de MUNDOTRONIC

Procedimientos para realizarse

- Identificar los elementos que requieren encriptación.
- Utilizar mecanismos de cifrado de datos para información reservada.
- Activar cifrado para los correos dentro los navegadores.
- El tiempo de vida de las llaves criptográficas es de 3 meses.

- Llevar un registro de cambios de llaves criptográficas.
- Es de responsabilidad del personal de MUNDOTRONIC almacenar y proteger las llaves criptográficas.

Derechos de MUNDOTRONIC

MUNDOTRONIC tiene el derecho de gestionar y mantener un repositorio de llaves criptográficas.

Seguridad

Todos los incidentes de seguridad deberán ser reportados al comité de riesgos.

Capacitación y concientización

Todos los empleados deberán ser previamente notificados y capacitados sobre el uso de controles criptográficos.

13.7. Política de eliminación segura o reutilización de equipos

Título del documento	Política de eliminación segura o reutilización de equipos
ID Documento	DP_008
Estado:	Vigente
Versión:	1.0

Historial de cambios			
Versión	Fecha	Descripción	Páginas
1.0	2019-11-25	Creación del documento	Todas

REV. 1	**Nombre y Apellidos**	**Cargo**	**Fecha**	**Firma**
Confeccionado	Katherine Merino	Maestrante	2019-11-25	
Aprobado	Miguel Huaraca	Gerente	2019-11-25	
Revisado	Miguel Huaraca	Gerente	2019-11-25	

MUNDOTRONIC en su afán de controlar los procedimientos de eliminación segura y de la reutilización de los equipos procede a la creación e implementación de la política de eliminación segura o reutilización de equipos.

Objetivo

Describir la forma de manipulación de los dispositivos y la metodología de eliminación de la información contenido en estos, además de evitar un traspaso no seguro de los equipos y los datos.

Alcance

Esta política presenta los procedimientos para terminar el ciclo de vida de los dispositivos y los datos.

Política

MUNDOTRONIC se reserva el derecho de especificar las acciones de eliminación segura y de la reutilización de los equipos que tienen relación con el tratamiento de los datos personales, siendo el responsable de esta política el responsable de tratamiento de datos personales y el responsable de los activos.

Actividades

- Cuando se requiera reutilizar los equipos estos deben ser gestionados por parte del responsable de los activos para que proceda con la eliminación de la información y proceder con la asignación de su nuevo propietario.
- Los medios electromagnéticos que contengan información sensible de carácter personales deben ser borrados, eliminados y destruidos de forma segura.
- Cuando un medio se ha considerado para ser descartado de uso, se debe eliminar la información contenida y proceder con su destrucción.
- Identificar la información contenida y de ser necesario realizar una copia de seguridad.

Métodos de destrucción de la información

Desmagnetización: Consiste en exponer al dispositivo a un potente campo magnético, este procedimiento se debe aplicar a discos duros y DVDs.

Sobreescritura: consiste en modificar los valores almacenados, se aplica en dispositivos regrabables para reutilizar los equipos.

Derechos de MUNDOTRONIC

MUNDOTRONIC tiene el derecho de eliminar y reutilizar sus activos en el caso de ser necesario para la organización.

MUNDOTRONIC es propietario de toda la información que se cree dentro de la organización y se transmita dentro de sus redes, por lo que también tiene el derecho a decidir sobre el futuro de los datos.

Seguridad

Todos los incidentes de seguridad deberán ser reportados al comité de riesgos.

Capacitación y concientización

Todos los empleados deberán ser previamente notificados y capacitados sobre la eliminación segura o reutilización de equipos.

13.8. Política de escritorio y pantalla limpia

Título del documento	Política de escritorio y pantalla limpia
ID Documento	DP_009
Estado:	Vigente
Versión:	1.0

Historial de cambios			
Versión	Fecha	Descripción	Páginas
1.0	2019-11-25	Creación del documento	Todas

REV. 1	**Nombre y Apellidos**	**Cargo**	**Fecha**	**Firma**
Confeccionado	Katherine Merino	Maestrante	2019-11-25	
Aprobado	Miguel Huaraca	Gerente	2019-11-25	
Revisado	Miguel Huaraca	Gerente	2019-11-25	

MUNDOTRONIC en su afán de controlar los procedimientos para salvaguardar los datos y documentos crea la política de escritorio y pantalla limpia.

Objetivo

Prevenir el robo y pérdida de la información dentro de las estaciones de trabajo y de los equipos de trabajo asignados por MUNDOTRONIC.

Alcance

Esta política se aplica a la protección de la información contenida en las estaciones de trabajo y los equipos de asignados por MUNDOTRONIC.

Política

MUNDOTRONIC se reserva el derecho de especificar las acciones para garantizar escritorio y pantalla limpia, y salvaguardar los documentos que se encuentran en las estaciones de trabajo y el acceso no autorizado a los equipos asignados.

Actividades de Escritorios limpios

- Para la ausencia de la estación de trabajo el personal debe ubicar los documentos y medio magnético u óptico en un sitio seguro y de difícil acceso.
- Al finalizar la jornada de trabajo se deberán guardar en un lugar seguro los documentos y medios que contengan información de MUNDOTRONIC.
- Cuando se imprima documentos con datos importantes deberá ser retirada inmediatamente.

Actividades de Pantallas limpias

- La pantalla de computador debe estar libre de archivos o enlaces a los sistemas de MUNDOTRONIC para el caso de requerir ausentarse de la ubicación de donde se encuentre el computador.
- Antes de ausentarse de la estación de trabajo el personal deberá bloquear las sesiones y bloquear los equipos de cómputo y demás dispositivos que se estén utilizando.
- Todos los computadores y dispositivos portátiles deberán tener aplicado el cierre de sesión por inactividad con un tiempo de espera de 5 minutos de inactividad.

Derechos de MUNDOTRONIC

MUNDOTRONIC tiene el derecho a solicitar escritorios y pantallas limpias a su personal para salvaguardar la información, documentos y los dispositivos que estén en uso y que sean de fácil traslado y visualización.

MUNDOTRONIC tiene el derecho de sancionar a su personal por incumplimiento de esta política.

Seguridad

Todos los incidentes de seguridad deberán ser reportados al comité de riesgos.

Capacitación y concientización

Todos los empleados deberán ser previamente notificados y capacitados sobre las acciones para garantizar escritorio y pantalla limpia.

13.9. Política para respaldos de la información

Título del documento	Política para respaldos de la información
ID Documento	DP_0010
Estado:	Vigente
Versión:	1.0

Historial de cambios			
Versión	Fecha	Descripción	Páginas
1.0	2019-11-25	Creación del documento	Todas

REV. 1	**Nombre y Apellidos**	**Cargo**	**Fecha**	**Firma**
Confeccionado	Katherine Merino	Maestrante	2019-11-25	
Aprobado	Miguel Huaraca	Gerente	2019-11-25	
Revisado	Miguel Huaraca	Gerente	2019-11-25	

MUNDOTRONIC en su afán de controlar los procedimientos para salvaguardar los datos y documentos crea la política de respaldos de la información.

Objetivo

Proporcionar los procedimientos necesarios para respaldar la información digital de MUNDOTRONIC y minimizar los riesgos por pérdida de información y salvaguardar su disponibilidad e integridad.

Alcance

Esta política se aplica para respaldar la información digital de MUNDOTRONIC y mantenerlos disponibles en el caso de requerirlos.

Política

MUNDOTRONIC se reserva el derecho de especificar las acciones para garantizar el respaldo de la información contenida en sus servidores y equipos de trabajo.

Actividades para el respaldo de información

- Actualizar cada cuatro meses las configuraciones de respaldo de los servidores y equipos de trabajo.
- Efectuar respaldo de la información si se efectúa una modificación significativa en los servidores y equipos de trabajo.
- Respaldar la información de los servidores y equipos de trabajo al finalizar el año.
- Para los recursos compartidos se realizarán respaldos diarios.
- El tiempo máximo de almacenamiento de la información de las estaciones de trabajo será de 3 meses a menos que se contenga información relevante para la organización.
- Los respaldos se realizarán en horas diferentes a las laborales a través de procesos automáticos.
- El tiempo máximo para restaurar la información no debe superar a un día laboral.

Registros de los respaldos de información

- Es responsabilidad del departamento técnico llevar el registro de los respaldos de información.
- Es responsabilidad del departamento técnico asegurar los contenedores de información.

- Es responsabilidad del departamento técnico comprobar la integridad y confiabilidad de la información respaldada.
- Se debe verificar cada 6 meses la integridad física de los contenedores de los respaldos.

Derechos de MUNDOTRONIC

MUNDOTRONIC tiene el derecho a establecer los procedimientos de respaldos de la información contenida dentro de su organización.

Seguridad

Todos los incidentes de seguridad deberán ser reportados al comité de riesgos.

Capacitación y concientización

Todos los empleados deberán ser previamente notificados y capacitados sobre los procesos de respaldos de la información.

13.10. Política de registro de eventos

Título del documento	Política de registros de eventos
ID Documento	DP_011
Estado:	Vigente
Versión:	1.0

Historial de cambios			
Versión	Fecha	Descripción	Páginas
1.0	2019-11-25	Creación del documento	Todas

REV. 1	Nombre y Apellidos	Cargo	Fecha	Firma
Confeccionado	Katherine Merino	Maestrante	2019-11-25	
Aprobado	Miguel Huaraca	Gerente	2019-11-25	
Revisado	Miguel Huaraca	Gerente	2019-11-25	

MUNDOTRONIC al detectar cambios importantes en los sistemas considera necesario la creación de la política de registros de eventos.

Objetivo

Monitorizar los sucesos importantes detectados para luego poderlos clasificarlos, categorizarlos, identificar las posibles respuestas, revisiones y cierre para normalizar la operación de los servicios de MUNDOTRONIC.

Alcance

Esta política se aplica para detectar, clasificar y categorizar las acciones de control necesarias a implementar, para mantener la disponibilidad de los servicios de MUNDOTRONIC.

Política

MUNDOTRONIC se reserva el derecho de especificar las acciones para realizar el registro de eventos detectados en sus servicios.

Actividades

- Todo cambio realizado dentro del servicio debe ser gestionado y controlado.
- Todos los componentes tecnológicos pertenecientes a MUNDOTRONIC que traten datos personales deben ser monitoreados.
- Se debe realizar y administrar un listado de métricas a monitorear, las cuales deberán ser documentadas.
- Las herramientas de monitoreo de los equipos que compartan con los usuarios deberán ser comunicadas a los usuarios, clientes o abonados.
- Los monitoreos deberán ser gestionados mediante una herramienta aprobada por el gerente y el jefe técnico para poder gestionar cambios.
- Se debe elegir a un administrador de eventos, el cual debe analizar mensualmente los eventos reportados para gestionar. Se debe correlacionar y suprimir eventos que produzcan falsas alarmas.
- El administrador de eventos debe derivar los incidentes o cambios al comité de riesgos para crear planes de mejoras.
- Es responsabilidad del administrador de eventos asegurar que el proceso sea definido, documentado, mantenido y comunicado.
- Si existe reportes de análisis de eventos registrados mayores o iguales a 3 días se deberán remitir de manera semanal al comité de riesgos para crear acciones correctivas y de cierre de los eventos.

Derechos de MUNDOTRONIC

MUNDOTRONIC tiene el derecho a gestionar y administrar los eventos detectados en sus sistemas.

Seguridad

Todos los incidentes de seguridad deberán ser reportados al comité de riesgos.

Capacitación y concientización

Todos los empleados deberán ser previamente notificados y capacitados sobre la gestión de registros de eventos.

13.11. Políticas de instalación de software

Título del documento	Política de instalación de software
ID Documento	DP_012
Estado:	Vigente
Versión:	1.0

Historial de cambios			
Versión	Fecha	Descripción	Páginas
1.0	2019-11-25	Creación del documento	Todas

REV. 1	Nombre y Apellidos	Cargo	Fecha	Firma
Confeccionado	Katherine Merino	Maestrante	2019-11-25	
Aprobado	Miguel Huaraca	Gerente	2019-11-25	
Revisado	Miguel Huaraca	Gerente	2019-11-25	

MUNDOTRONIC utiliza diferentes tipos de software para la gestión de sus procesos, por lo que crea la política de instalación de software y evitar intrusión de código malicioso en sus equipos.

Objetivo

Establecer las acciones a tomar al momento de realizar las instalaciones de software en los equipos pertenecientes a MUNDOTRONIC.

Alcance

Esta política se aplica a todos los equipos que son propiedad de MUNDOTRONIC o equipos que sean utilizados como herramientas de trabajo dentro de la organización.

Política

MUNDOTRONIC se reserva el derecho de especificar las acciones a implementarse para garantizar una instalación segura del software.

Actividades

- Es responsabilidad del departamento técnico la instalación de las aplicaciones en cada uno de los equipos de MUNDOTRONIC.
- Los dueños de los activos no deben instalar ningún tipo de software.
- Todo software instado en los equipos debe poseer su respectiva licencia o ser validada por instalación por parte del comité de riesgos.
- Es responsabilidad del departamento técnico llevar un inventario de los softwares instalados en cada uno de los equipos.

- Se deberá realizar respaldos de la información contenida en el equipo en el caso que la instalación del software realice un cambio significativo en el equipo.

Derechos de MUNDOTRONIC

MUNDOTRONIC tiene el derecho a que el software que se instala en sus equipos o en los equipos del personal sean usados como herramientas de trabajo.

Seguridad

Todos los incidentes de seguridad deberán ser reportados al comité de riesgos.

Capacitación y concientización

Todos los empleados deberán ser previamente notificados y capacitados sobre los procesos de instalación de software.

13.12. Políticas de procedimientos de seguridad de las redes

Título del documento	Política de procedimientos de seguridad de las redes
ID Documento	DP_013
Estado:	Vigente
Versión:	1.0

Historial de cambios			
Versión	Fecha	Descripción	Páginas
1.0	2019-11-25	Creación del documento	Todas

REV. 1	**Nombre y Apellidos**	**Cargo**	**Fecha**	**Firma**
Confeccionado	Katherine Merino	Maestrante	2019-11-25	
Aprobado	Miguel Huaraca	Gerente	2019-11-25	
Revisado	Miguel Huaraca	Gerente	2019-11-25	

MUNDOTRONIC considerando su red corporativa y los datos que se procesan en esta, crea la política de procedimientos de seguridad de las redes.

Objetivo

Establecer las acciones a implementar para asegurar la red corporativa de MUNDOTRONIC.

Alcance

Esta política se aplica a todos los procedimientos y equipos que formen parte de la red corporativa de MUNDOTRONIC.

Política

MUNDOTRONIC se reserva el derecho de especificar las acciones a implementarse para asegurar la red corporativa.

Actividades

- El departamento técnico debe proporcionar los recursos necesarios para la prestación del servicio de internet como: implementación, administración y mantenimiento.
- El departamento técnico debe monitorear periódicamente los canales de comunicación para identificar y prevenir incidentes de seguridad.
- El departamento técnico debe realizar registros de accesos a los sistemas y los procedimientos de monitoreo.
- El departamento técnico debe establecer controles para evitar el ingreso de código malicioso.
- El departamento técnico debe segmentar las redes de acuerdo con el tipo de usuario.
- El departamento técnico debe crear perímetros de seguridad en la red.
- Se debe instalar protección en la red interna y externa.
- Se debe instalar protección en las redes inalámbricas.
- Cambiar periódicamente las contraseñas de los equipos y sistemas.

Derechos de MUNDOTRONIC

MUNDOTRONIC tiene el derecho establecer las acciones y responsables que aseguren su red.

Seguridad

Todos los incidentes de seguridad deberán ser reportados al comité de riesgos.

Capacitación y concientización

Todos los empleados deberán ser previamente notificados y capacitados sobre los procedimientos de aseguramiento de la red.

13.13. Política de transferencia de información.

Título del documento	Política de transferencia de información
ID Documento	DP_014
Estado:	Vigente
Versión:	1.0

Historial de cambios			
Versión	Fecha	Descripción	Páginas
1.0	2019-11-25	Creación del documento	Todas

REV. 1	Nombre y Apellidos	Cargo	Fecha	Firma
Confeccionado	Katherine Merino	Maestrante	2019-11-25	
Aprobado	Miguel Huaraca	Gerente	2019-11-25	
Revisado	Miguel Huaraca	Gerente	2019-11-25	

MUNDOTRONIC considerando la necesidad de la transferencia de información de la importancia de esta, crea la polítca de transferencia de información.

Objetivo

Establecer las acciones a tomar al momento de realizar la transferencia de información contenida dentro de la organización.

Alcance

Esta polítca se aplica a todo tipo de información identificada dentro de MUNDOTRONIC.

Polítca

MUNDOTRONIC se reserva el derecho de especificar los procedimientos a realizarse en la transferencia de información.

Actividades

- Es responsabilidad del departamento técnico establecer los procedimientos de transferencia de información.
- Es responsabilidad del departamento técnico establecer los medios y controles confiables con el fin de garantizar la confiabilidad e integridad de la información.
- El departamento técnico debe ofrecer los servicios o herramientas que permitan el intercambio o transferencia de la información.
- El departamento técnico debe establecer procedimientos de transferencia de información mediante correo electrónico.
- Está prohibido el intercambio de contenido de información que atente contra la integridad de personas y de la organización.

- Es responsabilidad del departamento técnico establecer un registro de la información transferida, de sus destinatarios y el motivo del traslado.

Derechos de MUNDOTRONIC

MUNDOTRONIC tiene el derecho de establecer el proceso de transferencia de la información y de sancionar si de acuerdo con las normativas legales vigentes se identifica trasferencias que ponga en riesgo la integridad de las personas o la organización.

Seguridad

Todos los incidentes de seguridad deberán ser reportados al comité de riesgos.

Capacitación y concientización

Todos los empleados deberán ser previamente notificados y capacitados sobre los procedimientos de trasferencia de información.

13.14. Políticas de procedimientos de protección de datos en ambientes de pruebas

Título del documento	Política de procedimientos de protección de datos en ambientes de prueba.
ID Documento	DP_015
Estado:	Vigente
Versión:	1.0

Historial de cambios			
Versión	Fecha	Descripción	Páginas
1.0	2019-11-25	Creación del documento	Todas

REV. 1	**Nombre y Apellidos**	**Cargo**	**Fecha**	**Firma**
Confeccionado	Katherine Merino	Maestrante	2019-11-25	
Aprobado	Miguel Huaraca	Gerente	2019-11-25	
Revisado	Miguel Huaraca	Gerente	2019-11-25	

MUNDOTRONIC considerando los ambientes de pruebas que crea para probar nuevos equipos o servicio en su red corporativa crea la política de procedimientos de protección de datos en ambientes de prueba.

Objetivo

Establecer las acciones a tomar al momento de realizar pruebas con equipos o sistemas nuevos dentro de la red corporativa de MUNDOTRONIC.

Alcance

Esta política se aplica a todos los procesos y equipos que traten información de carácter personal y sean usados en ambiente de pruebas.

Política

MUNDOTRONIC se reserva el derecho de especificar las acciones a implementarse en ambientes de prueba.

Actividades

- Es responsabilidad del departamento técnico no revelar la información confidencial contenida en los equipos y sistemas de MUNDOTRONIC.
- El departamento técnico deberá aplicar medidas de encriptación y no revelación de la información confidencial utilizados en ambientes de pruebas.
- Es responsabilidad del departamento técnico eliminar la información una vez concluidas los ambientes de pruebas.
- Cada vez que se realicen copias de la información, se deberá contar con un registro de seguimiento de estas.

Derechos de MUNDOTRONIC

MUNDOTRONIC tiene el derecho a utilizar información generada dentro de su empresa siempre y cuando cuente con un documento de autorización de los propietarios de la información.

Seguridad

Todos los incidentes de seguridad deberán ser reportados al comité de riesgos.

Capacitación y concientización

Todos los empleados deberán ser previamente notificados y capacitados sobre uso de información en ambiente de pruebas.

13.15. Políticas de privacidad y protección de datos personales

Título del documento	Política de privacidad y protección de datos personales
ID Documento	DP_016
Estado:	Vigente
Versión:	1.0

Historial de cambios			
Versión	Fecha	Descripción	Páginas
1.0	2019-11-25	Creación del documento	Todas

REV. 1	**Nombre y Apellidos**	**Cargo**	**Fecha**	**Firma**
Confeccionado	Katherine Merino	Maestrante	2019-11-25	
Aprobado	Miguel Huaraca	Gerente	2019-11-25	
Revisado	Miguel Huaraca	Gerente	2019-11-25	

MUNDOTRONIC considerando la importancia a la protección de los datos crea la política de privacidad y protección de datos personales

Objetivo

Establecer los procedimientos que garanticen la protección de datos personales tratados dentro de MUNDOTRONIC.

Alcance

Esta política se aplica a todos los procesos y equipos que traten información de carácter personal.

Política

MUNDOTRONIC se reserva el derecho de especificar las acciones a implementarse para la protección de datos personales.

Actividades

- Identificar los tipos de datos personales tratados.
- Categorizar los datos personales tratados.
- Notificar el uso que se realizará con los datos tratados.
- Notificar a los propietarios de los datos personales el cambio en la política de privacidad y protección de datos personales.
- El personal no puede divulgar los datos personales.
- Los datos solo pueden ser accedidos por terceros previa autorización del titular de los datos personales o por requerimiento de una orden judicial.
- Implementar protocolos de seguridad tanto lógicos como físicos para salvaguardar los datos personales.

Derechos de MUNDOTRONIC

MUNDOTRONIC reconoce los derechos de sus clientes, abonados y usuarios como titulares de los datos personales para accesos y rectificaciones de la información receptada por MUNDOTRONIC.

MUNDOTRONIC puede actualizar su política de privacidad y protección de datos personales.

MUNDOTRONIC puede sancionar a su personal si se divulga los datos personales.

Seguridad

Todos los incidentes de seguridad deberán ser reportados al comité de riesgos.

Capacitación y concientización

Todos los empleados deberán ser previamente notificados y capacitados sobre los procedimientos de protección de datos personales.

ANEXO C: MODELOS Y PLANTILLAS

- **Formato de Registro de Incidencias**

REGISTRO DE INCIDENCIA **Cerrada [**SI/NO**]**

Incidencia Nº: _____
Fecha notificación: _____
Ficheros afectados: _____
Tipo de incidencia: _____

DETALLE DE LA INCIDENCIA

Fecha y hora que se produjo la incidencia: _____
Personas que realizan la notificación: _____
Descripción detallada de la incidencia: _____

ANÁLISIS DE LA INCIDENCIA

Personas a quien se les notifica:
_____
Efectos que puede producir:
_____
Medidas correctoras y preventivas aplicadas:
_____

RECUPERACIÓN DE DATOS

Procedimientos efectuados para la recuperación de los datos:
_____

Persona encargada de la recuperación:
_____
Datos restaurados:
_____
Datos grabados manualmente en el proceso de recuperación:
_____

Autoriza recuperación: _____

- **Formato de Inventario de Soportes Electrónicos Removibles**

Nº Identificación / Nº Serie	Tipo de Soporte	Lugar de almacenamiento	Tipo de Información que contiene	Archivos de datos personales donde procede la información	Fecha de creación

- **Formato de Inventario de Equipos**

Nº Identificación / Nº Serie	Persona que recibe el ordenador portátil	Firma del Receptor	Firma del Responsable de Seguridad	Archivos de Datos personales autorizados	Fecha de asignación

- **Formato de Registro de entrada / salida de soportes y documentos**

REGISTRO DE ENTRADA / SALIDA DE SOPORTES	
Fecha de entrada / salida del soporte	

SOPORTE	
Identificación	
Tipo de Soporte	
Tipo de Información	
Archivos de donde proceden los datos	
Fecha de creación	

ORIGEN / DESTINO Y FINALIDAD	
Organización de Origen / Destino	
Emisor / Destinatario	
Finalidad	

FORMA DE ENVÍO	
Medio de envío	
Remitente	
Precauciones especiales para el transporte	

REGISTRO DE FIRMAS	
Responsable de la entrega	
Nombre / Cargo	
Responsable del archivo / Responsable de Seguridad que autoriza	
Observaciones	
Fecha y firma	

- **Registro de personas usuarias autorizadas con acceso a los archivos**

RESPONSABLE DE SEGURIDAD GLOBAL	
Nombre y apellidos	Cargo
RESPONSABLES DE SEGURIDAD	
Nombre y apellidos	Cargo
RESPONSABLES DE ARCHIVOS	
Nombre y apellidos	Cargo
RESPONSABLES SERVICIOS TÉCNICOS	
Nombre y apellidos	Cargo

PERSONAS USUARIAS CON ACCESO FÍSICO A ZONAS RESTRINGIDAS		
Nombre y apellidos	**Cargo**	**Zonas a las que tiene acceso**

- **Registro de personas usuarias autorizadas para tratamiento de datos fuera de las oficinas**

PERSONAS USUARIAS AUTORIZADAS	
Cargos	**Archivos tratados**

Gmail **Katherine Adriana Merino Villa <kata.mevi@gmail.com>**

TRADUCCIÓN-RESUMEN

DIANA CASANDRA PAREDES PERALTA <diana.paredes@espoch.edu.ec> 16 de septiembre de 2022, 08:53
Para: "kata.mevi@gmail.com" <kata.mevi@gmail.com>
CC: Centro de Idiomas <idiomas@espoch.edu.ec>

Estimada Katherine,

Sírvase encontrar adjunta la traducción del resumen solicitada.

Saludos cordiales,
Ing. Diana Paredes
DOCENTE-CENTRO DE IDIOMAS

From: Centro de Idiomas <idiomas@espoch.edu.ec>
Sent: 15 September 2022 09:53
To: DIANA CASANDRA PAREDES PERALTA <diana.paredes@espoch.edu.ec>
Subject: RV: TRADUCCIÓN-RESUMEN

Saludos cordiales,

Favor realizar la siguiente traducción y enviar al mail del estudiante con copia al mail: idiomas@espoch.edu.ec

Atentamente,

Centro de Idiomas
"Saber para ser"

De: Katherine Adriana Merino Villa <kata.mevi@gmail.com>
Enviado: martes, 6 de septiembre de 2022 16:29
Para: Centro de Idiomas <idiomas@espoch.edu.ec>
Asunto: TRADUCCIÓN-RESUMEN

[Texto citado oculto]

---

2 archivos adjuntos

RESUMEN_Katherine Merino.docx
15K

RESUMEN_Katherine Merino.pdf