Universidad Internacional de La Rioja
Escuela Superior de Ingeniería y Tecnología

Máster Universitario en Dirección y Gestión de Tecnologías de la Información

Metodología de Seguridad de la Información aplicando la Norma ISO/IEC 27002 y herramientas de Análisis de Riesgos para el Ministerio del Trabajo (Ibarra)

Trabajo fin de estudio presentado por:	MARIO ANDRÉS CEVALLOS MICHILENA
Tipo de trabajo:	
Director/a:	JESUS CLARET TREMPS
Fecha:	

Resumen

Toda organización que es consciente del valor de la información para la consecución de sus propósitos y metas, está obligada a consolidar sus procesos, optimizar sus recursos, apoyarse de la tecnología, y mantener un control de los riesgos originados por errores o malas prácticas de las personas, con el fin de mantener los niveles de disponibilidad, integridad, y confidencialidad de sus datos. Sin embargo, este escenario no es común, y gran parte de las altas gerencias o autoridades, consideran de forma errada a la gestión de la seguridad de la información, como un tópico secundario, ajeno a las necesidades propias de la organización y de su personal, especialmente en las tareas vinculadas a su formación y concientización.

De esta manera, el presente estudio se enfoca precisamente en adoptar medidas orientadas a la gestión de las vulnerabilidades asociadas al recurso humano del Ministerio del Trabajo (Ibarra), mediante la declaración y difusión de un conjunto de directrices recogidas en un escrito formal de Políticas de Seguridad, destinadas a los servidores y terceros, vinculados con el tratamiento de su información, dentro del marco normativo de la ISO/IEC 27002. Además, la propuesta se encuentra sustentada y apoyada en un proceso previo de estimación del riesgo mediante la aplicación de la Metodología de origen español MAGERIT v3, con la intención de evaluar la relación existente entre sus recursos de información y su nivel de sensibilidad, frente a las distintas amenazas que tienen la capacidad de afectarlos.

En conclusión, el presente estudio permitió diagnosticar sistemática y metódicamente el estado de seguridad de la organización, se pudo definir acciones organizativas de control para su personal, con el fin de asegurar la correcta manipulación de su información y demás recursos relacionados, y finalmente, se consiguió concientizar transversalmente en cada nivel de gestión, respecto a los lineamientos de seguridad de la información que prescribe esta Cartera de Estado.

Palabras clave: Políticas de seguridad de la información, Norma ISO/IEC 27002, Análisis de riesgos, Metodología MAGERIT v3, Ministerio del Trabajo.

Abstract

Any organization that is aware of the value of information for the achievement of its purposes and goals, is obliged to consolidate its processes, optimize its resources, rely on technology, and maintain control of the risks caused by errors or bad practices of the people, in order to maintain the levels of availability, integrity, and confidentiality of their data. However, this scenario is not common, and a large part of the top management or authorities, mistakenly consider information security management as a secondary topic, unrelated to the organization and staff needs, especially in the tasks related to their training and awareness.

In this way, this study focuses precisely on adopting measures aimed at treating vulnerabilities associated with human resources at Ministerio del Trabajo (Ibarra), through the declaration and dissemination of a set of guidelines contained in a formal document of Policies of Security, intended for employees and third parties, linked to the processing of their information based on ISO/IEC 27002 Standard. In addition, the project is supported by a prior process of risk estimation applying the MAGERIT v3 Methodology, with the intention of evaluating the relationship between its information resources and their level of sensitivity, in the face of the different threats that have the capacity to affect them.

In conclusion, this study made it possible to systematically and methodically diagnose the organization's security status, it was possible to define organizational control actions for its employees, in order to ensure the correct handling of their information and other related resources, and finally, managed to raise awareness globally at each level of management, regarding the information security guidelines established by this institution.

Keywords: Information security policies, ISO/IEC 27002 Standard, Risk analysis, MAGERIT v3 Methodology, Ministerio del Trabajo.

Índice de contenidos

Índice de Figuras

Índice de Tablas

1. Introducción

Hoy en día, toda entidad que requiera alcanzar niveles adecuados de rendimiento, que le permita competir a la par con sus similares, necesita prioritariamente, explotar de forma segura su información, la cual ha ido incrementado en cuanto a volumen, importancia y por ende en vulnerabilidad. Adicionalmente, la evolución tecnológica y las nuevas capacidades de interconexión, han generado nuevas oportunidades de negocio y mejoras en su productividad, pero también han traído consigo grandes preocupaciones a los profesionales de TI, en cuanto al resguardo de los sistemas de información que gestionan. Pese a este panorama, gran parte de las organizaciones, no toman conciencia del riesgo y las que, si lo hacen, deciden invertir grandes cantidades de dinero en herramientas netamente tecnológicas, dejando de lado el factor humano.

Dentro de este contexto, el Ministerio del Trabajo, como organismo de regulación de las relaciones laborales ecuatorianas, procesa grandes volúmenes de información relevante, que requiere ser protegida de las distintas amenazas que ponen en riesgo su disponibilidad, integridad y confidencialidad. Sin embargo, se ha identificado que sus medidas de protección, se focalizan únicamente en la implementación de soluciones técnicas tradicionales, que por sí mismas, pueden resultar poco efectivas, en un entorno, donde predomina el desconocimiento, falta de compromiso e involucramiento de sus funcionarios, en cuestiones relacionadas a la seguridad de la información. En virtud de ésta problemática, el presente trabajo plantea definir lineamientos que regulen su comportamiento profesional y personal, en relación al uso de la información (física o electrónica) y de los equipos tecnológicos que la contienen. De esta manera, se recogerá un conjunto de Políticas de Seguridad de la Información, basadas en los Controles y Objetivos de la Normativa ISO/IEC 27002, con el propósito de enfrentar eficientemente las probables amenazas identificadas en un proceso previo de diagnóstico del estado del riesgo. La debida aplicación y cumplimiento de este documento formal, aportará enormemente al ordenamiento de sus procesos críticos, de las tareas, roles y responsabilidades de sus actores, la protección de sus activos sensibles y la consolidación de una cultura de seguridad de la información organizacional.

1.1.Justificación del Trabajo

BBVA (2020) menciona que la actual pandemia ha sido aprovechada por ciberdelincuentes para desplegar acciones mal intencionadas, a través de sitios web fraudulentos (phishing) y la utilización de vectores de propagación de malware más comunes como emails, redes sociales o mensajería instantánea. Adicionalmente, señala como agravante, la actual necesidad de las organizaciones por emplear mecanismos de conexión y comunicación remota para teletrabajo, lo cual genera un aumento del grado de exposición de sus sistemas de información. Por su parte, la empresa Consulting Informático (2019) afirma que es fundamental instaurar una cultura organizacional, a través de lineamientos de seguridad establecidos, que regulen el comportamiento del personal en temas de seguridad, debido a que son ellos quienes utilizan los recursos e información.

El Ministerio del Trabajo consciente de este escenario, y en respuesta a una serie de eventos que denotan el riesgo al que se enfrenta su información sensible, entre los que destacan: la penetración incesante de correos sospechosos, la generación de múltiples incidencias dentro de su sistema de gestión de tickets, derivadas de una incorrecta manipulación de sus activos, la pérdida o alteración no intencionada de información institucional, e incluso, la existencia de casos de robo de equipamiento, se ha propuesto establecer medidas administrativas para gestionar los riesgos asociados a las personas, mediante la definición de Políticas de Seguridad de la Información, para el alineamiento de sus tareas y el establecimiento de un compromiso a nivel institucional, en la cual sus funcionarios se apropien y sean conscientes del valor de la información que manejan. Esta tarea estará fundamentada y respaldada en una evaluación preliminar del riesgo de TI, la cual permita enfocar los esfuerzos en los puntos críticos que merecen ser atendidos de manera prioritaria, con el objetivo de optimizar recursos, eliminar desperdicios y afinar las distintas actividades.

De esta manera, se obtendrá un sistema de protección integral, que utilice mecanismos de protección técnicos, complementados por medidas organizativas, que fortalezcan el recurso humano, considerado el elemento más sensible de la cadena de seguridad.

1.2.Problema

El Ministerio del Trabajo como ente regulador del ámbito laboral, procesa diariamente información de carácter confidencial, plasmada en documentos como: contratos, finiquitos,

registros de pagos de multas, registros de denuncias en instituciones públicas, entre otros. Sin embargo, su personal encargado no gestiona debidamente estos datos críticos, a causa de su desconocimiento en temas de seguridad, falta de concientización y compromiso o en muchos casos debido a que sus administradores de servicios, subestiman o desestiman el riesgo de ser atacados.

Este contexto se agudiza ante la ausencia de Políticas institucionales, que promuevan la adecuada manipulación y gestión de sus datos, así como de los recursos de hardware y software que los almacenan y procesan. Asimismo, no se encuentran claramente delimitadas las competencias del personal, respecto a las tareas de gestión de la seguridad de la información, y se imputa toda la responsabilidad a su Departamento de TI, que, por su parte, carece de lineamientos que guíen sus labores de administración, mantenimiento y resguardo de los recursos tecnológicos.

Esta situación, también ha dado lugar a la arbitrariedad e improvisación de las decisiones de sus administradores de red, que, sin un sustento y conocimiento previo, tanto de lo que merece ser protegido, como de los márgenes de riesgo presentes en el sistema de información, se han limitado a la implementación de mecanismos técnicos de uso común, como su antivirus corporativo y filtrado de contenidos, mismos que pueden ser fácilmente burlados, mientras no se atienda y priorice el componente humano.

Sin duda, este escenario puede originar diversos eventos que comprometan la integridad y confidencialidad de sus datos, provoquen la indisponibilidad de sus servicios, y por ende generen malestar y desconfianza en sus usuarios y ciudadanía en general. De esta manera, se ha propuesto desarrollar Políticas destinadas a modelar las tareas y responsabilidades de sus funcionarios, con el fin de garantizar un comportamiento seguro, que minimice los niveles de riesgo identificados en un proceso de análisis previo, que resalte la situación actual de vulnerabilidad.

1.3.Planteamiento de la Solución

El proyecto propuesto, iniciará con una breve exposición de los conceptos iniciales, relacionados a la gestión de la seguridad de la Información, así como de los procesos de Análisis y Gestión de Riesgos dentro de los ámbitos organizacionales, señalando su importancia y aplicación en proyectos similares. Para complementar la literatura, se realizará

un breve análisis de la Metodología y Norma seleccionadas para el presente proyecto, puntualizando las razones por las que se eligió tanto MAGERIT versión 3 como ISO/IEC 27002.

En referencia a la solución propiamente dicha, la misma tendrá como punto de partida la ejecución de un proceso de Análisis de Riesgos de TI dentro de la institución, aplicando MAGERIT v3. Para lo cual, se realizará el levantamiento de los principales activos de información pertenecientes al Ministerio del Trabajo con sede en la ciudad de Ibarra, los cuales serán tipificados y valorados en varias dimensiones, conforme lo señala la Metodología seleccionada. Sus catálogos y técnicas, permitirán también, identificar y valorar las amenazas que pueden afectarlos, estimando sus niveles de impacto y riesgo asociados. Los entregables de este proceso previo, servirán de referencia para una adecuada selección de los Controles que propone la Normativa ISO/IEC 27002, a fin de estructurar un documento de Políticas, que moderen las tareas y responsabilidades de sus funcionarios, respecto al uso aceptable de los recursos de información institucionales. Finalmente, se propone socializar estos lineamientos, a través de medios electrónicos, como email institucional y Sistema de Gestión Documental, para su conocimiento y estricto cumplimiento.

La presente Metodología, integra las propiedades y capacidades de dos guías internacionales y reconocidas, como MAGERIT v3 e ISO/IEC 27002, permitiendo evaluar los riesgos desde diversas perspectivas, mediante técnicas de fácil implementación y con una guía completa de controles que se pueden adaptarse a la necesidad y situación de seguridad de cualquier entorno organizacional. La presente propuesta, se focaliza en reforzar las debilidades del elemento humano, creando medidas de carácter administrativo, para establecer responsabilidades, comportamientos deseados y la comprensión de la importancia del riesgo dentro de la organización, que, a diferencia de otros proyectos, propone un método estructurado que se sostiene en un análisis previo de la situación real de la entidad en términos de seguridad, que permita focalizar adecuadamente los esfuerzos y evitar desperdicios de recursos de forma innecesaria.

1.4.Estructura de la Memoria

CAPÍTULO 2: Contexto y Estado del Arte

Se recopila la literatura extraída de fuentes primarias y secundarias, para sentar las bases teóricas del presente proyecto, dirigida al conocimiento y revisión de los conceptos relacionados a la gestión de la seguridad de la información, y de los procesos de análisis y gestión del riesgo de TI, en el marco de la Metodología MAGERIT V3 y la Norma ISO/IEC 27002. Adicionalmente, se recoge las principales resoluciones de varios investigadores, extraídas de proyectos similares al propuesto, con el fin de comprender de mejor manera la problemática que será abordada en éste trabajo de investigación.

CAPÍTULO 3: Objetivos y Metodología de Trabajo

Se da a conocer los objetivos (general y específicos) que persigue el trabajo propuesto, y se presenta una breve explicación de las tareas que serán desarrolladas para su consecución. Además, se define la orientación que tendrá la investigación y se describen las técnicas e instrumentos a emplearse, dentro de las etapas de ejecución del proyecto.

CAPÍTULO 4: Desarrollo del Proyecto

En su inicio, se expone el contexto de la institución donde será aplicado el proyecto, para la comprensión del entorno que será analizado y evaluado en las etapas posteriores. A continuación, se detalla la parte medular del trabajo investigativo, en la cual se explica las tareas de implementación de la Metodología de Análisis del Riesgo MAGERIT v3 sobre los activos de información del Ministerio del Trabajo (Ibarra), y se presenta la propuesta de las Políticas de Seguridad de la información basadas en los Controles de la Normativa ISO/IEC 27002, con sus respectivas percepciones y resultados obtenidos.

CAPÍTULO 5: Conclusiones y Trabajo Futuro

Se citan las impresiones y resultados más relevantes, obtenidos en el transcurso del desarrollo del proyecto, demostrando que la problemática ha sido tratada, conforme el cumplimiento de los objetivos planteados inicialmente. Por último, se presenta algunas propuestas adicionales que podrían desarrollarse en futuras investigaciones, con el fin de complementar el alcance de la solución propuesta.

2. Contexto y Estado del Arte

2.1.Antecedentes

En este apartado, se presentará una visión global de los principales conceptos referentes a la gestión de la seguridad de la información y su importancia dentro de las organizaciones que, sin excepciones, deben enfrentarse a niveles de riesgo de TI, cada vez más significativos, los cuales requieren ser evaluados y tratados adecuadamente. De esta manera, se describirá la Metodología MAGERIT versión 3, detallando sus principales características, y resaltando los criterios que fueron tomados en cuenta para su selección, basados en la comparación con Metodologías similares. Adicionalmente, se expondrá los principales estándares de la Serie ISO para la seguridad de la información, haciendo énfasis en la normativa ISO/IEC 27002:2013, misma que será aplicada en el presente proyecto.

2.1.1. Gestión de la Seguridad de la Información

La información es un componente fundamental para la ejecución de las tareas diarias de cualquier entidad, y su correcta explotación, le permitirá tomar decisiones, alcanzar sus objetivos de negocio, y cumplir las expectativas de sus clientes o satisfacer las necesidades generales de la sociedad, en el caso de los organismos de la Administración Pública. De esta manera, se hace imperativa la necesidad de resguardarla de una manera multidimensional, es decir considerando los siguientes criterios, según Fronteras Security (2020):

- La disponibilidad: significa que la información se encuentra accesible para usuarios autorizados en cualquier momento.
- La integridad: asegura que la información no ha sido alterada o modificada sin autorización, ya sea de manera intencional o no.
- La confidencialidad: garantiza que el acceso a la información sea únicamente para personas autorizadas, asegurando que no sea divulgada de manera accidental o intencionada.
- La autenticidad: implica que el origen de la información sea confiable y fidedigno.
- La trazabilidad: asegura que se pueda rastrear el origen, camino y destino de la información.

Por su parte, Schwartz (2020) menciona que la información se genera y procesa en entornos que se digitalizan de manera creciente, lo cual la expone de manera consecuente, a un sinnúmero de amenazas cibernéticas, que se requiere sean abordadas de una manera holística, es decir, aplicando medidas de carácter técnico, administrativo, legal, de capacitación y concientización.

Estas apreciaciones, que buscan prioritariamente asegurar los datos, sin dejar de lado los procesos, la tecnología y sobre todo las personas, mediante la aplicación de medidas con distintas perspectivas, describen el nuevo concepto de Gestión de la Seguridad de la información.

Su aplicación demandará de un proceso de análisis previo del estado de seguridad, que defina los recursos que deberán ser protegidos, las amenazas que enfrentan, y los mecanismos de protección que buscan mitigar sus niveles de impacto y riesgo.

2.1.2. Análisis de Riesgos de TI

De acuerdo a AMBIT (2020) la ejecución de un debido proceso de análisis de riesgos dentro de una organización, le garantizará las siguientes ventajas o beneficios:

- Obtener una visión real y precisa de sus activos de información, que le permita ubicar los recursos que deben ser protegidos.
- Conocer los riesgos y priorizar aquellos que tengan mayor probabilidad de ocurrencia, para focalizar los esfuerzos en mitigarlos.
- Identificar las amenazas y el impacto que provocarían en la organización, para reducir los tiempos de actuación y respuesta, ante posibles incidentes de seguridad.
- Facilitar la toma de decisiones, respecto a la selección de la alternativa más idónea, para contrarrestar las amenazas y riesgos identificados.
- Evaluar su estado actual de seguridad, para implementar mejoras o reforzar aspectos débiles en cuanto a sus medidas de protección.
- Contar con una base de conocimiento, que sustente y facilite el desarrollo de planes relacionados a la continuidad del negocio, que le permitan recuperarse de incidentes importantes.
- Crear una cultura organizacional de prevención, que involucre y comprometa a todos los interesados.

Adicionalmente, Arteaga (2018) asevera que todo proceso de Análisis de Riesgos de TI, tiene como denominador común, la ejecución de las siguientes actividades:

- Identificar los activos e información sensible, con el fin de asociarlos con los niveles de riesgo y las dimensiones: disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.
- Evaluar el entorno en el que se desenvuelven los activos, para reconocer las amenazas a las que se enfrentan, y el potencial daño que pueden provocar en ellos.
- Diseñar escenarios en los cuales se pueda vincular el impacto que genera una amenaza, respecto a su probable ocurrencia, para encontrar el nivel de riesgo asociado.
- Elaborar estrategias de tratamiento del riesgo, basadas en estándares y buenas prácticas.

Por esta razón, varios organismos gestores de seguridad de la información de distintas latitudes, han creado una serie de Metodologías enfocadas precisamente, en ofrecer las herramientas, técnicas y procedimientos, para facilitar la ejecución de estas tareas, de modo que se desarrollen de manera sistemática y estandarizada. De esta manera, en la sección siguiente se expondrá los puntos fundamentales de MAGERIT v3, como Metodología escogida para el presente proyecto, su relación con guías similares y los criterios que fueron considerados para su adopción.

2.1.2.1. MAGERIT v3 (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información)

Esta guía creada por el Consejo Superior de Administración Electrónica de origen español (actualmente Comisión de Estrategia TIC), presenta en su última actualización de octubre de 2012 (versión 3), un conjunto de pasos ordenados para conocer y estimar el riesgo al que están sometidos los componentes de un sistema de información corporativo, mismos que son imprescindibles para poder gestionarlos, sin dar lugar a la improvisación y arbitrariedad del analista (Ministerio de Hacienda y Administraciones Públicas, 2012).

2.1.2.1.1. Objetivos

De acuerdo al Portal de Administración Electrónica (2012), entre los principales objetivos que persigue MAGERIT v3, se encuentran:

•Generar conciencia en los responsables de administrar los sistemas de información, sobre la existencia del riesgo y la creciente necesidad por eliminarlos o minimizarlos.

•Dar a conocer un proceso metódico para analizar los riesgos de una organización.

•Facilitar la planificación de medidas que ayuden a mantener los riesgos bajo control.

•Establecer un punto de partida, para facilitar la ejecución de futuros planes de certificación y auditoría dentro de la organización.

2.1.2.1.2. Estructura de la documentación

El Portal de Administración Electrónica (2012), describe las guías o libros que componen la documentación de MAGERIT v3, y se sintetizan en la Tabla siguiente:

Tabla 1. Resumen de los Libros de MAGERIT v3

Libro I – Método	▪ Describe la terminología y conceptos, enmarcados dentro de un proceso de análisis y gestión del riesgo, buscando una uniformidad de criterios. ▪ Determina cuáles serán las tareas o pasos a seguir, para implantar un proceso formal de análisis del riesgo. ▪ Cita casos prácticos y consejos, que pueden servir de guía para la implementación de la Metodología.
Libro II – Catálogo de elementos	▪ Ofrece modelos estándar para referenciar con mayor rapidez y facilidad, los tipos de activos, amenazas y salvaguardas dentro del entorno de TI. ▪ Detalla las escalas y criterios en las que serán valorados los activos de información, y los términos en los que serán dimensionados. ▪ Describe los criterios en los que serán evaluadas las amenazas, en relación a su nivel de daño y probabilidad de ocurrencia. ▪ Expone los criterios en los que serán evaluadas las salvaguardas, en relación a su nivel de efectividad.
Libro III – Guía de Técnicas	▪ Detalla las diversas técnicas y herramientas necesarias para la estimación de los niveles de impacto y riesgo, asociados a los activos y amenazas previamente identificadas. La Metodología propone las siguientes: Análisis mediante Tablas, Análisis Logarítmico, Árboles de ataque, valoración Delphi, entre otras. ▪ Cita algunos de los métodos que pueden ser empleados, para la recolección y representación de los datos, que serán analizados en el proceso. Por ejemplo: reuniones de trabajo, entrevistas, técnicas gráficas, etc.

Adaptación de PAE, 2012

2.1.2.1.3. Tareas de MAGERIT versión 3

De acuerdo al Libro I denominado "Método" (Ministerio de Hacienda y Administraciones Públicas, 2012), la implementación de MAGERIT v3 se fundamenta en el cumplimiento de una serie de tareas y subtareas de manera secuencial, mismas que se sintetizan a continuación:

Tabla 2.Tareas de MAGERIT v3

Tarea	Subtarea	Descripción
1.Caracterización de los activos	1.1Identificación 1.2Tipificación 1.3 Valoración *Informe: Modelo de valor*	▪ Son los bienes tangibles o intangibles de valor para una organización, mismos que son susceptibles a ser atacados. ▪ Tipos: datos, servicios, aplicaciones, equipos de cómputo, recursos de redes, recursos humanos, instalaciones, entre otros. ▪ Su valoración será en base a las consecuencias que supondrían una violación a su disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.
2.Caracterización de las amenazas	2.1Identificación 2.2Valoración *Informe: Mapa de riesgos*	▪ Son posibles eventos que, en caso de materializarse, provocarán un determinado nivel de daño o degradación a un activo. ▪ Su valoración conlleva la estimación (teórica) de este nivel de degradación y su frecuencia (probable) de ocurrencia.
3.Caracterización de las salvaguardas	3.1Identificación 3.2Valoración *Informe: Evaluación de salvaguardas*	▪ Representan las contramedidas, con los que cuenta la organización, para hacer frente a dichas amenazas. ▪ Pueden ser del tipo: limitante (limitan daño) o preventiva (reducen la ocurrencia). ▪ Su valoración será en base a su nivel de efectividad.
4.Estimación del estado de riesgo	4.1Estimación del Impacto 4.1Estimación del Riesgo *Informe: Estado del riesgo*	▪ El impacto refleja el grado de afectación causado por una amenaza sobre un activo, relacionándolo con su valor. ▪ El riesgo relaciona el impacto causado por una amenaza y su probable ocurrencia (frecuencia). ▪ En un inicio, la estimación del riesgo, se lo hará sin tomar en cuenta las salvaguardas con las que cuenta la organización (riesgo intrínseco). ▪ Posteriormente se evaluará considerando el efecto de las salvaguardas existentes, y el valor resultante se denominará riesgo residual o efectivo.

Adaptación de PAE, 2012

En concordancia con el Libro I: "Método" (Ministerio de Hacienda y Administraciones Públicas, 2012), la Figura 1 resume y correlaciona los conceptos y criterios expuestos anteriormente:

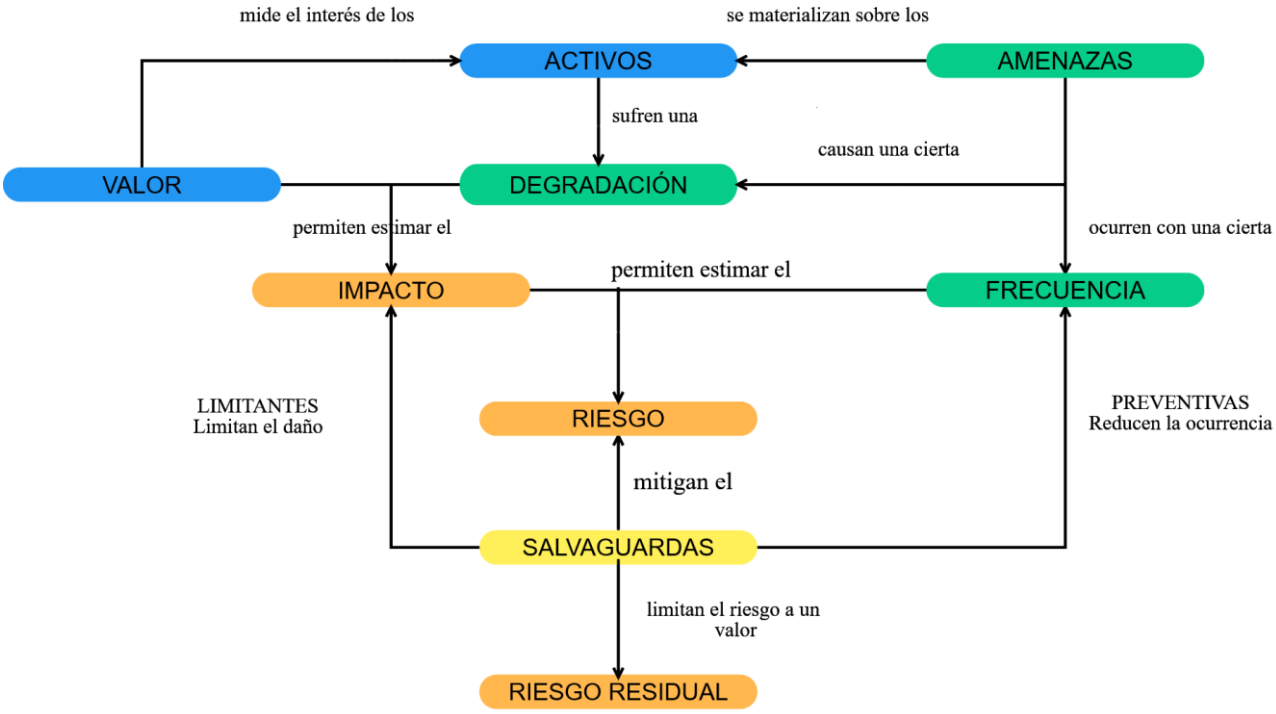

Figura 1.Resumen de la Metodología. (Adaptación del Libro I: "Método"-MAGERIT v3)

2.1.2.2. Comparativa con otras Metodologías de Análisis y Gestión del Riesgo

La Tabla siguiente, cita las principales Metodologías de Análisis del Riesgo de TI, y recoge los criterios clave que fueron cotejados para la elección de la mejor propuesta.

Tabla 3.Comparativa de Metodologías de Análisis y Gestión del Riesgo

	MAGERIT	OCTAVE	MEHARI	CRAMM
Siglas	Metodología de Análisis y Gestión de Riesgos de IT	Operationally Critical Threat, Asset, and Vulnerability Evaluation	Methode Harmonisée d'Analyse de Risques	CCTARisk Analysis and Management Method)
Elaborado por	Consejo Superior de Administración Electrónica.	Universidad Carnegie Mellon	CLUSIF (Club Francés de la Seguridad de la Información)	Agencia Central de Cómputo y Telecomunicaciones
País	España	Estados Unidos	Francia	Reino unido
Idioma	Español e inglés	inglés	Francés e inglés	inglés
Año revisión	2013	2011	2010	2005
Evaluación	cualitativa y cuantitativa	cualitativa	cualitativa y cuantitativa.	cualitativa
Dimensiones	Disponibilidad-Confidencialidad-Integridad-Autenticidad-Trazabilidad	Disponibilidad-Confidencialidad-Integridad	Disponibilidad-Confidencialidad-Integridad	Disponibilidad-Confidencialidad-Integridad
Herramientas	Tres libros: “Método”, "Catálogo de Elementos" y "Guía de Técnicas".	Guías, hojas de trabajo, y cuestionarios	Manuales y guías para identificar los activos y amenazas.	Base de datos con tipos de activos y amenazas, tipos de impacto y medidas de seguridad.
Fases	1.Caracterización de los activos: valoración, dimensionamiento. 2.Caracterización de las amenazas: relación con activos, valoración (degradación y frecuencia). 3.Caracterización de las salvaguardas: tipología, valoración (nivel eficacia). 4.Estimación del estado de riesgo: impacto y riesgo (intrínseco-residual).	1.Construcción de perfiles activo-amenaza, identificación de contramedidas actuales. 2.Análisis de vulnerabilidades en la infraestructura. 3.Definición de riesgos prioritarios y sus correspondientes planes de mitigación.	1.Fase preparatoria: evaluación del contexto técnico y estructural de la organización. 2.Fase operacional: análisis de activos, evaluación la calidad de los servicios de seguridad y evaluación del riesgo. 3.Fase de tratamiento: priorización del riesgo, selección de medidas e indicadores.	1.Evaluación de los activos de hardware y software. 1.1 Valoración de los datos según su impacto en el negocio. 2.Evaluación de las amenazas y vulnerabilidades. 2.1 Combinar las valoraciones de amenazas y vulnerabilidades para calcular la medida de los riesgos. 3.Selección de contramedidas.
Ámbitos de aplicación	Instituciones públicas, entidades privadas, PYMES.	PYMES	Instituciones públicas, entidades privadas, PYMES.	Instituciones públicas, entidades privadas.
Ventajas	▪ Acceso público.	▪ Acceso público.	▪ Acceso público.	▪ Posee una amplia base de conocimientos con más de 4000

	▪ Promueve la sensibilización a los responsables, sobre la existencia del riesgo. ▪ Analiza los activos en varias dimensiones. ▪ Está bien documentada en cuanto a tipos de activos de información y amenazas. ▪ Permite un análisis completo cualitativo y cuantitativo. ▪ Ofrece diversas técnicas para el cálculo del riesgo. ▪ Empleada en un sinnúmero de organizaciones españolas. ▪ Su versión original se encuentra en español. ▪ Su última revisión es la más reciente, respecto a la de sus similares.	▪ Compromete a todos los actores de la organización. ▪ Crea un ambiente colaborativo. ▪ Involucra los procesos y aspectos organizacionales como elementos del modelo. ▪ Se adapta al tamaño de la organización, ofreciendo una versión para cada caso. ▪ Analiza las vulnerabilidades y las relaciona con las amenazas.	▪ Análisis de riesgos cuantitativa en base a fórmulas. ▪ Permite identificar vulnerabilidades mediante auditorías.	medidas de seguridad, 400 tipos de activos, 38 tipos de amenazas y 25 tipos de impacto.
Desventajas	▪ No incluye los procesos, vulnerabilidades y aspectos organizacionales como elementos del modelo.	▪ Dimensionamiento limitado. ▪ La Fase 2 puede requerir subcontratación de terceros. ▪ Presenta un exagerado número de anexos. ▪ No explica claramente la definición de los activos de información.	▪ Dimensionamiento limitado. ▪ Se centra específicamente en mostrar las debilidades de un sistema de información. ▪ Complicaciones con su traducción. ▪ Poca o mediana cantidad de documentación. ▪ A pesar de tener actualizaciones, aún conserva un modelo tradicional.	▪ Dimensionamiento limitado. ▪ Su uso se enfoca en empresas grandes. ▪ Requiere amplios conocimientos técnicos. ▪ Requiere traducción. ▪ Requiere Licencia.

Adaptación de Santoja, 2019

2.1.2.3. Justificación de la Metodología de Análisis de Riesgo seleccionada

A partir del análisis de los ítems citados en la Tabla anterior, es posible deducir que la Metodología MAGERIT presenta varios puntos a favor, en relación a guías similares, entre los cuales se encuentran:

- Añade la autenticidad y trazabilidad, como dimensiones para el análisis de los activos, que se suman a las ya conocidas: disponibilidad, integridad, y confidencialidad.
- Posee un extenso catálogo de activos de información y amenazas, lo que reduce la complejidad y tiempos de ejecución, de las tareas de identificación, tipificación y dimensionamiento.
- Se puede acceder fácil y libremente a su documentación, no requiere licenciamiento y existen numerosos proyectos que muestran su implementación.
- Se puede optar por métodos tanto cualitativos como cuantitativos para estimar el riesgo.
- Ofrece un libro completo, que recopila varias técnicas y herramientas aplicables a un proceso de identificación y estimación del riesgo (Libro III: Guía de Técnicas).
- Adaptable a cualquier ámbito organizacional, de forma independiente al sector que aplica, tamaño o número de recursos tanto físicos como humanos, con los que cuenta.
- Su versión original es en español, por lo que se evita errores de traducción y ambigüedades en la interpretación de sus términos.
- Su última revisión, es la más actual en relación a las demás metodologías.

En base a estas consideraciones, se ha escogido MAGERIT versión 3, como guía para estimar el riesgo en los activos de información, pertenecientes al Ministerio del Trabajo con sede en la ciudad de Ibarra.

2.1.3. Gestión del Riesgo de TI

Una vez que los responsables e involucrados son conscientes de los riesgos y sus probables consecuencias, se encuentran obligados a dedicar sus esfuerzos y recursos, para controlarlos

y monitorearlos periódicamente, con el fin de mantenerlos bajo los límites consensuados con la organización, es decir, llevando a cabo un proceso formal de gestión del riesgo, que ha de ser correctamente estructurado, siguiendo un proceso metódico y sujeto a una evaluación continua (INCIBE, 2020).

Siguiendo esta premisa, la ejecución de un proceso de Gestión de riesgos correctamente constituido, demanda la adopción de directrices o buenas prácticas, como las planteadas por la serie ISO 27000, en el caso de requerirse una visión más profunda, en la estimación y tratamiento del riesgo, ligado a la seguridad de la información (27001Academy, 2018).

2.1.3.1. Serie ISO 27000

De acuerdo a MinTel (2020), una adecuada Gestión del riesgo de TI, requiere la implantación de un sistema basado en los requerimientos de la organización en términos de seguridad de la información, que permita establecer controles para enfrentar los posibles incidentes de manera anticipada, bajo un proceso debidamente comunicado y monitoreado, a lo largo de todas las tapas que transitan sus datos. Precisamente, este Sistema de Gestión de Seguridad de la Información (SGSI), es especificado por la Serie ISO 27000, a través de un conjunto de estándares, los cuales son brevemente descritos en la siguiente tabla:

Tabla 4. Principales Normativas de la Serie ISO 27000

Norma ISO/IEC	Descripción
27000	Expone de forma general el alcance y propósito de las normativas que conforman la serie 27000. Además, aporta con una breve introducción a los conceptos relacionados con un Sistema de Gestión de Seguridad de la Información (SGSI).
27001	Recopila los requisitos para poner en marcha un SGSI. Su Anexo A incorpora 114 controles de seguridad, adaptables a las organizaciones (no son todos obligatorios). Es certificable.
27002	Expone un conjunto de directrices y buenas prácticas que pretenden explicar y apoyar la implementación de los controles del Anexo A de ISO/IEC 27001.
27003	Proporciona una serie de directrices que orientan la planificación y ejecución de un SGSI, según lo estipulado por la Norma ISO/IEC 27001.
27004	Provee una guía para la implementación de métricas que estimen el rendimiento y resultados de un SGSI.
27005	Establece el conjunto de tareas que se necesitan ejecutar, para una adecuada gestión de riesgos de TI, desde su análisis, evaluación y posterior tratamiento. Describe el proceso que debe cumplir una metodología de análisis del riesgo.
27006	Recoge los requisitos que acreditan a una entidad auditora y certificadora de SGSI.

27007	Es una guía para ejecutar planes de auditoría, que verifiquen el cumplimiento de la Norma ISO 27001. Orienta las tareas de los organismos de certificación acreditados y equipos de auditores internos o externos.
27008	Es una guía para la ejecución de programas de evaluación y revisión de los controles implementados, de acuerdo a la ISO 27001.
27009	Complementa la ISO 27001, en cuanto a la inclusión de requisitos y nuevos controles, aplicables a sectores específicos como: finanzas, transporte, salud, proyectos de infraestructura, telecomunicaciones, entre otros.
27010	Especifica lineamientos para el intercambio seguro de información entre las distintas organizaciones, que buscan conformar un sistema de gestión comunitario.

Adaptación de INTECO, 2020

2.1.3.2. Norma ISO/IEC 27002

Tras la revisión de la literatura, se ha podido constatar una serie de criterios que intentan identificar y describir esta Norma, sin embargo, ISO Tools (2019) la refiere de manera concisa y clara, como un documento guía, en cuyo contenido se exponen un conjunto de recomendaciones para gestionar adecuadamente la seguridad de la información en una organización, a través de la selección y posterior implantación de los controles que recoge la ISO/IEC 27001, en su Anexo A. En otras palabras, señalará lo que debe realizarse en la práctica, para poder cumplir con los requerimientos que exige la ISO 27001, de acuerdo al escenario de riesgos encontrado.

2.1.3.2.1. Objetivos

De acuerdo a OSTEC (2020) entre los principales objetivos que persigue la Norma ISO/IEC 27002, se encuentran:

- Promover un mejor control de los activos e información sensible de una organización, a través de una adecuada definición de roles y responsabilidades, y el afinamiento de los procesos implicados.
- Ofrecer un marco de trabajo ideal, para la implementación de políticas y procedimientos de seguridad de la información.
- Generar conciencia en la organización, respecto a la debida gestión de la seguridad de la información, a través de un proceso transversal.
- Facilitar la identificación y corrección de los puntos débiles de la organización, desde las perspectivas: tecnología, procesos y personas.

- Gestionar los riesgos previamente identificados, actuando frente a ellos de manera proactiva y no reactiva.
- Apoyar la implementación de un SGSI en cualquier tipo de organización, en conformidad con una legislación o reglamentación internacional.

2.1.3.2.2. Estructura de la Norma

La última edición de la Norma ISO/IEC 27002:2013 establece 14 Dominios, dentro de los cuales se especifican 35 objetivos y 114 controles, con sus respectivas guías para su implantación. Todos estos elementos, están plenamente adaptados, al actual contexto tecnológico, a las amenazas vigentes y a los requerimientos de las organizaciones. Un objetivo de control define el fin que se desea alcanzar, y un control es el método empleado para lograr ese propósito (ISO Tools, 2019).

En la Tabla siguiente, se describe brevemente los Dominios, que conforman la Norma:

Tabla 5. Dominios de la Normativa ISO/IEC 27002

Dominio	Descripción
Sección de Introducción.	Muestra su estructura documental y campo de aplicación, así como, los términos, definiciones y normas relacionadas, que la complementan.
Políticas de seguridad.	Expone los objetivos que persigue el documento, y declara el compromiso por parte de las autoridades, para la aprobación, emisión y revisión continua de las políticas.
Aspectos organizativos de la Seguridad de la Información.	Especifica los roles y responsabilidades, que son atribuidos al personal implicado con la gestión de seguridad de la información institucional.
Seguridad ligada a los Recursos Humanos.	Define lineamientos para garantizar que el personal involucrado, entienda sus responsabilidades antes, durante y después de ser contratados, en el contexto de la seguridad de la información.
Gestión de activos.	Asegura que la organización tenga pleno conocimiento de sus activos, y de los responsables que velarán por su protección. Define directrices para garantizar que la información sea debidamente clasificada y protegida según su nivel de criticidad.
Control de accesos.	Gestiona el acceso a la información, sistemas y recursos para usuarios autorizados, en base a los privilegios que le han sido otorgados.
Cifrado.	Define la información y sistemas, que requieren la implementación de técnicas de cifrado, así como los responsables de la gestión de sus claves.
Seguridad física y ambiental.	Establece medidas para limitar o restringir el acceso físico a las instalaciones y equipamiento. Además, define controles para contrarrestar aquellos factores ambientales, que dificulten el normal funcionamiento de los equipos.

Seguridad de las operaciones.	Determina lineamientos relacionados a la operativa, para establecer una correcta protección contra malware, gestionar backups, registrar incidencias y resolver vulnerabilidades técnicas.
Seguridad en las telecomunicaciones.	Controla el acceso a los recursos de red, y a la información que procesan, tanto a nivel físico como lógico. Garantiza que éste equipamiento, sea albergado en instalaciones seguras y en condiciones ambientales óptimas.
Adquisición, desarrollo y mantenimiento de los sistemas de información.	Incluye controles de seguridad para la protección de los datos, en el ámbito de desarrollo y adquisición de software, por parte de la organización.
Relaciones con proveedores.	Busca proteger los activos de la organización, que son accesibles para los suministradores o proveedores.
Gestión de incidentes en la Seguridad de la Información.	Garantiza que los problemas de seguridad de la información, sean notificados oportunamente, y que se ejecuten acciones preventivas y/o correctivas para gestionarlos.
Aspectos de la Seguridad de la Información en la gestión de la continuidad de negocio.	Establece lineamientos para el desarrollo de planes de contingencia, que permitan restaurar los servicios prestados, dentro de los plazos requeridos.
Cumplimiento.	Su propósito principal es evitar el incumplimiento de las directrices plasmadas en el documento de políticas, mediante el alineamiento con los respectivos reglamentos, obligaciones legales y contractuales establecidos por la organización.

Adaptación de ISO27000, 2020

2.1.3.2.3. Ventajas y Desventajas de la Norma ISO 27002

A partir de una revisión exhaustiva de información relacionada a la Norma y de su documentación propiamente dicha, se ha podido determinar algunos criterios a favor y en contra, que pueden ser considerados para su elección y aplicación. La Tabla siguiente expone las deducciones más relevantes:

Tabla 6. Pros y Contras de la Normativa ISO/IEC 27002

Pros	
Adaptable y Flexible	▪ Se puede implantar en organizaciones de forma transparente a su tamaño o actividad. ▪ Se adapta a las necesidades de la organización, debido a que brinda flexibilidad en la elección de sus controles (no es obligatorio la aplicación de todos). ▪ Se ajusta fácilmente, a un plan específico de políticas de seguridad de la información y a su proceso previo de análisis de riesgos.
Clara y concisa	▪ Es una excelente alternativa para aquellas organizaciones, que requieren concentrar sus esfuerzos, expresamente en la implementación de controles, para gestionar sus riesgos. La Norma ofrece una guía de implementación clara y concisa.

	▪ Expone sus controles con un alto nivel de detalle y especificidad, lo que lo diferencia de otras normas existentes, que tienen un carácter más generalista y transversal.
Documentación y reconocimiento	▪ Existe documentación bien estructurada, procedente de múltiples fuentes primarias y secundarias, que guían su implementación. ▪ Es una Norma técnica reconocida y adoptada en Ecuador desde 2009, como NTE INEN-ISO/IEC 27002. ▪ Se puede acceder fácilmente a su documentación oficial (impresa o digital), a través del Servicio Ecuatoriano de Normalización (INEN). ▪ Es un estándar reconocido y adoptado ampliamente por organizaciones a nivel mundial, lo que le faculta un alto nivel de aceptación.
Contras	
Certificación	▪ No es certificable por sí misma, necesita implementarse de forma conjunta con la Normativa ISO 27001.
Alcance	▪ No contempla una guía para análisis de riesgos, necesita una Metodología que la complemente.

Adaptación de ISO27000, 2020

2.1.3.3. Justificación de la Normativa seleccionada

La elección de la normativa, se sustenta precisamente en las ventajas expuestas en la Tabla anterior, las cuales resaltan su capacidad para adaptarse a cualquier ámbito, mediante el alineamiento de sus controles de seguridad, con los requerimientos, disponibilidad de recursos y estrategias de negocio de la organización. Se consideró, su orientación a la gestión de riesgos de forma exclusiva y directa, tomando en cuenta que, en esa instancia de la investigación, ya se habrán identificado previamente los valores de riesgos con MAGERIT v3, y resulta innecesaria, la aplicación de alguna norma que contemple este proceso. Además, se destaca su flexibilidad para ajustarse a un plan específico de políticas de seguridad de la información, siendo este, el objetivo principal del presente proyecto. Finalmente, su amplio espectro documental, reconocimiento internacional y adopción a nivel local, son razones complementarias que reafirman la premisa, que esta normativa representa la mejor alternativa para satisfacer las necesidades del investigador e institución seleccionada.

2.2.Trabajos Relacionados

El presente estado del arte recoge las principales experiencias, conclusiones y resultados de investigadores, conseguidos a partir de la implementación de proyectos y propuestas de los últimos años, relacionadas con la ejecución de procesos de Análisis de Riesgos de TI,

principalmente enfocados en la Metodología de origen español MAGERIT versión 3, la cual ofrece una guía sistemática y una serie de técnicas para la evaluación de los riesgos que resultan del uso de las TIC (Ministerio de Hacienda y Administraciones Públicas, 2012).

Adicionalmente, se recogerán las principales conclusiones que obtuvieron tras la implantación de las Normativas ISO 27001 e ISO 27002 en organizaciones públicas y privadas, las cuales proveen los requisitos y buenas prácticas útiles para la implantación, mantenimiento, y certificación de Sistemas de Gestión de Seguridad de la Información (SGSI) (ISO, 2013). Finalmente, se expone y analiza nuevas herramientas, métodos y soluciones que están marcando la actual tendencia dentro de esta temática, y que podrían ser una alternativa válida para futuros trabajos de investigación.

Contero (2019), autor del proyecto "Diseño de una Política de Seguridad de la Información basada en la Norma ISO 27002:2013, para el Sistema de Botones de Seguridad del Ministerio del Interior"; menciona que los 25 controles que fueron implementados en la institución, se adaptaron satisfactoriamente al entorno, debido al proceso previo de análisis de riesgo con la Metodología española MAGERIT versión 3. Señala que, al determinar un entorno de riesgo real dentro de la institución, se pudo definir de forma más precisa, las acciones necesarias para gestionar la seguridad de la información, mediante el establecimiento de las definiciones, terminologías, abreviaturas y responsabilidades adecuadas, con el fin de preservar la naturaleza de los datos. Finalmente, destaca a MAGERIT como una herramienta válida en instituciones estatales, por su flexibilidad, adaptabilidad y facilidad de implementación.

Crespo y Cordero (2018) en su proyecto denominado "Estudio comparativo entre las metodologías CRAMM y MAGERIT para la Gestión de riesgo de TI en las MPYMES" manifiesta que MAGERIT presenta varios puntos a favor, respecto a su contendor y a otras Metodologías similares. Por ejemplo, indica que CRAMM (CCTA Risk Analysis and Management Method), desarrollada por Agencia Central de Comunicaciones y Telecomunicaciones británica, ahora renombrada como Oficina de Comercio Gubernamental (CCTA, s.f.), ha sido diseñada específicamente para grandes empresas, lo cual no encajaría en la mayoría de organizaciones a nivel nacional, sumado a que MAGERIT si es adaptable a cualquier entorno. Otro punto a considerar, es la forma de distribución de sus herramientas de software, siendo de manera comercial en el caso de CRAMM y libre para la Metodología de origen español.

Adicionalmente, expone que el ciclo de MAGERIT es completo e integral, debido a que valora los activos en cinco dimensiones, evalúa las amenazas en términos de degradación y frecuencia, y estima los riesgos de forma intrínseca y residual. Por su parte la Metodología CRAMM únicamente reconoce los riesgos y posteriormente, calcula la frecuencia de los mismos. De esta manera, el autor concluye que MAGERIT es la guía que mejor se acopla, a la realidad de las MPYMES ecuatorianas.

Holguín (2018), en su proyecto "Modelo de Madurez para el Análisis de Riesgos de los Activos de Información basado en las Metodologías MAGERIT, OCTAVE y MEHARI", propone un Modelo de Madurez dirigido a Empresas Navieras, basado en las metodologías MAGERIT, OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) y MEHARI (Methode Harmonisée d'Analyse de Risques), desarrolladas por la Universidad estadounidense Carnegie Mellon y el Club Francés de la Seguridad de la Información (CLUSIF) respectivamente (CMU, 2001) (CLUSIF, s.f.).

El modelo integra las Metodologías antes citadas y posteriormente, establece sus niveles de madurez mediante el Modelo Capability Maturity Model Integration (CMMI) creado por el Software Engineering Institute de la Universidad Carnegie Mellon de Estados Unidos (CMU, 2009), con el objetivo de evaluar los niveles de cumplimiento de las tareas de Análisis del Riesgo en una organización. El autor manifiesta, que el modelo se adaptó satisfactoriamente al contexto de estas empresas, y adicionalmente menciona que las mismas, obtuvieron una calificación importante, en cuanto su nivel de madurez, con valores que fluctúan entre tres y cinco puntos, lo cual significa que han llegado a obtener un proceso de análisis formalizado, basado en la aplicación de herramientas y técnicas proactivas, que llevan una evaluación continua.

Santonja (2019), en su estudio denominado "Análisis y correlación entre probabilidad e impacto de los riesgos", indica que los modelos cualitativos de evaluación del riesgo, son mucho más ágiles, su costo es reducido, y posee tiempos de desarrollo relativamente pequeños; por su parte, los cuantitativos permiten identificar los riesgos a detalle y de forma granular utilizando modelos matemáticos y probabilísticos cuyos resultados poseen mayor exactitud. Adicionalmente, menciona que a mediano plazo la tendencia será la automatización

del cálculo del impacto y riesgo con el uso de Big Data, para la elaboración de proyecciones y predicciones a partir de un repositorio de eventos o logs.

Finalmente, el investigador declara que la ejecución de un Análisis de Impacto al Negocio (BIA), es una alternativa que podría sumarse o combinarse con el análisis del riego tradicional, para determinar las repercusiones en términos de costos y tiempos de recuperación.

Urgilés y Caiza (2017) en su proyecto "La concientización como factor crítico para la gestión de la seguridad de la información", deducen que existen tres parámetros que deben ser reforzados en las organizaciones para reducir los niveles de riesgo: la tecnología, los procesos y las personas, sin embargo, indican que se invierte de forma desproporcionada únicamente en el primer factor, dejando de lado a las personas. Ante esta situación, Urgilés y Caiza, resaltan la importancia de contar con un compromiso serio por parte de la gerencia para capacitar al personal, sumado a un proceso de identificación de información sensible y crítica, ejecutado de manera profesional y objetiva. Sintetizando su idea, se podría expresar que los pilares fundamentales para esta nueva cultura organizacional serán: la responsabilidad, confianza, comunicación y cooperación entre sus actores.

Parra (2019), en su artículo denominado: "Amenazas Persistentes Avanzadas (APT) y su impacto en Latinoamérica ¿cómo estar preparados?", señala que Venezuela y Ecuador fueron los países más afectados por parte de este malware en la región, de acuerdo a un estudio realizado por la empresa ESET en 2018. Indica que la APT denominada "Machete", con fines de espionaje, generó el 42 y 36% de los ataques a estos países respectivamente, mediante correos electrónicos, técnicas de ingeniería social y pishing. El autor señala que, bajo este escenario, empresas reconocidas de seguridad han sugerido el uso de herramientas sofisticadas de protección, como: técnicas heurísticas de detección, cifrado de datos con algoritmos, inteligencia artificial, uso de big data y monitoreo de logs, entre otros. Sin embargo, Parra concluye, señalando que estas técnicas serán inútiles sin una formación del personal, puesto que la naturaleza de incursión de las amenazas APT, es el explotar el factor humano, sea por métodos de ingeniería social o medios sencillos como mails y páginas web falsas.

Pérez (2020), en su artículo denominado "Importancia de un sistema de gestión de seguridad de la información para empresas de tecnología", señala que la implantación de un SGSI, puede

complementarse con el establecimiento de un Plan de Continuidad del Negocio, debido a que, para cualquier empresa con medidas de seguridad o no, le es imposible evitar en su totalidad la materialización de un probable incidente de seguridad. De esta manera, la organización estará en capacidad de dar respuesta a aquellos eventos inesperados, para mantener disponibles sus servicios dentro de rangos aceptables.

Pérez señala, que el éxito del Plan de Continuidad en cualquier empresa, depende de gran manera, del interés que ésta preste a la fase de pruebas y de un proceso coherente de difusión e inclusión hacia todo el personal, puesto que el éxito del proyecto dependerá también, del grado de conocimiento de cada uno de sus actores, involucrados de forma directa o indirectamente con la organización.

Gantiva (2020), en su artículo "Gestión de Riesgos en el Internet de las Cosas (IOT)", considera que una empresa que cuente previamente con Políticas basadas en las ISO 27001 e ISO 27002, tendrán menos inconvenientes al momento de gestionar la seguridad respecto al uso de esta tecnología, puesto que, únicamente requerirá añadir a estas medidas, las recomendaciones definidas en los estándares complementarios como la ISO/IEC 27017 (Controles de Seguridad para Servicios Cloud) e ISO 27018 (Protección de información personal en la nube). Manifiesta que generalmente el usuario, carece de suficientes conocimientos técnicos o legales, relacionados a los dispositivos de IoT, y adicionalmente los proveedores no entregan suficiente información al comprador, sobre su uso adecuado.

Además, recomienda el uso de metodologías cómo MAGERIT, para identificar correctamente las vulnerabilidades presentes en la organización o inherentes en el usuario del IoT y herramientas técnicas, para revisar logs de eventos inesperados, provenientes de sus dispositivos y servicios.

Arévalo et al. (2017), en su artículo "Metodología Ágil para la Gestión de Riesgos Informáticos", mencionan que el proceso de Gestión del Riesgo del tipo tecnológico, implementado en una PYME de la ciudad de Cuenca, se basó en el estándar ISO/IEC 27005, al cual se incorporó las recomendaciones, conceptos y buenas prácticas de otras Guías y Metodologías de seguridad como MAGERIT, ISO 27001, ISO 27002 y lo correspondiente a la seguridad en la gestión de servicios de ITIL (Information Technology Infrastructure Library) en

su versión 3, disponible desde 2007, la cual define directrices para una adecuada prestación de servicios de TI en las organizaciones (CCTA, s.f.).

Como resultado, se obtuvo una Metodología ágil e integral, que permitió la identificación de altos niveles de Riesgo, en al menos el 60 por ciento de sus activos de información (datos de clientes, proveedores, transacciones diarias, recetas, costos, etc.), resaltando además que ninguno de ellos, obtuvo una valoración Baja o Despreciable. Indican que las amenazas identificadas, corresponden en su mayoría a errores no intencionados por parte del usuario, lo cual respaldó la necesidad de capacitar a los usuarios internos en temas de seguridad.

Recalde (2019), autora del proyecto "Plan de implementación de un SGSI y aplicación de controles críticos en el Centro de Operaciones de Seguridad en la Empresa GMS", manifiesta que, para lograr los objetivos esperados, es de vital importancia el apoyo constante de la Gerencia o Comité de Seguridad a lo largo del proceso de implementación de un SGSI, alineando los objetivos del negocio y de seguridad de la información.

Además, menciona que es fundamental una revisión periódica del proceso, con una frecuencia de al menos dos veces al año, para evaluar los nuevos activos, niveles de riesgo y controles implementados, para avalar la efectividad de las medidas implantadas. Finalmente, se ha hecho visible la intención de la Gerencia, por impulsar la Certificación de la empresa con la Norma ISO/IEC 27001:2013, en razón de la concientización realizada y el conocimiento de los riesgos inherentes en su sistema informático.

Domínguez et al. (2017), en su artículo "Aplicación de técnicas de fuerza bruta con diccionario de datos, para vulnerar servicios con métodos de autenticación simple "Contraseñas", pruebas de concepto con software libre y su remediación", manifiestan que existe un incremento importante en el número de ataques mediante técnicas de fuerza bruta, siendo evidente que la principal falencia o vulnerabilidad que está siendo explotada, es el uso de contraseñas débiles como único método de autenticación, confirmando de esta manera, la poca concientización en el uso y manejo de las mismas.

Manifiestan que la formación a los empleados son factores claves para mitigar los riesgos asociados a la seguridad; un empleado capacitado conoce las recomendaciones para crear contraseñas robustas y cambiarlas periódicamente, por lo tanto, es menos propenso a que

sufra ataques de fuerza. De esta manera, colaborará con la seguridad de la empresa y/o de su hogar.

Altamirano y Bayona (2017) manifiestan en su artículo "Políticas de Seguridad de la Información: Revisión Sistemática de las Teorías que Explican su Cumplimiento", que el cumplimiento de las políticas de seguridad de la información que implementan las organizaciones, está relacionado directamente con el estudio del comportamiento humano. Para ello, explican, es necesario un estudio profundo de las teorías psicológicas o sociales de cada uno de los actores de un sistema de información, para obtener un enfoque interdisciplinario que no dependa únicamente de la perspectiva tecnológica.

Indican que son parámetros a considerar en el comportamiento del factor humano, los siguientes: la actitud y percepción de la persona de cara a la obligación de cumplir una normativa, el nivel de percepción que el individuo tiene respecto a una amenaza o riesgo, su capacidad de respuesta y conducta frente a ello; también consideran como factores: el apego y compromiso natural al cumplimiento de reglas o normas, el deseo de entrar en comportamientos antisociales, su nivel de interacción social, el nivel de compromiso por su desarrollo personal, el nivel de confianza en sí mismo, su nivel de auto control, su motivación intrínseca, entre otros indicadores.

Muñoz y Ponce (2017), en su artículo "Metodología para seleccionar políticas de seguridad informática en un establecimiento de educación superior", exponen la realidad de algunas instituciones de educación superior respecto al establecimiento de políticas de seguridad de la información, y de forma específica en la Universidad de Cuenca. En su estudio, señalan que la selección e implementación de estas buenas prácticas, puede resultar una tarea tediosa, cuando no se emplea un procedimiento adecuado, que no cuente con los datos históricos provenientes de auditorías informáticas o procesos de análisis del riesgo, los cuales sirvan de sustento, para determinar el estado de seguridad en estos establecimientos. En vista de esta problemática, los autores proponen una metodología para identificar las vulnerabilidades dentro del Departamento de TI de la citada universidad, mediante la técnica Delphi, y una posterior selección de controles basados en la Norma ISO 27002. Como resultado, identificaron aquellos puntos débiles del sistema expuesto, y lograron rediseñar el manual

actual, tomando en consideración 133 controles, que fueron socializados previo respaldo y aprobación de sus autoridades.

2.3.Conclusiones del Estado del Arte

Mediante el análisis de las propuestas antes citadas, se obtuvo una visión actual del contexto en que las organizaciones se están enfrentado a los riesgos de TI en aras de resguardar sus activos de información. Se conoció algunos de los resultados que se alcanzaron, al implantar metodologías similares a las que propone el presente trabajo investigativo, mismos que han sido satisfactorios, y de esta manera, se justifica su elección. A su vez, se conocieron experiencias tras la utilización de herramientas alternativas, que buscan emerger y posicionarse a futuro, como son las técnicas de análisis de impacto y riesgo automatizado, que hacen uso de predicciones mediante Big Data, o la instauración de metodologías híbridas, que combinen los mejores atributos tanto de las técnicas de estimación del riesgo, del tipo cualitativo y cuantitativo. Se pudo constatar, que una metodología de análisis del riesgo, puede también complementarse con evaluaciones del tipo operativo, para verificar el impacto que podría ocasionar un problema de seguridad, sobre los procesos de negocio, y determinar tanto el "qué" y el "cómo" podría verse afectada la organización. Análogamente, se verificó que, a la implementación de un SGSI, puede añadirse un plan detallado, que exponga las respectivas medidas de recuperación o restauración en caso de incidentes, con el objetivo primordial de las organizaciones, por mantener sus servicios con un nivel de disponibilidad aceptable.

Adicionalmente, se evidenció la intención de varios investigadores por destacar la importancia de llevar a cabo una etapa de verificación y estudio de riesgos previo, con el objetivo de definir salvaguardas con mayor precisión y a la medida de la organización, evitando el desperdicio de recursos, acciones innecesarias o retrabajo. Finalmente, resaltan la necesidad de ejecutar acciones de comunicación, formación y concientización continua al personal, para la obtención de los resultados esperados.

En síntesis, a través de este estudio del estado de la cuestión, se logró recoger las principales conclusiones, recomendaciones y sugerencias que compartieron investigadores de toda índole, en el ámbito de la seguridad de la información y riesgos de TI, mismas que fueron

obtenidas de diversos entornos y sistemas de información, y que servirán como referencia, para trazar la mejor ruta que deba seguir el presente proyecto.

3. Objetivos y Metodología de Trabajo

3.1.Objetivo Principal

Diseñar Políticas de Seguridad de la Información basadas en la Norma ISO/IEC 27002 y MAGERIT versión 3, que propicien una adecuada protección de los activos de información pertenecientes al Ministerio del Trabajo de la ciudad de Ibarra.

3.2.Objetivos Específicos

- Identificar, tipificar y dimensionar los principales activos de información, pertenecientes al Ministerio del Trabajo de la ciudad de Ibarra, siguiendo el Catálogo de Elementos de MAGERIT v3, para la estimación de su valor.
- Identificar y evaluar el nivel de impacto y riesgo de las posibles amenazas, mediante la técnica de Análisis de Tablas propuesta por MAGERIT v3, con el objetivo de definir el estado de seguridad institucional.
- Definir Políticas de Seguridad de la Información en base a los controles de la Norma ISO/IEC 27002 seleccionados, con el fin de establecer medidas para salvaguardar los datos y activos de información de la entidad.
- Validar el diseño de las Políticas de Seguridad de la Información según la Norma ISO 27002, a través del personal técnico del Departamento de TICs del Ministerio del Trabajo.

3.3.Metodología de Trabajo

En base a Garay (2020), se puede determinar las diversas tipologías, técnicas e instrumentos de investigación, que se aplicarán y usarán en el presente proyecto, mismos que se exponen en la tabla siguiente:

Tabla 7.Metodología de Trabajo

Tipología	• **Documental:** para la recolección de información, se hará uso de material electrónico disponible en páginas web, repositorios de diversos centros de estudio, bases de datos, artículos científicos, entre otros.
	• **Aplicada:** en razón que el proyecto tiene como objetivo final, la creación de Políticas de Seguridad de la Información, orientadas a sus funcionarios, para el buen uso de sus activos informáticos
	• **Exploratoria:** debido a que ejecutará un proceso de identificación de activos relevantes de la institución y se evaluarán las amenazas y riesgos que pueden comprometer su seguridad.
	• **Cuantitativa:** puesto que se hará uso de la técnica denominada Análisis mediante Tablas descrita por MAGERIT, para la estimación de los niveles de riesgo.
Técnicas	• **Observación y revisión de documentación**: para definir los activos de información con los que cuenta actualmente la institución, se observará y se contrastará la información con inventarios disponibles.
	• **Reuniones y entrevistas:** se planificará reuniones con el personal y se realizarán entrevistas semiestructuradas (siguen un orden que no es rígido), para la extracción de información útil que alimenten el proceso.
	• **Internet:** como principal medio para recabar información respecto al objeto de estudio.
Instrumentos	• Libreta de campo • Plantillas de MAGERIT (Libro “Catálogo de Elementos”)

Adaptación de Garay, 2020

Finalmente, se sintetizan las tareas que serán ejecutadas, para la consecución de los objetivos propuestos en el presente proyecto:

Tarea 1: Para la recolección de la literatura correspondiente a las normativas ISO de la seguridad de la información, así como de las Metodologías de Análisis de Riesgo Informático y estado del arte, se recogió material electrónico publicado y depositado en la web, extraído principalmente de artículos y trabajos de titulación de los últimos años. Esta Tarea fue desarrollada en los Apartados "Antecedentes" y "Trabajos Relacionados", dentro del Capítulo 2 del presente documento.

Tarea 2 (Objetivo 1): Posteriormente al análisis del contexto de la entidad, dónde se conocerá su misión, visión, valores y estructura organizacional, se realizará el levantamiento de sus activos de información más relevantes, mediante observación directa, el uso de inventarios institucionales y de las plantillas que describe MAGERIT versión 3. Además, se planificarán reuniones virtuales y entrevistas semiestructuradas, con los Coordinadores de las Unidades institucionales, para recoger sus criterios de valoración, respecto a los activos que tiene a cargo. Siguiendo la misma estrategia, también se procederá a valorar las amenazas que podrían afectar estos recursos, en términos de degradación y frecuencia, acorde al Libro "Catálogo de Elementos" dispuesto por la Metodología en mención.

Tarea 3 (Objetivo 2): A partir de los datos recolectados, se aplicará la técnica de "Análisis mediante Tablas" propuesta por MAGERIT v3, con el objetivo de evaluar de forma cualitativa los niveles de impacto y riesgo, tanto intrínseco como residual, en conformidad con los criterios del personal de la organización. Con la finalidad de facilitar dichos cálculos, se elaborará una plantilla con la herramienta Microsoft Excel, la cual será adjuntada como Anexo del presente proyecto.

Tarea 4 (Objetivo 3): Para el desarrollo de las Políticas de Seguridad de la Información, se tomará como marco de referencia los Dominios y Controles de la Norma ISO/IEC 27002 que mejor se adecúen a las necesidades de la institución. La selección de los Dominios y el alcance de las Políticas, guardará relación con los resultados obtenidos de las tareas de evaluación del riesgo antes mencionado y el documento final será socializado a través de medios electrónicos como el correo electrónico institucional o el Sistema de Gestión Documental Quipux, previa autorización de la autoridad correspondiente.

Tarea 5 (Objetivo 4): Finalmente, para la validación de las Políticas de Seguridad de la Información, se optará por la evaluación y juicio de expertos, representados por personal técnico de la Dirección de TIC del Ministerio del Trabajo.

4. Desarrollo del Proyecto

En el presente Capítulo, se expondrá la parte medular de la propuesta planteada, la cual corresponde a la ejecución del proceso de Análisis de Riesgos utilizando la guía MAGERIT v3, y el desarrollo de las Políticas de Seguridad de la Información, en referencia a los Controles de la Norma ISO/IEC 27002, dentro del Ministerio del Trabajo de la ciudad de Ibarra.

4.1.Contexto de la Organización

De acuerdo al Plan Estratégico Institucional 2019 – 2021 (Ministerio del Trabajo, 2019), se exponen los aspectos más relevantes del contexto de la organización, para entender el ámbito en el cual se desarrollará el presente proyecto, respecto a su misión, visión, objetivos estratégicos y estructura. Mediante esta indagación preliminar, se podrá distinguir los principales servicios prestados por la entidad, así como el personal implicado, a fin de apoyar y fundamentar el proceso de Análisis de Riesgo a desarrollarse en los siguientes apartados.

4.1.1. Antecedentes

El Ministerio del Trabajo es un organismo de la Administración Pública ecuatoriana, encargado de la ejecución de políticas y normas en materia laboral, promoción del empleo, y fomento del trabajo digno e inclusivo, mediante la coordinación y control de las condiciones individuales y colectivas del talento humano (Ministerio del Trabajo,2021).

El proyecto propuesto, será implementado en ésta importante entidad de Gobierno, cuya sede se encuentra ubicada en la ciudad de Ibarra, desde donde ejerce su rectoría y competencias para la Región 1, que comprende las provincias de Imbabura, Carchi, Esmeraldas y Sucumbíos.

4.1.2. Misión y Visión

Misión

> Somos la Institución rectora de políticas públicas de trabajo, empleo y del talento humano del servicio público, que regula y controla el cumplimiento a las obligaciones laborales mediante la ejecución de procesos eficaces, eficientes, transparentes y democráticos enmarcados en modelos de gestión integral, para conseguir un sistema

de trabajo digno, de calidad y solidario para tender hacia la justicia social en igualdad de oportunidades (Ministerio del Trabajo,2019, p.59).

Visión

Seremos un referente a nivel nacional e internacional como una institución que fomenta el trabajo digno, impulsa el cumplimiento de los derechos individuales y colectivos de trabajadores y empleadores, líder en el desarrollo del talento humano e institucionaliza el diálogo social a través de procesos eficientes que permitan brindar servicios de calidad, con transparencia, efectividad, responsabilidad, solidaridad y lealtad (Ministerio del Trabajo,2019, p.59).

4.1.3. Objetivos estratégicos

Dentro de sus objetivos estratégicos 2019-2021, se encuentran: incrementar el trabajo digno en igualdad de oportunidad y de trato en el Ecuador, mantener el cumplimiento de derechos y obligaciones de la ciudadanía laboral, incrementar la eficiencia operacional, incrementar el uso eficiente del presupuesto, de los recursos físicos-tecnológicos y el desarrollo del talento humano (Ministerio del Trabajo,2019, p.60).

4.1.4. Estructura Organizacional

El Ministerio del Trabajo con sede en la ciudad de Ibarra, para el cumplimiento de sus objetivos, se encuentra organizada internamente de manera jerárquica, a través de Direcciones y Unidades Organizacionales, las cuales se evidencian a detalle en la Tabla y Figura siguientes:

Tabla 8. Estructura Organizacional y Servicios

Dirección	Unidad Organizacional	Personal a cargo	Servicios prestados a la ciudadanía
Dirección Regional		▪ Director Regional	Aprobación de documentos
Dirección Jurídica		▪ Asesor Jurídico ▪ Secretario Regional	Regulación de Contratos Colectivos, Procesos de reclamación colectiva, Diálogos sociales.
Dirección de Procesos Coactivos		▪ Juez ▪ Secretario de Coactivas ▪ Notificador de Coactivas	Atención por juicios coactivos, actas procesales y multas.
Dirección del Trabajo	Inspección del Trabajo	▪ Coordinador Inspectores ▪ Inspector Integral ▪ Notificador	Absolución de consultas de empleados del sector privado.
	Organizaciones Laborales	▪ Analista de Organizaciones Laborales	Aprobación de directivas Artesanales, refrendación de títulos y conformación de tribunales de artesanos.
	Seguridad y Salud en el Trabajo	▪ Analista de Seguridad y Salud	Revisión de Reglamentos de Higiene y Seguridad y de Planes Integrales de Prevención de Riesgos Laborales.
Dirección de Empleo	Atención de Grupos Prioritarios	▪ Técnico de Grupos Prioritarios	Desarrollo de talleres dirigidos a grupos de atención prioritaria y/o en condiciones de vulnerabilidad, ejecución de talleres de sensibilización y registro de sustitutos.
	Red Socio Empleo: contiene los Proyectos Mi Primer Empleo y Empleo Joven	▪ Técnico de Red Socio Empleo ▪ Técnico de Mi Primer Empleo ▪ Técnico Empleo Joven	Asesoramiento en la Plataforma Red Socio Empleo para búsqueda de ofertas laborales, capacitaciones en empresas.
Dirección de Evaluación y Control del Servicio Público	Control Técnico del Servicio Público	▪ Analista de Evaluación y Control Técnico	Consultas y denuncias del sector público
Dirección Administrativa Financiera	Contabilidad y Tesorería	▪ Contador Regional ▪ Tesorero Regional	Atención para legalización de Décimos y Utilidades, Consignaciones, Convenios de Pago de multas, Reporte de pagos a terceros.

	Secretaría General	▪ Secretario ▪ Técnico de Archivo	Ingreso de trámites y documentos
	Tecnologías de la Información y Comunicaciones	▪ Asistente de TICs	Soporte técnico sobre la Plataforma SUT y Salarios.

Elaboración propia

Figura 2. Estructura Organizacional (Elaboración Propia)

4.2.Análisis

En este apartado, se desarrolla la etapa inicial de la Metodología MAGERIT v3, que implica la ejecución de las tareas de Caracterización de los activos y amenazas dentro del Ministerio del Trabajo (Ibarra), como parte del análisis de su situación y estado de seguridad inicial. Las tareas restantes de dicha guía, correspondientes a las valoraciones de los niveles de impacto y riesgo, así como, la definición de las Políticas propuestas, se exponen en la sección 4.3 del presente proyecto.

4.2.1. Caracterización de los activos de información

Mediante esta tarea, se pudo identificar y tipificar los recursos institucionales que requieren ser protegidos, y se determinó su valor cualitativo, en base a un consenso de criterios entre los Coordinadores de las Unidades Administrativas y el Gestor de Seguridad, representado por el investigador del presente proyecto.

Esta estimación, se traduce como el nivel de daño que se provocaría a la entidad, si el activo fuese vulnerado en su disponibilidad, integridad, autenticidad, confidencialidad o trazabilidad. Cabe indicar, que estos cinco criterios de valoración, conforman las dimensiones de seguridad propuestas por MAGERIT versión 3, las cuales serán detalladas más adelante.

4.2.1.1. Identificación y Tipificación de los activos

MAGERIT v3 propone clasificar y agrupar los activos de información de la siguiente manera:

Tabla 9. Tipificación de Activos

TIPO	DESCRIPCIÓN	CÓDIGO
SERVICIOS	Actividades que presta una organización, para satisfacer las necesidades del usuario.	[S]
DATOS	Representa la información que manejan las personas para la prestación de servicios y se almacena en los equipos o soportes de información.	[D]
SOFTWARE	Son los programas utilizados para gestionar y explotar los datos, para realizar la prestación de servicios.	[SW]

EQUIPOS INFORMÁTICOS	Elementos físicos que soportan y procesan los datos, utilizando las aplicaciones o software, para la prestación de servicios.	[HW]
REDES DE COMUNICACIÓN	Medios físicos para la transmisión de datos sobre la red, a nivel interno o externo.	[COM}
SOPORTES DE INFORMACIÓN	Dispositivos o medios físicos que almacenan los datos, por períodos de tiempo o de manera definitiva (CD/DVDs, memorias flash, discos externos, impresos).	[MEDIA]
EQUIPAMIENTO AUXILIAR	Dispositivos o medios físicos de soporte, mismos que no están relacionados de forma directa con el tratamiento de los datos. Por ejemplo: Sistemas de Alimentación Ininterrumpida (UPS), sistemas de climatización, cableado, suministros de impresoras, mobiliario, entre otros.	[AUX]
INSTALACIONES	Espacio físico que alberga los recursos de información.	[L]
PERSONAL	Usuarios internos, externos o terceras personas, que hacen uso de los recursos de información.	[P]

Adaptación del Libro II de MAGERIT v3: Catálogo de Elementos, 2012

En base a estos criterios, y en la información obtenida de los inventarios institucionales, visitas de campo o entrevistas semiestructuradas a su personal, se extrajo una lista de los activos más relevantes (ANEXO 1:"ValAct_RI"), los cuales se resumen en la Tabla siguiente, para fines informativos:

Tabla 10. Resumen de Activos institucionales

TIPO ACTIVO	ACTIVO
SERVICIOS [S]	**Servicios prestados:** Absolución de consultas a empleados sector público y privado. Registro de Contratos y Finiquitos (Sistema Único de Trabajo). Registro de Reglamentos de Higiene y Salud (Sistema Único de Trabajo). Ingreso de desahucios, vistos buenos, notificaciones. (Sistema SINACOI). Registro de Inspecciones (Sistema SINACOI). Registro de Décimos y Utilidades (Sistema Salarial). Registro de Multas (Sistema Salarial). Registro de Multas Coactivas. Ingreso de trámites (Sistema Control Documental-Archivo). Búsqueda de ofertas (Plataforma Red Socio Empleo). **Servicios recibidos:** Enlace de datos (Corporación Nacional de Telecomunicaciones)

DATOS [D]	Contratos y Finiquitos (Sistema Único de Trabajo). Reglamentos de higiene y seguridad. Registro de vistos buenos e inspecciones. Registro de utilidades, décimos cuartos, décimos terceros. Pago de multas Documentos de Denuncias Datos de funcionarios de empresas Hojas de vida dentro de la Plataforma Red Socio Empleo Información de Recursos Humanos Respaldos de información sensible y correos Archivos de configuración de equipos
APLICACIONES [SW]	Sistema Único de Trabajo (SUT) Sistema Nacional de Control de Inspectores (SINACOI) Sistema de Registro Documental Sistema Salarial Plataforma Red Socio Empleo y Mi Primer Empleo Sistema de Recepción y Control de trámites (Archivo) Sistema Informático Integrado de Talento Humano (SIITH). Sistema de Mesa de Ayuda (GLPI) Sistema de Control de Tickets (GOIA) Sistema Integrado de Tributación (SITAC) Plataforma FielWeb Sistema Alfresco Sistema de Gestión Documental (Quipux) Software de ofimática
EQUIPOS INFORMÁTICOS [HW]	Servidor para Consola de Antivirus (Kaspersky) Servidor para Sistema de Videovigilancia (NUUO) Desktops y laptops (marcas HP, Dell, ACER) Impresoras y escáners (marcas HP, Samsung, Lexmark) Polycom HDX 7000 Teléfonos IP y análogos
REDES DE COMUNICACIÓN [COM]	Router (enlace de datos CNT) Switch administrable capa 2 (marca Avaya 3526T PWR+) Switch administrable capa 2 (marca 3COM 4228G) Switch no administrable (marca D-link DES1024A) Switch no administrable (marca TP-Link TL-SF1008D) Central telefónica híbrida (marca Avaya IP Office500V2) Puntos de acceso (marca Cisco WAP 321) Rack (marca Beaucoup) Patch panel (marca NEXXT) Organizador de cables (marca Beaucoup)
SOPORTES DE INFORMACIÓN [SI]	Medios magnéticos (CDs y DVDs) Discos Externos Impresos
EQUIPAMIENTO AUXILIAR [AUX]	UPS (marca EATON) Reguladores de voltaje Aire acondicionado (marca Lennox) Cableado estructurado Mobiliario

INSTALACIONES [L]	Centro de datos Oficinas Bodegas Puntos de atención al público Sala de reuniones Sala de videoconferencias
PERSONAL [P]	Funcionarios Usuarios externos Proveedor del enlace de red (CNT) Proveedores de equipos, repuestos y suministros

Elaboración propia

4.2.1.2. Dimensión de los activos

Como se mencionó anteriormente, MAGERIT v3 establece una valoración de activos bajo cinco dimensiones, y es precisamente una de sus principales fortalezas, respecto a Metodologías similares, que basan este análisis únicamente en tres de ellas. Estos criterios, permiten evaluar el nivel de daño que causaría en la organización, el hecho hipotético, en que un activo sea vulnerado o afectado en su disponibilidad, integridad, autenticidad, confidencialidad o trazabilidad. La Tabla siguiente detalla las dimensiones, con las que se llevará a cabo esta tarea:

Tabla 11. Dimensiones según MAGERIT v3

Dimensión	Descripción	Código
Disponibilidad	¿Qué daño provocaría a la organización, el escenario en que el activo no estuviera disponible?	**[D]**
Confidencialidad	¿Qué daño provocaría a la organización, el escenario en que el activo fuera conocido por personas no autorizadas?	**[C]**
Integridad	¿Qué daño provocaría a la organización, el escenario en que los datos fueran modificados sin autorización?	**[I]**
Autenticidad de los usuarios del servicio	¿Qué daño provocaría a la organización, el escenario en el cual, el individuo que accede al servicio, no es realmente quien dice ser?	**[A_S]**
Autenticidad del origen de los datos	¿Qué daño provocaría a la organización, el escenario en que los datos no fueran realmente generados por quién se cree?	**[A_D]**
Trazabilidad del servicio	¿Qué daño provocaría a la organización, el escenario en el cual, no quedara evidencia de quién hizo uso del servicio?	**[T_S]**
Trazabilidad de los datos	¿Qué daño provocaría a la organización, el escenario en el cual, no quedara evidencia de quién accedió a los datos?	**[T_D]**

Adaptación del Libro II de MAGERIT v3: Catálogo de Elementos, 2012

Es importante destacar, que dichas dimensiones no son todas aplicables para cada uno de los activos de información, por cuanto dependerá de su naturaleza. En este sentido, la Metodología distribuye un determinado grupo de dimensiones, para cada tipo de activos, de la siguiente manera:

Tabla 12.Relación Tipo de Activo-Dimensión

Tipo Activo	Dimensión	Código Dimensión
Servicios	Disponibilidad	D
	Autenticación del servicio	A_S
	Trazabilidad del servicio	T_S
Datos	Disponibilidad	D
	Integridad	I
	Confidencialidad	C
	Autenticación de los datos	A_D
	Trazabilidad de los datos	T_D
Aplicaciones	Integridad	I
	Autenticación del servicio	A_S
	Autenticación de los datos	A_D
	Trazabilidad del servicio	T_S
	Trazabilidad de los datos	T_D
Equipos informáticos	Disponibilidad	D
	Trazabilidad del servicio	T_S
	Trazabilidad de los datos	T_D
Redes de comunicación	Disponibilidad	D
	Trazabilidad del servicio	T_S
	Trazabilidad de los datos	T_D
Soportes de información	Disponibilidad	D
	Trazabilidad del servicio	T_S
	Trazabilidad de los datos	T_D
Equipamiento Auxiliar	Disponibilidad	D
Instalaciones	Disponibilidad	D
	Autenticación del servicio	A_S
Personal	Disponibilidad	D
	Autenticación del servicio	A_S

Adaptación del Libro II de MAGERIT v3: Catálogo de Elementos, 2012

4.2.1.3. Valoración de los activos

Para dar cumplimiento a la presente tarea, se requirió la participación activa del personal de la institución, con quienes se valoraron los recursos de información que tienen a su cargo, en base a las cuestiones expuestas en la Tabla 11 y en la siguiente escala de calificación cualitativa:

Tabla 13. Niveles de valoración de Activos

Valor	Nivel	Criterio Valoración
0	MB (Muy Bajo)	Daño Irrelevante a la organización
1 a 3	B (Bajo)	Daño menor a la organización
4 a 6	M (Medio)	Daño importante a la organización
7 a 9	A (Alto)	Daño grave a la organización
10	MA (Muy Alto)	Daño muy grave a la institución

Adaptación del Libro II de MAGERIT v3: Catálogo de Elementos, 2012

Los resultados de esta tarea, se exponen de manera detallada en el ANEXO 1 ("ValAct_RI") del presente proyecto, sin embargo, se ha visto pertinente, elaborar los siguientes diagramas de barras sobre la plataforma de visualización Tableau, con el objetivo de facilitar la lectura y comprensión de los valores obtenidos:

Figura 3.Valoración de Servicios (Elaboración Propia)

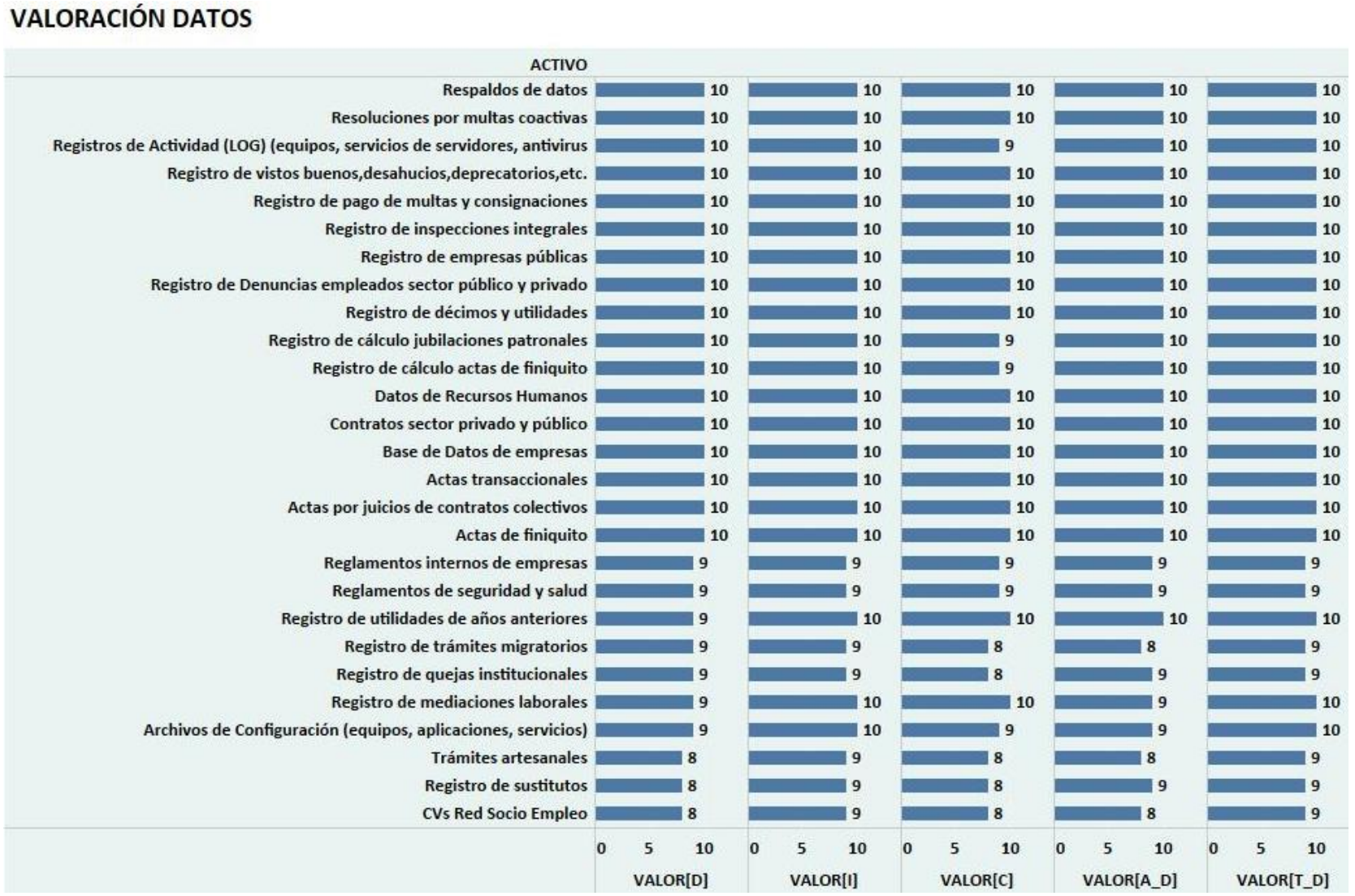

Figura 4.Valoración de Datos (Elaboración Propia)


VALORACIÓN APLICACIONES
ACTIVO
Zimbra 10 10 10 10 10
Windows 8 10 5 5 8 8
Windows 7 10 5 5 8 8
SUT-Módulo Registro Denuncias 10 10 10 10 10
SUT-Módulo IESS 10 9 9 9 9
Sistema Único del Trabajo(SUT)-Módulo Actas de Finiquito 10 10 10 10 10
Sistema Único del Trabajo (SUT)-Módulo Contratos y Datos empleador 10 10 10 10 10
Sistema Salarial-Registro Utilidades 10 10 10 10 10
Sistema Salarial-Registro Décimos 10 10 10 10 10
Sistema Quipux 10 10 10 10 10
Sistema Oficial Contratación Pública 10 10 10 10 10
Sistema Nacional de Control de Inspectores(SINACOI)-Módulo Registro de trámites (vistos buenos, desahu.. 10 10 10 10 10
Sistema Nacional de Control de Inspectores(SINACOI)-Módulo Registro de inspecciones integrales 10 10 10 10 10
Sistema Nacional de Control de Inspectores(SINACOI)-Módulo Legalización Décimos y Utilidades 10 10 10 10 10
Sistema Nacional de Control de Inspectores(SINACOI)-Módulo Generación Boletas 10 10 10 10 10
Sistema de Registro de Documentos (Dirección) 10 10 10 10 10
Sistema Dato Seguro 10 10 10 10 10
SINACOI-Módulo Financiero-Pago multas 10 10 10 10 10
Mozilla Thunderbird 10 10 10 10 10
Kaspersky 10 10 10 10 10
SUT-Sistema para instituciones pública-Selección de personal (concursos) 9 10 10 10 10
SUT-Sistema para instituciones pública-Registro 9 9 9 10 10
SUT-Sistema para instituciones pública-Módulo SIITH 9 9 9 10 10
SUT-Sistema para instituciones pública-Evaluación de desempeño 9 10 10 10 10
SUT-Módulo Registro Capacitaciones 9 7 7 7 7
Sistma SITAC (SRI) 9 9 9 10 10
Sistema Único del Trabajo(SUT)-Módulo Reglamentos internos 9 9 9 9 9
Sistema Único del Trabajo(SUT)-Módulo Reglamentos de seguridad y salud 9 9 9 9 9
Sistema Nacional de Control de Inspectores(SINACOI)-Módulo Sorteo de inspecciones integrales 9 9 9 10 10
Sistema Nacional de Control de Inspectores(SINACOI)-Módulo Sorteo Boletas 9 9 9 9 9
Sistema Alfresco 9 8 8 8 8
SINACOI-Módulo Financiero-Pago utilidades años anteriores 9 10 10 10 10
VNC 8 10 10 10 10

Figura 5.Valoración de Aplicaciones (Elaboración Propia)

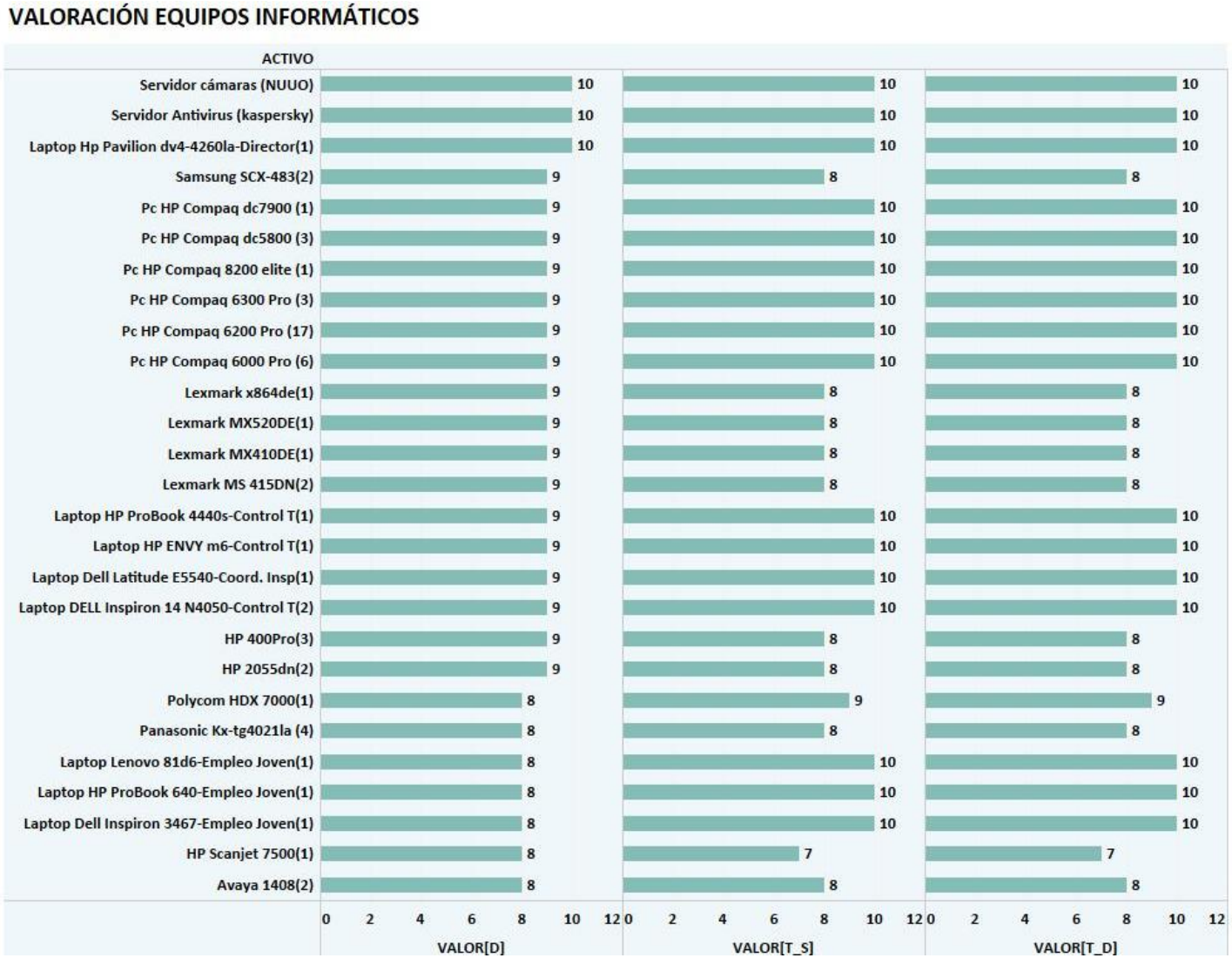

Figura 6.Valoración de Equipos de Informáticos (Elaboración Propia)

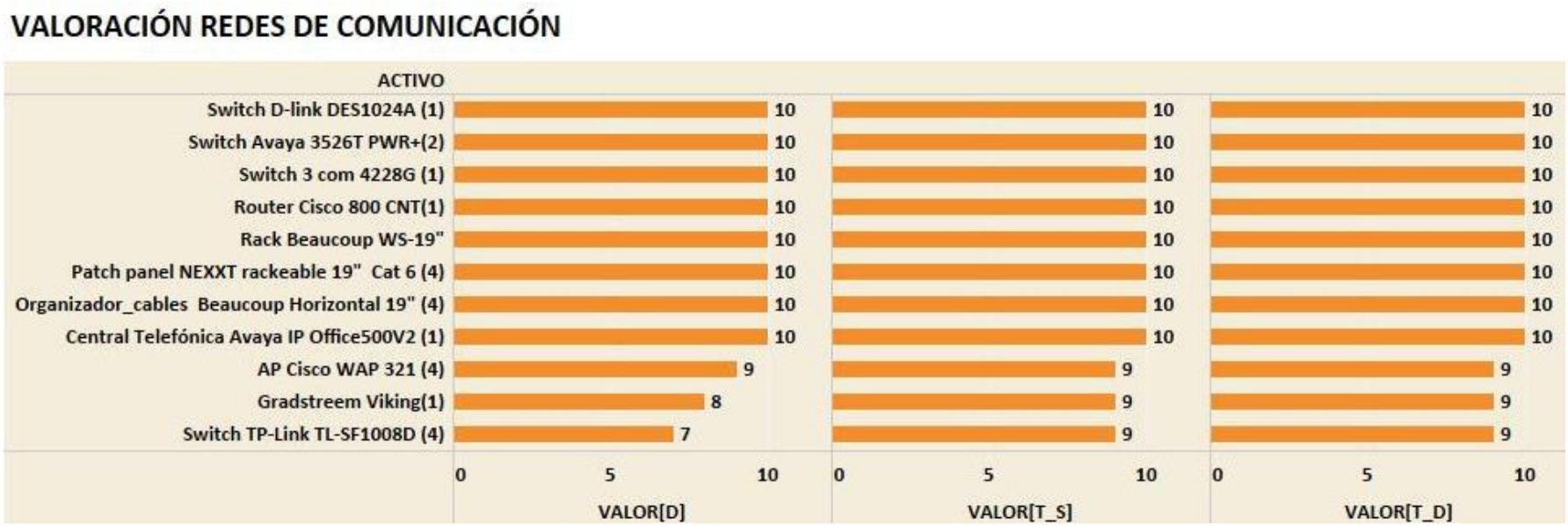

Figura 7.Valoración de Activos (Redes de Comunicación) (Elaboración Propia)

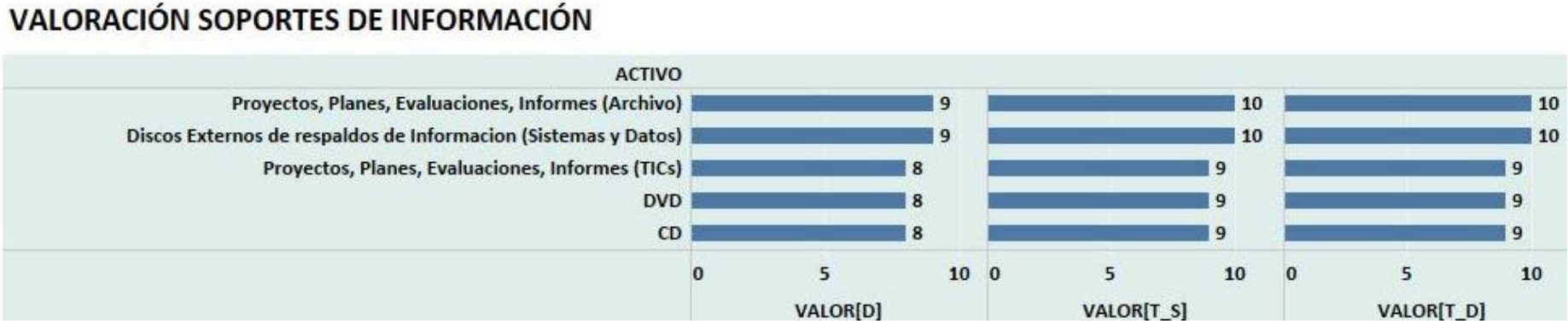

Figura 8.Valoración de Activos (Soportes de Información) (Elaboración Propia)

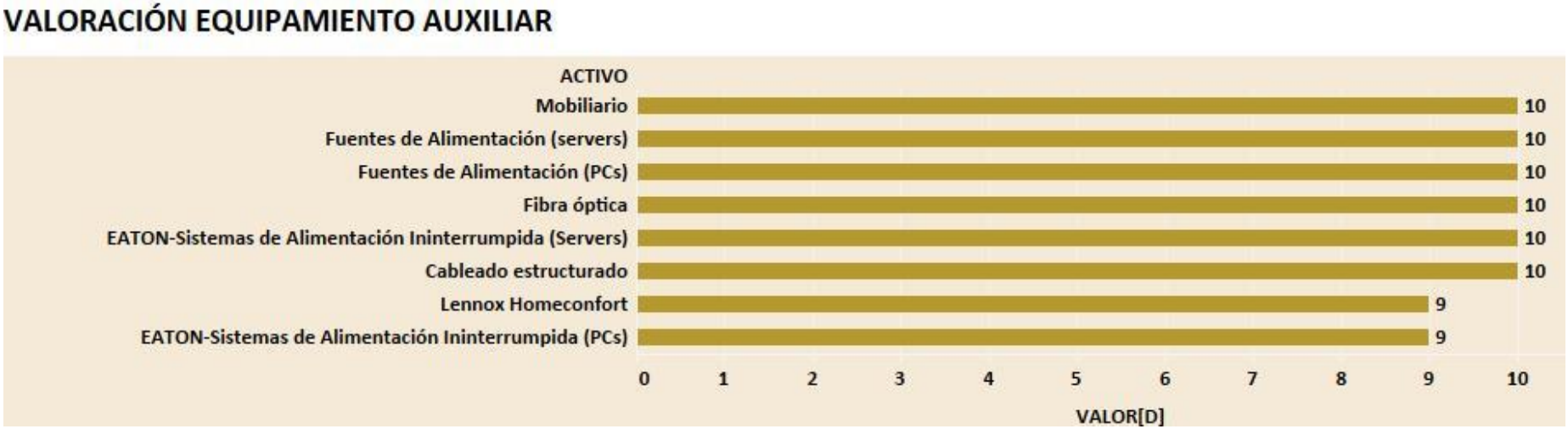

Figura 9.Valoración de Activos (Equipamiento auxiliar) (Elaboración Propia)

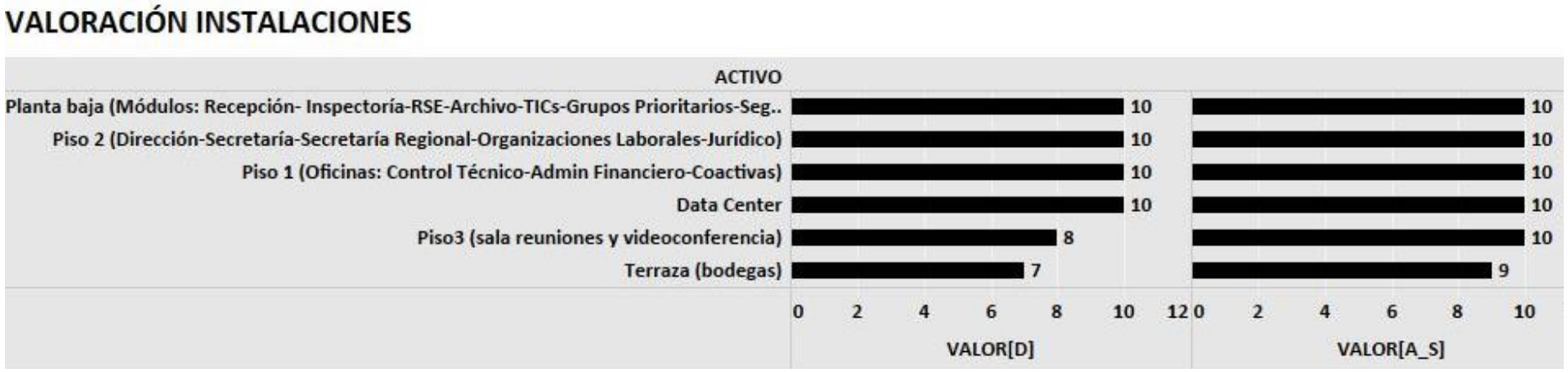

Figura 10.Valoración de Instalaciones (Elaboración Propia)

Figura 11.Valoración de Personal (Elaboración Propia)

De la tarea de caracterización de activos dentro del Ministerio del Trabajo (Ibarra), se pudo extraer las siguientes impresiones:

- Debido a la actual pandemia, las tareas de identificación y calificación de los activos, se las desarrolló a través de reuniones virtuales con los responsables de las Unidades Administrativas de la institución, con previa autorización del Director Regional.
- Las convocatorias a las reuniones fueron emitidas mediante correo interno, de parte de la máxima autoridad, para asegurar el compromiso y participación activa del personal involucrado.
- MAGERIT v3 ya define de forma previa, las dimensiones en las que deben ser valorados cada grupo de activos, por lo que no fue necesario analizar la aplicabilidad o alcance de cada una de ellas. (la distribución se encuentra detallada en la Tabla 12).
- La valoración basada en dimensiones, permitió distinguir de manera más profunda la importancia de cada activo y el posible impacto para la organización, de modo que se pudo evaluar las vulnerabilidades desde distintas perspectivas.
- Los activos del tipo Servicios y Aplicaciones, que obtuvieron las más altas calificaciones, se originan de los procesos más sensibles de la institución, es decir, a aquellos que están relacionados con la gestión de la información reservada y/o vinculada al registro de valores monetarios. De esta manera, los activos del tipo Datos con mayor valor, corresponden a los registros de contratos, finiquitos, Décimos y Utilidades, pagos de multas coactivas y denuncias por parte de empresas públicas y privadas.
- Los datos obtuvieron altas valoraciones en las dimensiones, integridad y confidencialidad, mientras que la autenticación, fue el tema de mayor preocupación, en cuanto a las aplicaciones. A criterio de los funcionarios, también es trascendental, asegurar el origen de los datos (autenticidad) y conocer quién los usó y a qué momento (trazabilidad).
- Adicionalmente, merecen ser citados otros activos que no están íntimamente relacionados con el core de la institución, pero que dan soporte a los mismos, por lo que también obtuvieron valoraciones importantes. Por ejemplo, resalta el

servicio de enlace de datos que la Corporación Nacional de Telecomunicaciones presta a la entidad, los activos del tipo datos como: respaldos de funcionarios, información de recursos humanos y logs de servidores, así como el correo institucional, sistema Quipux y antivirus, en el caso de los activos del tipo aplicaciones.

- En cuanto a los activos de hardware, destacan los equipos encargados de gestionar la consola del antivirus Kaspersky y el sistema de video vigilancia institucional (NUUO), los cuales fueron altamente valorados en la dimensión de disponibilidad. Cabe mencionar, que la institución cuenta únicamente con los servers citados, pues mantiene un enlace da datos con el edificio matriz, de donde se comparte la mayoría de servicios de red. En este mismo ítem, también resaltan los ordenadores pertenecientes a los funcionarios del Nivel Jerárquico Superior, y al personal involucrado con la prestación de servicios críticos.
- En lo que respecta a los activos del tipo redes de comunicaciones, sobresalen los equipos router y switch administrables, mismos que fueron considerados como muy sensibles, debido a que no disponen de redundancias, y la prestación de servicios depende absolutamente de su disponibilidad. En este mismo grupo, el valor de trazabilidad también obtuvo una calificación importante, por cuanto, a criterio de los administradores, es vital reconocer quién accedió a sus configuraciones.
- Los activos del tipo soporte de información con los niveles de valor más altos, corresponden a los discos externos que almacenan los respaldos de los ordenadores de los funcionarios, las copias de seguridad de las cuentas de correo institucional y Sistema de Gestión Documental Quipux, así como los archivos de configuración de los equipos de red y servidor de Antivirus.
- Dentro del equipamiento auxiliar, destacan los Sistemas de Alimentación Ininterrumpida (UPS), situados en el Centro de Datos, los cuales abastecen a los servidores mencionados.
- En lo referente a los activos del tipo instalaciones, se consideran relevantes: el Centro de Datos, las Unidades que prestan servicios sensibles o críticos y las áreas donde se asientan los módulos de atención al público.

- Finalmente, obtuvieron altas valoraciones, los Usuarios internos (funcionarios), externos (ciudadanía) y administradores de red, dentro del tipo de activo denominado “Personal.”

4.2.2. Caracterización de las amenazas

Una vez identificados los recursos institucionales que requieren ser protegidos, resulta evidente la necesidad de conocer los factores que pueden afectarlos, en qué medida y con qué frecuencia. Para este cometido, se dispuso del inventario de amenazas descrito por la Metodología MAGERIT v3 en su Libro denominado “Catálogo de Elementos”, el cual facilitó las tareas de identificación y clasificación, mediante el uso de un lenguaje común en cuanto a las definiciones y terminología. La valoración de las amenazas encontradas, fue ejecutada en conjunto con los representantes de las Unidades Administrativas, con quienes se analizó y debatió respecto a los niveles de daño (Degradación) y probable materialización (Frecuencia) sobre los activos registrados en la tarea anterior, conforme lo señala la Metodología citada.

4.2.2.1. Identificación y Tipificación de las amenazas

MAGERIT v3 en su Libro “Catálogo de Elementos”, pone a disposición, un listado y descripción de las amenazas más recurrentes dentro de los ambientes de TI, mismas que se encuentran agrupadas en cuatro categorías en base a su origen: natural (catástrofes naturales), industrial (fuego, inundaciones, descargas eléctricas, rangos de temperatura y humedad inadecuadas, interferencias, etc.), por errores no intencionados del usuario (respecto al uso o configuración de los activos, alteración de datos, errores de mantenimiento o pérdida de equipos, agotamiento de recursos de hardware, etc.) y por ataques intencionados (difusión de malware, suplantación de identidad, abuso de privilegios ,alteración intencionada de datos, entre otros). Además, la Metodología atribuye a cada subconjunto de amenazas, un tipo de activos en específico, dependiendo de si, son afectados directamente o no. El resumen de esta distribución, se expone en el ANEXO 2 del presente proyecto, y corresponde a una adaptación del catálogo de amenazas descrita por MAGERIT v3 (Ministerio de Hacienda y Administraciones Públicas, 2012, pp.25-52).

4.2.2.2. Valoración de las amenazas

De acuerdo a MAGERIT v3 (Ministerio de Hacienda y Administraciones Públicas, 2012), la tarea de valoración de las amenazas, se basa en el análisis y estimación de su nivel de afectación sobre los activos, representado en las métricas siguientes:

- **Degradación:** se refiere al porcentaje del daño causado por una amenaza sobre un activo específico. Una degradación del 100%, representará la pérdida total del activo y una estimación del 1%, será tomada como irrelevante.
- **Probabilidad:** es la frecuencia en la que se estima, que una amenaza se pueda materializar. Desde muy frecuentes, para aquellas que se materializan o ejecutan diariamente, o poco frecuentes, para las que se cree que puedan presentarse cada varios años.

La Metodología propone las siguientes escalas de valoración, con el propósito de facilitar y estandarizar las estimaciones de Degradación y Frecuencia:

Tabla 14. Niveles de Degradación

Nivel	Degradación del Activo
MB (Muy Baja)	Daño del 1 % del activo
B (Baja)	Daño del 10 % del activo
M (Media)	Daño del 50 % del activo
A (Alta)	Daño del 80 % del activo
MA (Muy Alta)	Daño del 100 % del activo

Adaptación del Libro I de MAGERIT v3: Método, 2012

Tabla 15.Niveles de Frecuencia

Nivel	Frecuencia de materialización
PF (poco frecuente)	Cada varios años
FN (frecuencia normal)	Cada año (anual)
F (frecuente)	Mensual
MF (muy frecuente)	A diario

Adaptación del Libro I de MAGERIT v3: Método, 2012

De forma análoga a las secciones anteriores, la tarea de estimación de las métricas citadas, respondió a un proceso de recopilación y consenso de criterios entre el personal institucional e investigador, para establecer sus niveles cualitativos resultantes, mismos que se encuentran detallados en el ANEXO 1 ("ValAme_Salv") del presente proyecto. Sin embargo, para fines informativos, se ha visto necesario, resumir los resultados más relevantes en la Tabla siguiente:

Tabla 16. Resumen de Valoración de Amenazas

SERVICIOS [S]				
Tipo de Amenaza	**Nombre**	**Código**	**Nivel de Degradación**	**Nivel de Frecuencia**
Ataques intencionados	Suplantación de identidad	A.5	MA	PF
	Acceso no autorizado	A.11	MA	PF
	Denegación de servicio	A.24	MA	FN
DATOS [D]				
Tipo de Amenaza	**Nombre**	**Código**	**Nivel de Degradación**	**Nivel de Frecuencia**
Errores y Fallos no intencionados	Difusión de software dañino	E.8	A	MF
	Alteración de información	E.15	MA	PF
	Introducción de Información incorrecta	E.16	MA	FN
	Degradación de la Información	E.17	MA	PF
	Destrucción de la Información	E.18	MA	PF
	Vulnerabilidades del software	E.20	MA	FN
	Errores de Mantenimiento	E.21	MA	FN
Ataques intencionados	Manipulación de configuración	A.4	MA	PF
	Suplantación de identidad	A.5	MA	PF
	Difusión de software dañino	A.8	MA	PF
	Acceso no autorizado	A.11	MA	PF
	Modificación de información	A.15	MA	PF
	Introducción de falsa Información	A.16	MA	PF
	Corrupción de la Información	A.17	MA	PF
	Destrucción de la Información	A.18	MA	PF
	Manipulación programas	A.22	MA	PF
	Robo	A.25	MA	PF
APLICACIONES [SW]				
Tipo de Amenaza	**Nombre**	**Código**	**Nivel de Degradación**	**Nivel de Frecuencia**
De origen industrial	Avería física o lógica	I.5	MA	PF
Errores y Fallos no intencionados	Errores de los usuarios	E.1	B	MF
	Difusión de software dañino	E.8	A	MF
	Errores de Mantenimiento	E.21	MA	FN
Ataques intencionados	Manipulación de configuración	A.4	MA	FN

	Difusión de software dañino	A.8	MA	PF
	Acceso no autorizado	A.11	MA	PF
	Manipulación de programas	A.22	MA	PF
EQUIPOS INFORMÁTICOS [HW]				
Tipo de Amenaza	**Nombre**	**Código**	**Nivel de Degradación**	**Nivel de Frecuencia**
De origen industrial	Fuego	I.1	MA	PF
	Agua	I.2	MA	PF
Ataques intencionados	Denegación de Servicio	A.24	MA	PF
	Robo	A.25	MA	PF
REDES DE COMUNICACIÓN [COM]				
Tipo de Amenaza	**Nombre**	**Código**	**Nivel de Degradación**	**Nivel de Frecuencia**
De origen industrial	Fuego	I.1	MA	PF
	Agua	I.2	MA	PF
Ataques intencionados	Denegación de Servicio	A.24	MA	PF
	Robo	A.25	MA	PF
SOPORTES DE INFORMACIÓN [SI]				
Tipo de Amenaza	**Nombre**	**Código**	**Nivel de Degradación**	**Nivel de Frecuencia**
De origen natural	Fuego	N.1	MA	PF
	Agua	N.2	MA	PF
	Otros	N.*	MA	PF
De origen industrial	Fuego	I.1	MA	PF
	Avería física o lógica	I.5	MA	FN
Ataques intencionados	Robo	A.25	MA	PF
EQUIPAMIENTO AUXILIAR [AUX]				
Tipo de Amenaza	**Nombre**	**Código**	**Nivel de Degradación**	**Nivel de Frecuencia**
De origen industrial	Fuego	I.1	MA	PF
	Agua	I.2	MA	PF
Ataques intencionados	Robo	A.25	MA	PF
INSTALACIONES [L]				
Tipo de Amenaza	**Nombre**	**Código**	**Nivel de Degradación**	**Nivel de Frecuencia**
De origen natural	Fuego	N.1	A	PF
Ataques intencionados	Ataque destructivo	A.26	A	PF
	Ocupación enemiga	A.27	A	PF
PERSONAL [P]				
Tipo de Amenaza	**Nombre**	**Código**	**Nivel de Degradación**	**Nivel de Frecuencia**
Errores y Fallos no intencionados	Deficiencias de la organización	E.7	A	FN
Ataques intencionados	Indisponibilidad del personal	A.28	A	PF
	Ingeniería social	A.30	A	PF

Elaboración propia

De la tarea de caracterización de amenazas dentro del Ministerio del Trabajo (Ibarra), se pudo extraer las siguientes impresiones, basadas en el criterio de los evaluadores:

- Las amenazas del tipo ataques, relacionadas a suplantaciones de identidad, denegación del servicio, o acceso no autorizado, suponen una alta degradación sobre los activos, sin embargo, se concluyó en que su frecuencia de ejecución es relativamente baja.
- Por el contrario, las amenazas correspondientes a errores no intencionados, obtuvieron altas valoraciones, en cuanto a su nivel de ocurrencia o frecuencia, por cuanto, se estimó que en su mayoría se suscitan de forma diaria.
- Para la ponderación del punto anterior, se analizó el Sistema de Tickets institucional para soporte informático, el cual corroboró un alto índice de incidencias originadas por una inadecuada manipulación de los activos de información y la difusión accidental de software dañino.
- En el ámbito de amenazas no intencionadas, se concluyó también, que afectan con mayor periodicidad a los activos del tipo Datos y Aplicaciones, en relación al grupo de activos de Hardware.
- Las amenazas del tipo industrial y por catástrofes naturales, suponen una degradación muy alta sobre los activos, que contrasta con su nivel de probabilidad o frecuencia. A pesar de aquello, no deberían quedar totalmente desatendidas, y tendrían que gestionarse a medida de las posibilidades y prioridades de la institución.
- Deberán ser objeto de atención prioritaria, aquellas amenazas que hayan obtenido valores significativos tanto en degradación como frecuencia de manera simultánea, pues tienen mayores probabilidades de generar altos niveles de riesgo.
- Los niveles de degradación y frecuencia, darán una visión inicial del contexto de inseguridad al que se enfrentan los activos institucionales, sin embargo, estos valores no son determinantes y deberán cotejarse con otras métricas para determinar su real impacto, y riesgo asociado, como se analizará en el siguiente apartado.

4.3.Ejecución

En este apartado, se expone la implementación de las tareas restantes de la Metodología MAGERIT v3, necesarias para la obtención de los resultados finales, en cuanto a la estimación del estado del riesgo dentro del ámbito institucional que es objeto de estudio. Es decir, se muestra el proceso, los resultados y conclusiones obtenidas de la evaluación de los niveles de impacto y riesgo tanto intrínsecos, como residuales respecto a sus activos de información, y a la acción de las salvaguardas o medidas de protección con las que cuenta actualmente.

Finalmente, el apartado presenta la etapa cumbre del proyecto, la cual consiste en la creación del documento de Políticas de Seguridad de la información institucional, como propuesta planteada para gestionar los riesgos encontrados, en concordancia y alineamiento con los Controles y Objetivos establecidos por la Norma ISO/IEC 27002.

4.3.1. Estimación del impacto intrínseco

En la sección anterior, se definió la métrica degradación como el margen de daño ocasionado por una amenaza sobre un recurso específico, expresada en una escala cualitativa que oscila entre Muy Bajo a Muy Alto. Si este indicador es comparado con el nivel de valor estimado para cada uno de los activos, se obtendrá consecuentemente, el nivel de impacto ocasionado, mismo que es denominado del tipo intrínseco, debido a que su cálculo no contempla, el efecto de las medidas de seguridad o salvaguardas presentes en la institución (Ministerio de Hacienda y Administraciones Públicas, 2012).

Para facilitar esta tarea, MAGERIT v3 en su Libro III: Guía de Técnicas, establece el método de "Análisis de Tablas", que consiste en cotejar las variables mencionadas, relacionando sus niveles cualitativos en una tabla de dos entradas, tal como se indica a continuación:

Tabla 17.Cálculo del Impacto

IMPACTO		DEGRADACIÓN				
		MB(1%)	B(10%)	M(50%)	A(80%)	MA(100%)
VALOR ACTIVO	MA	M	A	A	MA	MA
	A	B	M	M	A	A
	M	MB	B	B	M	M
	B	MB	MB	MB	B	B
	MB	MB	MB	MB	MB	MB

Adaptación del Libro III de MAGERIT v3: Guía de Técnicas-Análisis de Tablas, 2012

De la Tabla anterior, se deduce fácilmente que un activo de muy alto valor para la organización, que sufra una degradación total (MA) o del 80 % (A), por parte de una amenaza específica, provocará un nivel de Impacto elevado (MA), y el mismo se irá intensificando o atenuando respecto a la comparación de las variables de entrada.

En este sentido, el cálculo del impacto dentro de la organización se basó en la comparación entre los valores de todos sus activos, respecto al nivel de degradación otorgado a cada una de las amenazas, que fueron definidas en la etapa de caracterización. Los resultados de esta tarea, se exponen en su totalidad, en el ANEXO 1("ValAct_RI") del presente proyecto, sin embargo, a modo ilustrativo, se cita el siguiente ejemplo:

Tabla 18.Ejemplo de cálculo del Impacto intrínseco

Activo Tipo Servicios	Amenaza	Dimensión [D]		
		Valor del Activo	Nivel de Degradación	NIVEL DE IMPACTO
Enlace de datos	Denegación del servicio [A.24]	MA	A	MA
Atención por multas coactivas	Suplantación de identidad [A.5]	MA	MA	MA
Atención para registro de denuncias	Acceso no autorizado [A.11]	MA	MA	MA
Atención por trámites Artesanales.	Ingeniería social [A.30]	A	A	A

Elaboración propia

4.3.2. Estimación del riesgo intrínseco

Según MAGERIT v3, el riesgo se deriva de la comparación entre el nivel de impacto generado por una amenaza y su frecuencia. El resultado es denominado intrínseco, puesto que, para su estimación no se toma en cuenta las medidas de protección o salvaguardas usadas por la organización.

De esta manera, se podrá cotejar el impacto que se origina de la relación entre el nivel de daño provocado por una amenaza (degradación) y el valor de un activo, versus la frecuencia en que dicha amenaza se pueda materializar (Ministerio de Hacienda y Administraciones Públicas, 2012).

Para este cometido, la Metodología utiliza la siguiente Tabla de dos entradas:

Tabla 19.Cálculo del Riesgo Intrínseco

RIESGO INTRÍNSECO		FRECUENCIA			
		PF	FN	F	MF
IMPACTO	MA	A	MA	MA	MA
	A	M	A	MA	MA
	M	B	M	A	MA
	B	MB	B	M	A
	MB	MB	MB	B	M

Adaptación del Libro III de MAGERIT v3: Guía de Técnicas-Análisis de Tablas, 2012

Los resultados de la estimación del riesgo intrínseco en la institución que es objeto de este estudio, se detallan en el ANEXO 1 ("ValAct_RI" y "ReporteFinal") del presente documento, sin embargo, se expone el siguiente ejemplo, para fines demostrativos:

Tabla 20.Ejemplo de cálculo del Riesgo Intrínseco

Activo Tipo Servicios	Amenaza	Dimensión [D]		
		Nivel de Impacto	Frecuencia	NIVEL DE RIESGO INTRÍNSECO
Enlace de datos	Denegación del servicio [A.24]	MA	FN	MA
Atención por multas coactivas	Suplantación de identidad [A.5]	MA	PF	A
Atención para registro de denuncias	Acceso no autorizado [A.11]	MA	PF	A
Atención por trámites Artesanales.	Ingeniería social [A.30]	A	PF	M

Elaboración propia

4.3.3. Caracterización de las salvaguardas

Desde un punto de vista global, será fundamental que el estudio del estado del riesgo en una organización, incluya una evaluación de las medidas de protección con las que cuenta ese momento, con el fin de identificar los puntos débiles respecto su nivel de gestión de la seguridad de la información, y motivar la ejecución de acciones para fortalecerlos.

Dentro del contexto de la Metodología en estudio, esta tarea también será necesaria para determinar los niveles de impacto y riesgo residual, que son valores más precisos, debido a que su estimación, si toma en cuenta la efectividad de las medidas de protección o salvaguardas vigentes en la organización, a fin de determinar su real estado de seguridad.

4.3.3.1. Identificación de las salvaguardas vigentes

MAGERIT v3 categoriza las salvaguardas según el efecto o acción que producen sobre las amenazas identificadas, como se explica a continuación:

- Salvaguardas limitantes: su objetivo es limitar el nivel de daño ocasionado por la materialización de una amenaza, por ende, se encuentra enfocada en mitigar el nivel de degradación sobre un activo.
- Salvaguardas preventivas: permiten reducir la probabilidad de ocurrencia de las amenazas, es decir, su acción se basa en minimizar la frecuencia de las mismas (Ministerio de Hacienda y Administraciones Públicas, 2012).

4.3.3.2. Valoración de las salvaguardas vigentes

La Metodología valora las salvaguardas, de acuerdo a su grado de efectividad, que será evaluado en base a la siguiente escala cualitativa:

Tabla 21. Grado de efectividad de las Salvaguardas

Grado de Efectividad	Descripción
No existe (NE)	No se ha implantado ninguna salvaguarda
Poca efectividad (PE)	La salvaguarda tiene un impacto indirecto sobre la amenaza.
Efectiva (E)	La salvaguarda reduce la frecuencia o el impacto de la amenaza.
Muy efectiva (ME)	Salvaguarda específicamente diseñada para la amenaza.

Adaptación del Libro I de MAGERIT v3: Método, 2012

Para la ejecución de la tarea de caracterización de salvaguardas, se necesitó de la participación activa de los administradores de red y del responsable de la Dirección Administrativa Financiera, con el fin de identificar y constatar las medidas de protección con las que cuenta la institución, tanto a nivel técnico como organizativo, a través de reuniones e inspecciones de forma conjunta. La valoración de las mismas, requirió el consenso de criterios entre los participantes mencionados y el investigador, para determinar el nivel de efectividad de cada una de las salvaguardas encontradas, en base a la escala de la Tabla 21 y a la información referente a los activos y amenazas, recopilada anteriormente (ANEXO 1:"ValAct_RI" y ANEXO 2).

De esta manera, en el ANEXO 1 (“Salvaguardas”) del presente documento, se expone el listado de las contramedidas que fueron identificadas, su nivel de efectividad o carencia, y su relación con los diversos tipos de activos y amenazas que corresponden al entorno de la institución. En la Tabla siguiente, se presenta un resumen de las principales salvaguardas encontradas:

Tabla 22.Resumen Salvaguardas-Ministerio del Trabajo (Ibarra)

Amenaza	Tipo de Activo Afectado	SALVAGUARDA		
		Descripción	Tipo	Nivel Efectividad
Fuego [I.1]	Equipos Informáticos Redes de Comunicación Soportes de Información Equipamiento Auxiliar Instalaciones	Centro de datos: extinguidores de Clase A Recomendación: uso de pintura retardante Oficinas: extinguidores de Clase A Recomendación: implantación de un Sistema de extinción de incendios.	Limitante	PE
Contaminación mecánica [I.3] Avería de origen físico o lógico [I.5]	Equipos Informáticos Redes de Comunicación Soportes de Información Equipamiento Auxiliar	Equipos del Centro de datos: Programa anual de mantenimiento. Equipos de funcionarios: Programa semestral de mantenimiento preventivo y correctivo.	Preventiva-Limitante	E
Corte del suministro eléctrico [I.6]	Equipos Informáticos Redes de Comunicación Equipamiento Auxiliar	Equipos del Centro de datos: UPS de 18 KVA Equipos de funcionarios: Reguladores de voltaje	Preventiva	PE
Condiciones inadecuadas de temperatura/humedad [I.7]	Equipos Informáticos Redes de Comunicación Soportes de Información Equipamiento Auxiliar	Centro de Datos: Aire acondicionado tipo split de 12000 BTU. Recomendación: Sistema de Climatización de precisión.	Preventiva-Limitante	PE
Interrupción de otros servicios y suministros esenciales [I.9]	Equipamiento Auxiliar	Adquisición de suministros a inicio de año. Recomendación: Procesos definidos de adquisición y ejecución de un POA (Plan Operativo Anual).	Preventiva	PE
Errores de los usuarios [E.1]	Servicios Datos Aplicaciones	Respaldos de datos y correo. Validaciones en los sistemas institucionales.	Limitante	E
Deficiencias en la organización [E.7]	Personal	Estructura orgánica y funcional del personal (manuales)	Preventiva	E

Difusión de software dañino [E.8]	Datos Aplicaciones	Antivirus institucional (Kaspersky). Firewall corporativo Sophos Firewall de Windows.	Preventiva-Limitante	E
Escapes de información [E.14]	Datos	Credenciales de acceso a los sistemas. Niveles de privilegios según los roles. Cierre automático de sesiones.	Preventiva	E
Alteración de la información [E.15] Introducción de información incorrecta [E.16]	Datos	Validaciones en los sistemas institucionales.	Preventiva	E
Destrucción de la información [E.18]	Datos	Respaldos de datos y correo.	Limitante	E
Vulnerabilidades de los programas [E.20]	Datos Aplicaciones	Actualización del software. Mantenimiento preventivo y correctivo del Software. Recomendación: Políticas sobre el uso apropiado de las aplicaciones y cuentas.	Preventiva-Limitante	PE
Errores de mantenimiento/actualización (software) [E.21]	Datos Aplicaciones	Uso de Instructivos del fabricante.	Preventiva	PE
Errores de mantenimiento/actualización (hardware) [E.23]	Equipos Informáticos	Manuales para mantenimiento de equipos. Programa semestral de mantenimiento preventivo y correctivo.	Preventiva-Limitante	E
Manipulación de la configuración [A.4] Abusos de privilegios de acceso [A.6] Acceso no autorizado [A.11] Modificación de información [A.15] Introducción de falsa información [A.16] Destrucción de la información [A.18] Manipulación de programas [A.22]	Servicios Datos Aplicaciones Equipos Informáticos Redes de Comunicación	Credenciales de acceso a los sistemas. Niveles de privilegios según los roles.	Preventiva	E
Difusión de software dañino [A.8]	Datos Aplicaciones	Firewall Corporativo Sophos Antivirus Kaspersky	Preventiva	PE

Robo [A.25]	Datos Equipos Informáticos Redes de Comunicación Soportes de Información Equipamiento Auxiliar	Centro de Datos: cerraduras manuales. Recomendación: Sistema biométrico de control de acceso. Oficinas: Guardianía privada y sistema de video vigilancia en planta baja.	Preventiva	PE
Ataque destructivo [A.26]	Equipos Informáticos Redes de Comunicación Soportes de Información Equipamiento Auxiliar Instalaciones	Centro de Datos: cerraduras manuales. Recomendación: Sistema biométrico de control de acceso. Oficinas: Guardianía privada y sistema de video vigilancia en planta baja.	Preventiva	PE
Indisponibilidad del personal [A.28]	Personal	Reglamento interno	Preventiva	E

Elaboración propia

De la tarea de caracterización de las salvaguardas dentro del Ministerio del Trabajo (Ibarra), se pudo extraer las siguientes conclusiones, basadas en el criterio de los evaluadores:

- A nivel general, la institución evidencia grandes falencias en sus mecanismos de protección de la información y de los recursos que la gestionan, tanto a nivel de procesos, tecnología y personas.
- La organización utiliza herramientas tecnológicas tradicionales como el servidor de antivirus Kaspersky y Firewall Sophos, para contrarrestar la difusión de malware y realizar filtrado de contenido. Sin embargo, su administración depende de matriz y a criterio de los analistas de red, las soluciones tienen un alcance limitado, en cuanto a la mitigación de amenazas más sofisticadas, ataques internos y a la gestión de vulnerabilidades en las personas.
- Se evidenció debilidades importantes en cuanto al control del acceso físico al Data Center, el cual carece de mecanismos electrónicos o biométricos de seguridad, y su protección depende de cerraduras manuales.
- El Data Center cuenta con herramientas básicas y no estandarizadas, para mitigar aquellas amenazas de origen industrial como: incidentes por incendios, inundaciones, fallos eléctricos, así como aquellas de origen ambiental. Es decir, su protección se basa en la utilización de extintores, UPS de poca capacidad de respaldo de energía y aires acondicionados de baja precisión.
- La entidad no cuenta con salvaguardas de carácter organizacional, que permitan definir los procesos relacionados a las tareas de mantenimiento, adquisición y baja de equipos tecnológicos, o para la obtención de licencias y actualizaciones de las aplicaciones.
- Adicionalmente, la institución carece de procesos para la gestión de copias de seguridad, redundancias y migración a nuevas tecnologías.
- Un aspecto a considerar, fue la ausencia de medidas administrativas para gestionar los errores no intencionados por parte de los funcionarios y administradores, en cuanto a la manipulación de los datos y sus recursos tecnológicos.
- En este mismo contexto, la organización no tiene definidos los lineamientos necesarios para asegurar que los funcionarios no sean víctimas de ataques por suplantación de identidad, ingeniería social y demás acciones que saquen provecho de su vulnerabilidad.

- Finalmente, esta evaluación permitió despertar el interés de las autoridades, por gestionar las deficiencias encontradas, por lo que manifestaron su compromiso y respaldo a la presente propuesta y la apertura para la ejecución de futuros proyectos de gestión del riesgo.

4.3.4. Estimación de la degradación y frecuencia residual

Esta tarea consiste básicamente en tomar los valores de Degradación y Frecuencia obtenidos del proceso de Caracterización de Amenazas descrito anteriormente, y contrastarlos con los niveles de efectividad de las salvaguardas identificadas. Los niveles de Degradación serán cotejados con los valores de efectividad de las salvaguardas limitantes, mientras que la Frecuencia deberá compararse con las salvaguardas preventivas. Los resultados obtenidos, serán denominados efectivos o residuales (Ministerio de Hacienda y Administraciones Públicas, 2012).

La estimación de dichas métricas, también se efectúa mediante el Análisis de Tablas de dos entradas, como se expone a continuación:

Tabla 23. Degradación Residual

DEGRADACIÓN RESIDUAL		**EFECTIVIDAD SALVAGUARDA LIMITANTE**			
		NE	**PE**	**E**	**ME**
DEGRADACIÓN	**MA**	MA	A	M	B
	A	A	M	B	B
	M	M	B	MB	MB
	B	B	MB	MB	MB
	MB	MB	MB	MB	MB

Adaptación del Libro III de MAGERIT v3: Guía de Técnicas, 2012

Tabla 24. Frecuencia Residual

FRECUENCIA RESIDUAL		**EFECTIVIDAD SALVAGUARDA PREVENTIVA**			
		NE	**PE**	**E**	**ME**
FRECUENCIA	**MF**	MF	F	FN	PF
	F	F	FN	PF	PF
	FN	FN	PF	PF	PF
	PF	PF	PF	PF	PF

Adaptación del Libro III de MAGERIT v3: Guía de Técnicas, 2012

La estimación de la Degradación y Frecuencia Residual, se detalla en el ANEXO 1 (“RiesgoR”), sin embargo, a modo ilustrativo, se cita el siguiente ejemplo:

Tabla 25.Ejemplo de estimación de la Degradación y Frecuencia Residual

Activo de Tipo Aplicaciones	Amenaza	SALVAGUARDA		Dimensión [I]			
		Tipo	Efectividad	Deg.	Deg R	Frec.	Frec. R
Sistema Único del Trabajo (SUT)	E.8 (Difusión software dañino)	Preventiva y Limitante	E	A	B	MF	FN
Sistema Nacional de Control de Inspectores (SINACOI)	E.1 (Errores de los usuarios)	Limitante	E	B	MB	MF	MF
Sistema Informático Integrado de Talento Humano (SIITH)	A.4 (Manipulación configuración)	Preventiva	E	MA	MA	FN	PF
Software de ofimática	E.4 (Errores de configuración)	No existe	NE	A	A	PF	PF

Elaboración Propia

4.3.5. Estimación del impacto y riesgo residual

Corresponde a la tarea final de la Metodología, la cual nos permitirá conocer finalmente los resultados efectivos de impacto y riesgo presentes en el ámbito de estudio, que servirán de sustento para la toma de decisiones dirigidas a su gestión o tratamiento.

Para la estimación de estas métricas, se usará nuevamente las Tablas que fueron empleadas para el cálculo del impacto y riesgo intrínseco (Tablas 17 y 19), pero en esta ocasión, se tomará en cuenta los niveles de Degradación y Frecuencia Residuales. En el ANEXO 1 (“RiesgoR”), se detalla esta tarea, y se resumen los resultados obtenidos, en la Hoja de Cálculo denominada “ReporteFinal”. A continuación, se cita un ejemplo, donde se divisan los niveles de riesgo intrínseco y residual, encontrados en la institución:

Tabla 26.Ejemplo de cálculo del Riesgo Residual

Activo de Tipo Aplicaciones	Amenaza	SALVAGUARDA		Dimensión [I]					
		Tipo	Efectividad	Deg.	Deg R	Frec.	Frec. R	RI	RR
Sistema Único del Trabajo (SUT)	E.8 (Difusión software dañino)	Preventiva y Limitante	E	A	B	MF	FN	MA	A
Sistema Nacional de Control de Inspectores (SINACOI)	E.1 (Errores de los usuarios)	Limitante	E	B	MB	MF	MF	MA	MA
Sistema Informático Integrado de Talento Humano (SIITH)	A.4(Manipulación configuración)	Preventiva	E	MA	MA	FN	PF	A	M
Software de ofimática	E.4 (Errores de configuración)	No existe	NE	A	A	PF	PF	A	A

Elaboración Propia

4.3.6. Análisis de resultados de la aplicación de la Metodología MAGERIT v3

Mediante su implementación se ha podido responder a las interrogantes: ¿Qué recursos de información requieren ser protegidos?, y ¿De qué factores se los debe proteger?, es decir se ha conseguido identificar aquellos recursos cuyos índices de Riesgo alcanzan niveles altos o muy altos (se los ha denominado Activos Críticos) y se ha podido identificar las Amenazas, que los sitúan en dicha posición (Amenazas Resultantes). Además, se definió responsables o custodios para cada uno de los activos críticos encontrados, a fin de establecer una medida de control adicional. Estos resultados se exponen a detalle, en el ANEXO 3 ("ActCríticovsResp" y "AmeResul") del presente proyecto, sin embargo, en la Tabla siguiente, se exponen algunos de los datos más relevantes:

Tabla 27.Resumen de resultados-MAGERIT

SERVICIOS		
Activo Crítico	**Riesgo**	**Amenaza Resultante**
Servicio-Enlace Datos (CNT)	MA	E.24 (Caída por agotamiento de recursos) A.24 (Denegación de servicio)
Atención a usuarios por multas coactivas		
Atención a usuarios para ingreso de vistos buenos.		
Atención a usuarios para inscripción de inspecciones.		
Atención a usuarios para legalización de Contratos y Actas de finiquito		
Atención a usuarios para legalización de Décimos y Utilidades		
DATOS		
Activo Crítico	**Riesgo**	**Amenaza Resultante**
Contratos sector privado y público	MA	E.1 (Errores de los usuarios) E.2 (Errores Administrador) E.19 (Divulgación Información) E.21 (Errores Mantenimiento)
Registros de Denuncias empleados sector público y privado		
Registros de pago de multas y consignaciones		
Registros de inspecciones integrales		
Registros de Décimos y utilidades		
APLICACIONES		
Activo Crítico	**Riesgo**	**Amenaza Resultante**
Sistema Único del Trabajo (SUT)-Contratos y Actas	A	E.1 (Errores de los usuarios) E.2 (Errores Administrador)
Sistema Nacional de Control de Inspectores(SINACOI)-Módulo Décimos y Utilidades		
Sistema Nacional de Control de Inspectores(SINACOI)-Módulo Registro de inspecciones integrales		
SINACOI-Módulo Financiero-Pago multas		
SUT-Módulo Registro Denuncias		

EQUIPOS INFORMÁTICOS		
Activo Crítico	**Riesgo**	**Amenaza Resultante**
Servidor Antivirus (Kaspersky) Servidor cámaras (NUUO)	MA	E.2 (Errores Administrador) E.4 (Errores de configuración)
REDES DE COMUNICACIÓN		
Activo Crítico	**Riesgo**	**Amenaza Resultante**
Router (enlace de datos CNT) Switch capa 2 (marca Avaya 3526T PWR+) Switch capa 2 (marca 3COM 4228G) Switch no administrable (marca D-link DES1024A) Central telefónica híbrida (marca Avaya)	MA	I.8 (Fallo servicios Comunicaciones) E.2 (Errores Administrador) E.4 (Errores de configuración)
EQUIPAMIENTO AUXILIAR		
Activo Crítico	**Riesgo**	**Amenaza Resultante**
Fuentes de Alimentación (servers) Sistemas de Alimentación Ininterrumpida (servers)	A	I.1 (Fuego) I.2 (Agua) A.11 (Acceso no autorizado)
INSTALACIONES		
Activo Crítico	**Riesgo**	**Amenaza Resultante**
Centro de Datos Puntos de atención al público	A	N.* (Otros) A.26 (Ataque destructivo) A.27 (Ocupación enemiga)
PERSONAL		
Activo Crítico	**Riesgo**	**Amenaza Resultante**
Usuarios externos Funcionarios	A	E.28 (Indisponibilidad del personal) A.30 (Ingeniería social)

Elaboración Propia

Finalmente, se citan algunas impresiones originadas en el transcurso del proceso de Análisis del Riesgo efectuado, desde un punto de vista global:

- Su implementación precisó la autorización, aprobación y seguimiento del Director Regional, con el fin de contar con los recursos necesarios para planificar las inspecciones y reuniones virtuales con el personal, y obtener el acceso a sus documentos institucionales.
- Se requirió la planificación de varias reuniones con los funcionarios y Coordinadores de las Unidades Administrativas, las cuales fueron comunicadas por varios canales institucionales, como correo y Sistema de Gestión Documental Quipux.
- A criterio de los evaluadores, los Datos resultaron ser más sensibles en su integridad, respecto a las dimensiones de disponibilidad y confidencialidad.

- Según el criterio de los evaluadores, las dimensiones de Confidencialidad y Disponibilidad en los Datos, son muy vulnerables, sin embargo, una violación de su integridad, provocaría mayores pérdidas a nivel organizacional y de sus usuarios externos (ciudadanía).
- A criterio de los administradores de red, es más importante estar al tanto de: "quién accedió a los servicios" (Autenticación del Servicio) y determinar "cuál es el origen de los datos" (Autenticación de los Datos), en relación al conocimiento de: "lo que hizo el usuario" (Trazabilidad).
- Un activo de alto valor para la organización, muy probablemente genere niveles considerables de impacto y riesgo.
- Los activos del tipo Datos con niveles de riesgo elevados, provienen de los servicios críticos institucionales, es decir de aquellos vinculados con el core de la institución.
- Las amenazas del tipo: "Errores no intencionados del usuario y "Errores del Administrador", provocan índices de riesgo muy alto respecto a los Datos (MA) y alto (A) en las Aplicaciones, debido a que la institución no cuenta con medidas administrativas que orienten las tareas de sus funcionarios.
- A criterio de los evaluadores, las salvaguardas destinadas a gestionar la autenticación y los niveles de privilegio, para el uso y acceso a las Aplicaciones, han servido para atenuar sus niveles de riesgo, por lo que, este tipo de activos no están considerados como críticos, sin embargo, sus niveles aún son altos.
- Tanto los Equipos Informáticos como los recursos destinados a mantener disponible la red y los servicios institucionales (Servers y equipos activos de comunicaciones), obtuvieron índices muy altos de riesgo (MA), respecto a las amenazas del tipo: "Errores del Administrador" y "Errores de Configuración".
- El equipamiento auxiliar que arrojó valores altos de riesgo (A), está representado por los dispositivos UPS (Sistemas de Alimentación Ininterrumpida) y las fuentes de alimentación, que realizan el abastecimiento de energía a los servidores de antivirus y cámaras. Además, los activos del tipo Soportes de Información, alcanzaron niveles medios de riesgo (M), por tanto, no forman parte del grupo de activos críticos.
- En referencia a los activos del tipo Instalaciones, los evaluadores consideraron al Centro de Datos institucional y los puntos de atención al público, como espacios con un alto valor de riesgo (A).

- Respecto a los activos del grupo denominado “Personal”, los funcionarios obtuvieron niveles de riesgo importantes, puesto que son quienes hacen uso de la información institucional, considerada el recurso más relevante para la consecución de los objetivos organizacionales. En este mismo ítem, los usuarios externos también fueron altamente valorados, debido a que son los receptores de los servicios y por ende representan la razón de ser de esta Cartera de Estado.
- Adicionalmente, las amenazas del tipo: “Errores no intencionados del usuario”, “Errores del Administrador”, “Errores de configuración” e “Ingeniería social”, son recurrentes y suponen índices de riesgo elevado.
- Estas premisas reafirman la necesidad de implantar medidas administrativas en pro del fortalecimiento del ámbito de las personas, lo cual se alinea con el propósito principal de este proyecto, el cual persigue instaurar políticas destinadas a orientar sus tareas y comportamiento.

4.3.7. Definición de Políticas de Seguridad de la Información en base a la Normativa ISO/IEC 27002 para el Ministerio del Trabajo (Ibarra)

El estudio del estado del riesgo dentro del sistema de información del ámbito de estudio, reveló la existencia de potenciales riesgos directamente relacionados con errores en la ejecución de las tareas de sus funcionarios y administradores, en cuanto al manejo de información reservada, uso del equipamiento y de los servicios de red, errores en la configuración de los recursos de hardware y software, entre otras acciones, que han podido ser identificadas y visibilizadas mediante el listado de amenazas resultantes, que arrojó la Metodología MAGERIT(ANEXO 3: “AmeResul”). Adicionalmente, se ha podido constatar una creciente demanda de peticiones e incidencias, derivadas de la incorrecta manipulación de sus activos, mismas que se encuentran registradas en su sistema de gestión de tickets (GLPI). Estas condiciones desfavorables, demandan la debida regulación de sus tareas y comportamiento, con el propósito de generar una cultura organizacional involucrada y consciente con la seguridad de la información. Bajo esta premisa, se ha elaborado el siguiente documento de Políticas de Seguridad de la Información, el cual recopila un conjunto de lineamientos, en conformidad al marco establecido por la Normativa ISO/IEC 27002.

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA EL MINISTERIO DEL TRABAJO (IBARRA)

DATOS DE ELABORACIÓN

	NOMBRE Y APELLIDO/CARGO	FECHA APROBACIÓN	FIRMA
Aprobación:	Ab. William Tréboles B. Director Regional		
Revisión:	Ing. Alexandra Elizabeth Quinchuquí S. Especialista de TIC		
Elaboración:	Ing. Mario Andrés Cevallos M. Asistente de TIC		

I. OBJETIVO DEL DOCUMENTO

El presente documento recoge los lineamientos que deben cumplir los funcionarios del Ministerio del Trabajo en su sede de la ciudad de Ibarra, así como sus proveedores de servicios internos o externos, con el fin de mantener niveles adecuados de disponibilidad, integridad y confidencialidad en sus recursos de información.

II. ÁMBITO DE APLICACIÓN

El campo de acción en el que trasciende la presente guía atañe:

- A todos los funcionarios de ésta Cartera de Estado, usuarios externos, suministradores y visitantes en general.
- A todos los recursos de información institucionales, incluyendo sus instalaciones físicas.
- A toda la información física o digital, gestionada por el Ministerio del Trabajo (Ibarra), dentro de sus competencias.

III. GENERALIDADES

- Esta guía pretende llevar un lenguaje sencillo, evitando terminología de carácter técnico, de modo que sea entendido por cualquier involucrado.
- El documento será difundido dentro de la organización de manera oportuna y por varios canales de comunicación, para garantizar su fiel cumplimiento.
- Quien haga uso de los activos de información del Ministerio del Trabajo (Ibarra), deberá aceptar los lineamientos establecidos en el presente documento, y el eventual desconocimiento de sus preceptos, no lo exoneran de su responsabilidad, ante cualquier incidente de seguridad.
- Las Políticas pueden estar sujetas a modificaciones, siempre y cuando mantengan la debida concordancia con los objetivos de seguridad institucional y sean comunicadas oportunamente.

IV. ROLES

ROL	DESCRIPCIÓN
Máxima autoridad o su delegado	Su representante es el Director Regional del Trabajo o su delegado. Es el encargado de la aprobación del documento de políticas.
Gestor de Seguridad (investigador)	Responsable del desarrollo y presentación de la propuesta, así como de la difusión del documento de políticas.
Comité de Gestión de la Seguridad de la Información Institucional	Equipo integrado por un responsable de cada Unidad Organizacional, designado por el Director Regional.
Unidad de TIC (Tecnologías de la Información y Comunicaciones)	Unidad Organizacional del Ministerio del Trabajo (Ibarra), responsable del Servicio de Mesa de Ayuda (nivel 1), así como de los procesos de mantenimiento de equipos informáticos y software.
Administradores de red	Personal técnico de la Dirección de TIC (matriz), encargado de la gestión de la red del Ministerio del Trabajo a nivel nacional.
Funcionarios, usuarios externos y terceras personas	Fiel cumplimiento de la normativa.

V. VIGENCIA

Los lineamientos establecidos en el presente documento, estarán vigentes desde su aprobación por parte de la máxima autoridad, y tendrán que ser revisados y/o actualizados conforme las necesidades institucionales y exigencias de su entorno.

VI. BASE LEGAL

La base legal de la presente guía, se sustenta en los Dominios, Objetivos de control y Controles de la Normativa ISO/IEC 27002, los cuales han sido seleccionados en conformidad con las decisiones de la organización, respecto a sus criterios de aceptación y tratamiento del riesgo.

DOMINIOS PARA LA PROPUESTA

En esta sección se exponen los **DOMINIOS,** Objetivos de Control y *Controles,* seleccionados para la propuesta de Políticas institucionales, los cuales han sido enumerados de acuerdo a la guía original. Cabe indicar que, por decisiones de la organización, las cuales obedecen a sus necesidades o requerimientos, no se han considerado los Dominios 10 y 14, destinados para el cifrado de datos y desarrollo del software respectivamente.

5. POLÍTICAS DE SEGURIDAD.
5.1 Directrices de la Dirección en seguridad de la información.
5.1.1 Conjunto de políticas para la seguridad de la información.
5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN
6.1 Organización interna.
6.1.1 Asignación de responsabilidades para la seguridad de la información.
6.2 Dispositivos para movilidad y teletrabajo.
6.2.1 Política de uso de dispositivos para movilidad.
6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
7.1 Antes de la contratación.
7.1.1 Investigación de antecedentes
7.1.2 Términos y condiciones de contratación.
7.2 Durante la contratación.
7.2.1 Responsabilidades de gestión.
7.2.2 Concienciación, educación y capacitación en segur. de la información
7.2.3 Proceso disciplinario.
7.3 Cese o cambio de puesto de trabajo
7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.
8.1 Responsabilidad sobre los activos.
8.1.1 Inventario de activos.
8.1.2 Propiedad de los activos.
8.1.3 Uso aceptable de los activos.
8.1.4 Devolución de activos.
8.2 Clasificación de la información.
8.2.1 Directrices de clasificación.
8.2.2 Etiquetado y manipulado de la información.
8.3 Manejo de los soportes de almacenamiento.
8.3.1 Gestión de soportes extraíbles.

9. CONTROL DE ACCESO
9.1 Requisitos de negocio para el control de acceso
9.1.1 Política de control de acceso
9.1.2 Control de acceso a las redes y servicios asociados.
9.2 Gestión de acceso de usuario.
9.2.1 Gestión de altas/bajas en el registro de usuarios.
9.3 Responsabilidades del usuario.
9.3.1 Uso de información confidencial para la autenticación.
9.4 Control de acceso a sistemas y aplicaciones.
9.4.1 Restricción del acceso a la información.

11. SEGURIDAD FÍSICA Y AMBIENTAL
11.1 Áreas seguras.
11.1.1 Controles físicos de entrada.
11.1.2 Seguridad de oficinas, despachos y recursos.
11.1.3 Protección contra las amenazas externas y ambientales.
11.2 Seguridad de los equipos.
11.2.1 Emplazamiento y protección de equipos.
11.2.2 Mantenimiento de los equipos.
11.2.3 Salida de activos fuera de las dependencias de la empresa.

11.2.4 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.
12.1 Responsabilidades y procedimientos de operación.
12.1.1 Documentación de procedimientos de operación.
12.2 Protección contra código malicioso.
12.2.1 Controles contra el código malicioso.
12.3 Copias de seguridad.
12.3.1 Copias de seguridad de la información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.
13.1 Gestión de la seguridad en las redes.
13.1.1 Controles de red.

15. RELACIONES CON SUMINISTRADORES.
15.1 Seguridad de la información en las relaciones con suministradores.
15.1.1 Política de seguridad de la información para suministradores.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
16.1 Gestión de incidentes de seguridad de la información y mejoras.
16.1.1 Responsabilidades y procedimientos.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
17.1 Continuidad de la seguridad de la información.
17.1.1 Planificación de la continuidad de la seguridad de la información.

18. CUMPLIMIENTO.
18.1 Cumplimiento de los requisitos legales y contractuales.
18.1.1 Cumplimiento de las políticas y normas de seguridad.
18.1.2 Identificación de la legislación aplicable.

VII. GLOSARIO

Término/Abreviatura	Descripción
Activo	Cualquier recurso de valor para la organización.
Activo crítico	Recurso esencial para el cumplimiento de las metas organizacionales. Su vulneración supondría un grave perjuicio institucional.
Activo de información	Elemento de un sistema de información involucrado con el tratamiento de los datos. Incluye: servicios, aplicaciones, equipos informáticos y de redes, soportes de almacenamiento, recursos humanos, entre otros.
Amenaza	Cualquier factor con condiciones para explotar una debilidad y generar daños a un activo de información.
Antivirus	Herramienta de hardware o software con el potencial para identificar y eliminar software dañino en un equipo o sistema informático.
Archivo ejecutable	Archivo que contiene una secuencia de instrucciones para iniciar una aplicación o programa.
Bitácora	Recopila eventos, tareas o actividades de forma diaria, semanal o mensual.

Centro de Datos	Espacio físico centralizado, donde se alojan los equipos de TI, destinados a la prestación de servicios de red de una organización.
Cibercafé	Establecimiento comercial donde se ofrece acceso a internet, al público en general.
Cifrado de datos	Permite convertir la información a un formato ilegible para personas no autorizadas.
Conexión remota	Permite acceder a un ordenador, desde una locación externa, usando la conectividad y prestaciones del Internet.
Confidencialidad	Garantiza que los recursos de información estén protegidos del acceso y uso no autorizado, sea éste de manera intencional o accidental.
Contraseña	Conjunto de caracteres confidenciales, necesario para acceder a un determinado servicio o recurso informático.
Controles	Medidas de protección de carácter técnico u organizacional, empleadas para mitigar el riesgo.
Controles físicos	Medidas tangibles de control, que actúan frente a amenazas físicas que afectan el hardware.
Controles lógicos	Medidas basadas en software para limitar el acceso a los datos.
Credenciales de acceso	Corresponde al nombre de usuario y la clave que lo acompaña, para el acceso a un determinado sistema o aplicación.
Datos	Representa la información que manejan las personas para la prestación de servicios y se almacena en forma impresa o digital.
Disco duro	Dispositivo de almacenamiento de datos digitales, en un ordenador.
Disponibilidad	Asegura que los usuarios autorizados accedan a los recursos de información en todo momento.
Divulgación	Se refiere al acto de dar a conocer información y ponerla al alcance de terceras personas.
Equipo informático, computador u ordenador	Componente electrónico encargado de almacenar y procesar la información, con el uso de programas y aplicaciones.
Escritorio remoto	Herramienta para el acceso de un ordenador a otro, ubicado en una locación o red diferente.
Espía	Código malicioso cuyo objetivo es recopilar información de un ordenador, de forma no autorizada.
Evaluación del riesgo	Valora la probabilidad y consecuencias de la materialización de una amenaza sobre un activo.
Evento de seguridad de la información	Suceso que puede provocar un problema de seguridad en una organización, el cual, no necesariamente generará una interrupción de sus servicios.
Firewall	Elemento de hardware o software encargado de permitir o denegar conexiones a un equipo o red privada, con la finalidad de evitar accesos no autorizados.
GLPI (Gestionnaire libre de parc informatique)	Plataforma de gestión de incidencias tecnológicas, basada en software libre.

Gusano	Tipo de software malicioso, que se replica así mismo, para expandirse en diferentes ubicaciones del ordenador, con el propósito de colapsarlos.
Help desk	Servicio de soporte tecnológico, para la resolución de incidencias y gestión de requerimientos.
HTTPS (Hyper Text Transfer Protocol Secure)	Protocolo de comunicación mediante el cual, se accede a un sitio web de forma segura y privada.
IEC (International Electrotechnical Commission)	La Comisión Electrotécnica Internacional, es la organización encargada de la creación y publicación de normativas internacionales dentro del ámbito: eléctrico, electrónico y tecnologías relacionadas.
Incidente de seguridad de la información	Evento que afecta de forma negativa el negocio y provoca una interrupción de su servicio.
Información	Es el principal activo de una organización, necesario para sus operaciones diarias.
Información sensible	Es la información de carácter reservado, que posee un individuo u organización, misma que debe ser protegida de accesos no autorizados.
Integridad	Garantiza que la información no sea alterada o modificada, sin autorización.
Intranet	Es una red de carácter privado, que utiliza su conectividad para compartir información o servicios dentro de una organización.
ISO (International Organization for Standardization.)	Entidad internacional destinada a la creación de normas para el correcto suministro de bienes y servicios.
Malware o software malicioso	Abreviación de “malicious software”. Son programas malintencionados que intentan vulnerar los sistemas y recursos tecnológicos.
Navegador	Aplicación que habilita el acceso a la información de una página web, generalmente con el uso de Internet, y desde ordenadores o dispositivos móviles.
Política de seguridad de la información	Es una serie de directrices declaradas de manera formal, que regulan el uso de la información y sus recursos.
Proceso	Tareas relacionadas entre sí, para generar un resultado u objetivo general.
Procedimiento	Acciones específicas y puntuales a seguir, para completar una tarea determinada.
Quipux	Plataforma para la gestión de documentos digitales de las instituciones públicas ecuatorianas.
Redundancia	Consiste en reproducir los elementos críticos (hardware o software) de un sistema, para asegurar la disponibilidad de los servicios ante fallos.
Respaldo o copia de seguridad	Copia o duplicado de los datos originales, con el fin de recuperarlos, ante cualquier pérdida parcial o total.
Riesgo	Nivel de incertidumbre que genera la probable materialización de una amenaza sobre un recurso de la organización. Relaciona el impacto de una amenaza versus su probabilidad de ocurrencia.

Router	Dispositivo físico que gestiona el tráfico de datos dentro de una red, para determinar las mejores rutas que deben tomar sus paquetes.
Seguridad de la información	Conjunto de técnicas y operaciones dedicadas a la preservación de la confidencialidad, integridad y disponibilidad de la información, y de los recursos que la gestionan.
Sistema de Gestión de Seguridad de Información (SGSI)	Consiste en el conjunto de controles, procedimientos y lineamientos, para reducir los riesgos tecnológicos de una organización.
Sistemas de información	Conjunto de componentes de hardware, software y personas, que se encuentran interrelacionados entre sí, para el procesamiento o tratamiento de la información de una organización.
Soporte de información o almacenamiento	Medios físicos para el resguardo de datos en formato electrónico o digital.
Switch	Dispositivo de interconexión de equipos dentro de una red común.
Teletrabajo	Trabajo ejercido fuera de las instalaciones de la entidad contratante, mediante el uso de las nuevas tecnologías.
Troyano	Tipo de malware que se hace pasar como un programa inofensivo, con la finalidad de que pueda ser descargado y ejecutado.
Usuario	Personas que hacen uso de la información y sus recursos para la prestación de servicios. También se puede referir a los receptores de los mismos.
UPS (Uninterruptible Power Supply)	Dispositivo electrónico capaz de suministrar energía a uno varios equipos, en caso de corte eléctrico.
Vulnerabilidad	Representa la debilidades inherentes de un sistema o activo, que pueden ser aprovechados por una amenaza.
Zimbra	Plataforma que permite enviar y recibir correo electrónico, así como, agendar citas y reuniones. No tiene costo de licenciamiento.

VIII. DESCRIPCIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

El presente documento, denominado Políticas de Seguridad de la Información para el Ministerio del Trabajo (Ibarra), comprende 193 Artículos cuyo orden no se fundamenta en su prioridad, sino más bien, en la estructura definida por 12 de los 14 Dominios de la Normativa ISO/IEC 27002, y a sus respectivos Objetivos de Control y Controles.

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA EL MINISTERIO DEL TRABAJO (IBARRA)

[Versión 1.0]

Ministerio del Trabajo — República del Ecuador — Gobierno del Encuentro — Juntos lo logramos

MACROPROCESO:	Gestión de Estudios y Generación de Políticas
PROCESO:	Gestión de Generación de Políticas y Normas
CÓDIGO:	POL-GEP-01

DOMINIO	5. POLÍTICAS DE SEGURIDAD.
OBJETIVO DE CONTROL	5.1 Directrices de la Dirección en seguridad de la información.
CONTROL	*5.1.1 Conjunto de políticas para la seguridad de la información.*

Artículo 1.- El Ministerio del Trabajo (Ibarra), consciente de la necesidad de apoyar y promover una adecuada gestión de la información, declara su compromiso para establecer y difundir el presente compendio de directrices conforme lo estipulado por la ISO/IEC 27002, en estricta concordancia con sus metas institucionales.

Artículo 2.- El Ministerio del Trabajo (Ibarra) con el propósito de mantener un control de los riesgos asociados a sus activos de información, se compromete a brindar el debido acompañamiento para la ejecución de las siguientes acciones:

- Ejecutar procesos alineados con los pilares y principios de seguridad de la información.
- Crear medidas efectivas para resguardar sus activos de información.
- Reducir los valores de riesgo que superan los rangos aceptados por la institución.
- Mantener niveles adecuados de disponibilidad, integridad y confidencialidad en sus activos, para generar confianza en sus funcionarios y ciudadanía.
- Desarrollar una cultura organizacional que alinee el comportamiento de sus funcionarios y terceros, con los objetivos de seguridad institucionales.
- Asegurar la disponibilidad y continuidad de los servicios institucionales ante un determinado evento o incidente de seguridad.

DOMINIO	5. POLÍTICAS DE SEGURIDAD.
OBJETIVO DE CONTROL	5.1 Directrices de la Dirección en seguridad de la información.
CONTROL	*5.1.2 Revisión de las políticas para la seguridad de la información.*

Artículo 3.- Para garantizar la vigencia del presente documento, sus lineamientos serán sujetos de revisión al menos una vez por año, o en respuesta a algún cambio relevante dentro de la institución, en cuanto a sus operaciones, aspectos financieros, tecnológicos, legales, entre otros.

DOMINIO	6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN
OBJETIVO DE CONTROL	6.1 Organización interna.
CONTROL	*6.1.1 Asignación de responsabilidades para la seguridad de la información.*

Artículo 4.- Responsabilidades del Director Regional o delegado para la gestión de la seguridad de la información

- Revisar y aprobar los lineamientos establecidos en el presente documento, brindando el apoyo necesario para su puesta en ejecución.
- Mantener el debido seguimiento a la normativa para controlar su cumplimiento, difusión y sensibilización.
- Aprobar la realización de eventuales modificaciones en su normativa, que aseguren su vigencia.
- Designar de manera oficial, a los integrantes del Comité de Gestión de la Seguridad de la Información Institucional.

Artículo 5.- Responsabilidades del Comité de Gestión de la Seguridad de la Información Institucional

- Gestionar tanto la aprobación del documento de políticas por parte de la máxima autoridad de la institución y la puesta en marcha del mismo, para el cumplimiento de sus funcionarios.
- Mantener reuniones con los representantes de cada Unidad Organizacional, a fin de evaluar periódicamente los riesgos asociados a los activos de información institucional. Se deberá elaborar las respectivas actas de reunión, con un previo registro de sus participantes.
- Llevar una bitácora de lecciones aprendidas, referentes a los incidentes de seguridad suscitados, para el diseño oportuno de medidas de mitigación.
- Nombrar a los custodios o responsables de los activos de información críticos institucionales.
- Difundir adecuadamente los lineamientos de la presente guía, de modo que sea conocida por todos los involucrados de manera oportuna, mediante el uso de distintos canales de comunicación.
- Brindar un adecuado seguimiento a los funcionarios y terceros, respecto al cumplimiento de los lineamientos establecidos.

Artículo 6.- Responsabilidades de la Unidad de TIC para la gestión de la seguridad de la información

- Documentar las tareas y acciones necesarias, para garantizar la correcta operación del sistema de información institucional, y para la preservación de su seguridad.
- Evaluar el impacto provocado por los cambios en la infraestructura tecnológica institucional, en el alcance y vigencia de las políticas.
- Implementar las medidas de control que han sido seleccionadas para mitigar los riesgos encontrados, en coordinación con el Comité de Gestión de la Seguridad de la Información Institucional.
- Establecer los procedimientos adecuados para gestionar los distintos eventos e incidentes de seguridad de la información, conforme al registro de lecciones aprendidas.
- Otras actividades relacionadas a la gestión de la seguridad de la información.

DOMINIO	6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN
OBJETIVO DE CONTROL	6.2 Dispositivos para movilidad y teletrabajo.
CONTROL	*6.2.1 Política de uso de dispositivos para movilidad.*

Artículo 7.- Todo funcionario que requiere obtener acceso a la red inalámbrica institucional, deberá levantar su requerimiento a través de la Plataforma GLPI, y se sujetará a los niveles de acceso estipulados en el apartado *9.1.2 Control de acceso a las redes y servicios asociados: Respecto al uso de Internet.*

Artículo 8.- Los dispositivos móviles de la institución, serán utilizados única y exclusivamente en lugares que les ofrezcan las garantías de seguridad física, con el propósito de impedir su pérdida o robo.

Artículo 9.- No se deberá transmitir información institucional, a través de redes inalámbricas de carácter público como aquellas disponibles en parques, centros comerciales, restaurantes, hoteles, cibercafés, entre otros).

Artículo 10.- Todo funcionario evitará almacenar datos o archivos personales, en los dispositivos móviles asignados.

Artículo 11.- Todo funcionario evitará ejecutar e instalar aplicaciones de fuentes sospechosas o desconocidas, en los dispositivos móviles institucionales.

Artículo 12.-Todo funcionario que detecte o sospeche de la intrusión de malware en su equipo asignado, deberá notificarlo oportunamente al personal de la Unidad de TIC.

Sección para la Unidad de TIC:

Artículo 13.- Elaborar y mantener una bitácora para el préstamo de equipos portátiles a funcionarios autorizados.

Artículo 14.- La asignación de equipos portátiles a terceros o visitantes, y su correspondiente acceso a los recursos de red, necesitará de la previa autorización de la máxima autoridad institucional o de su delegado.

Artículo 15.- Todo equipo móvil institucional, deberá contar al menos con las siguientes medidas de protección:

- Mantener un software de antivirus instalado y actualizado.
- Contar con herramientas técnicas para limitar o restringir la instalación de software no autorizado.
- Disponer de mecanismos de protección física, como candados de seguridad para portátiles.
- Contar con medidas de protección lógica, como las credenciales de acceso con usuario y contraseña.
- Elaborar copias de seguridad de su información crítica de manera periódica.

DOMINIO	6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN
OBJETIVO DE CONTROL	6.2 Dispositivos para movilidad y teletrabajo.
CONTROL	*6.2.2 Teletrabajo.*

Artículo 16.- Todo funcionario que requiera tener acceso a los servicios y sistemas institucionales de manera remota, deberá contar con la aprobación de la máxima autoridad o su delegado, y tendrá que levantar el requerimiento por la plataforma GLPI.

Artículo 17.-Las conexiones remotas deberán establecerse desde ordenadores institucionales o personales previamente registrados, evitando el uso de equipos de cómputo de sitios públicos.

Artículo 18.- Todo funcionario deberá cerrar las conexiones remotas y las sesiones de acceso a los sistemas institucionales, en los periodos de inactividad, incluso si se encuentra laborando desde el hogar.

Artículo 19.- Todo funcionario deberá fortalecer las contraseñas para el acceso remoto a los equipos y sistemas institucionales, cumpliendo las recomendaciones del apartado *9.3.1 Uso de información confidencial para la autenticación*.

Sección para los Administradores de red y Unidad de TIC:

Artículo 20.- Implementar herramientas de cifrado o encriptación de datos, para el establecimiento de conexiones remotas seguras, que garanticen su confidencialidad e integridad.

Artículo 21.- Brindar la asistencia y soporte necesario, para asegurar la disponibilidad del equipamiento y aplicaciones relacionadas con las conexiones para teletrabajo. Artículo 22.- Promover el uso de contraseñas seguras y el establecimiento de tiempos cortos de suspensión por inactividad, en los sistemas y equipos utilizados para el acceso remoto. Artículo 23.- Concientizar a los funcionarios, sobre los potenciales riesgos que acarrea el acceso remoto a los recursos institucionales.	
DOMINIO	7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
OBJETIVO DE CONTROL	7.1 Antes de la contratación.
CONTROL	*7.1.1 Investigación de antecedentes.*
Artículo 24.- La Unidad encargada de la contratación de personal, deberá comprobar la veracidad de la información de la Hoja de Vida de cada candidato y adicionalmente revisará el informe de antecedentes judiciales o disciplinarios.	
DOMINIO	7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
OBJETIVO DE CONTROL	7.1 Antes de la contratación.
CONTROL	*7.1.2 Términos y condiciones de contratación.*
Artículo 25.- El personal seleccionado deberá conocer y aceptar los lineamientos establecidos en este documento, antes de su contratación. Artículo 26.- El personal seleccionado, deberá firmar una Cláusula de Confidencialidad respecto al manejo adecuado de la información institucional, la cual deberá formar parte del documento del contrato.	
DOMINIO	7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
OBJETIVO DE CONTROL	7.2 Durante la contratación.
CONTROL	*7.2.1 Responsabilidades de gestión.*
Artículo 27.-El personal contratado deberá cumplir y acatar fielmente los lineamientos establecidos en el presente documento. Artículo 28.- Toda información procesada en la Institución es de propiedad exclusiva del Ministerio del Trabajo (Ibarra) y de la Unidad Organizacional que la origina, por tanto, ningún funcionario puede hacer uso de la misma para beneficios personales. Artículo 29.- Todo funcionario deberá mantener la confidencialidad de la información que utiliza en sus labores diarias. Artículo 30.- Todo funcionario será responsable de evitar la alteración de la información que procesa en el ejercicio de sus funciones, exceptuando casos especiales en los que las aplicaciones o sistemas requieran, para mantener su operación.	

Artículo 31.- La modificación accidental de información o manipulación errónea de los sistemas institucionales, deberá reportarse oportunamente al personal de la Unidad de TIC. Artículo 32.- Todo funcionario es responsable de generar copias de seguridad de sus datos, en base a sus propios criterios de valoración y priorización.	
DOMINIO	7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
OBJETIVO DE CONTROL	7.2 Durante la contratación.
CONTROL	*7.2.2 Concienciación, educación y capacitación en segur. de la información*
Artículo 33.- La Unidad de TIC y el Comité designado, deberán planificar periódicamente charlas de capacitación dirigidas a los funcionarios, para sensibilizarlos en temas de seguridad. Artículo 34.- La Unidad de TIC y la Unidad Administrativa Financiera deberán planificar la socialización de la presente guía a los nuevos funcionarios, de forma previa a la entrega de sus credenciales de acceso. Artículo 35.- Se deberá llevar un registro de las capacitaciones ejecutadas, que contenga los puntos y temas abordados, así como los datos de los funcionarios instruidos. Artículo 36.- Todo funcionario tiene la obligación de asistir a las distintas charlas de capacitación y socialización planificadas por la entidad.	
DOMINIO	7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
OBJETIVO DE CONTROL	7.2 Durante la contratación.
CONTROL	*7.2.3 Proceso disciplinario.*
Artículo 37.- La Unidad de TIC y la Unidad Administrativa Financiera deberán informar oportunamente a los funcionarios, sobre las penalizaciones que suponen el incumplimiento de la presente normativa. Artículo 38.- Es responsabilidad del Comité de Gestión de la Seguridad de la Información Institucional y de todos los funcionarios, reportar a la máxima autoridad o su delegado, sobre las acciones de incumplimiento a la presente guía.	
DOMINIO	7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
OBJETIVO DE CONTROL	7.3 Cese o cambio de puesto de trabajo
CONTROL	*7.3.1 Cese o cambio de puesto de trabajo.*
Artículo 39.- Todo funcionario cesante deberá realizar la entrega formal de los activos de información que le fueron asignados para el ejercicio de sus funciones. Artículo 40.- Es responsabilidad del jefe inmediato, notificar oportunamente a la Unidad de TIC, sobre la desvinculación de su personal a cargo, para la suspensión de sus cuentas y credenciales de acceso.	

Artículo 41.- Todo jefe inmediato deberá garantizar que el personal cesante que está a su cargo, entregue su información de manera íntegra, formal y completa, como requisito indispensable para la firma del "Acta de Paz y Salvo".

Artículo 42.- El personal desvinculado, se comprometerá a no entregar o divulgar la información reservada a terceros.

Artículo 43.- Todo servidor cesante deberá compartir la información generada en el transcurso de su relación contractual con la entidad, entregando una copia tanto a su jefe inmediato como al nuevo personal.

DOMINIO	8. GESTIÓN DE ACTIVOS.
OBJETIVO DE CONTROL	8.1 Responsabilidad sobre los activos.
CONTROL	*8.1.1 Inventario de activos.*

Artículo 44.- El personal encargado de Bienes, deberá coordinar con la Unidad de TIC, la ejecución periódica de procesos para el registro de activos institucionales. Estos inventarios deberán actualizarse, al menos de forma anual o cuando la entidad lo amerite.

Sección para la Unidad de TIC:

Artículo 45.- Deberá garantizar que los activos de información con mayor nivel de sensibilidad, sean identificados y valorados de manera oportuna, en coordinación con el Comité de Gestión de Seguridad de la Información institucional.

DOMINIO	8. GESTIÓN DE ACTIVOS.
OBJETIVO DE CONTROL	8.1 Responsabilidad sobre los activos.
CONTROL	*8.1.2 Propiedad de los activos.*

Artículo 46.- Los activos de información institucional y especialmente aquellos con mayor nivel de sensibilidad, deberán tener asignado un custodio o responsable, quién velará por mantener su integridad.

DOMINIO	8. GESTIÓN DE ACTIVOS.
OBJETIVO DE CONTROL	8.1 Responsabilidad sobre los activos.
CONTROL	*8.1.3 Uso aceptable de los activos.*

Artículo 47.- Todo funcionario es responsable de resguardar y mantener en condiciones óptimas, los recursos de cómputo asignados para sus operaciones diarias.

Artículo 48.- Todo servidor deberá usar sus recursos de cómputo asignados, única y exclusivamente, para las tareas o actividades relacionadas a su cargo o función.

Artículo 49.- Cada Unidad Organizacional, deberá hacer uso de las impresoras asignadas, y para las tareas propias de la institución, manteniendo criterios de ahorro y cuidado de sus suministros.

Artículo 50.- Todo funcionario evitará reubicar los equipos de cómputo asignados de manera arbitraria, y deberá solicitar asistencia a la Unidad de TIC, mediante la plataforma GLPI.

Artículo 51.- Todo funcionario evitará instalar dispositivos o aplicaciones adicionales a los que se le ha asignado o autorizado.

Artículo 52.- Todo servidor es responsable de que sus equipos de cómputo asignados, no sean manipulados por personas ajenas o no autorizadas.

Artículo 53.- Todo servidor que reciba a su cargo un equipo de cómputo, se responsabilizará de la información almacenada en el mismo y deberá corroborar que haya sido respaldada y/o correctamente eliminada.

Artículo 54.- Todo servidor que reciba a su cargo un equipo de cómputo, deberá acatar los lineamientos del apartado *9.3.1 Uso de información confidencial para la autenticación*, referente al uso adecuado de sus credenciales.

Artículo 55.- Todo funcionario deberá respaldar y eliminar de forma segura sus datos personales o confidenciales, en caso de baja del equipamiento que le fue asignado, en coordinación con el personal de la Unidad de TIC.

Artículo 56.- Todo servidor que requiera ausentarse momentáneamente de su estación de trabajo, deberá cerrar las sesiones del ordenador asignado, independientemente del tiempo que ha previsto para su inactividad.

Artículo 57.- Todo servidor que, por diversos motivos, requiera usar su ordenador personal para desempeñar sus actividades laborales, deberá notificar a la Unidad de TIC para su autorización y registro del dispositivo.

Artículo 58.- Todo funcionario deberá conservar una conducta apropiada respecto a la manipulación de su equipamiento, manteniendo prácticas de buen uso, como las siguientes:

- Debe evitar fumar o consumir alimentos en su estación de trabajo.
- No debe colocar objetos sobre el equipamiento tecnológico, principalmente si cubren sus mecanismos de ventilación.
- No debe colocar objetos sobre los cables de conexión del equipamiento (USB, de red, de alimentación, etc.) para evitar su deterioro o mal funcionamiento.
- No debe conectar dispositivos electrónicos, tales como: cargadores, ventiladores, radios, cafeteras, entre otros, en las regletas o tomas de corriente asignadas para los equipos de cómputo institucionales.
- Debe preservar el orden y limpieza de su estación de trabajo, así como de los equipos de cómputo y demás dispositivos asignados.

- No debe manipular bruscamente los equipos de cómputo asignados, especialmente los componentes de escáneres e impresoras.
- Debe apagar adecuadamente sus equipos asignados tras la culminación de la jornada, evitando realizar esta acción de manera forzada.
- Debe evitar dejar encendido el monitor, tras una ausencia prolongada de su estación de trabajo.
- Entre otras buenas prácticas.

Artículo 59.- Todo funcionario que detecte cualquier tipo de daño a nivel físico o lógico en su equipamiento, deberá reportarlo oportunamente a la Unidad de TIC, mediante la plataforma GLPI.

DOMINIO	8. GESTIÓN DE ACTIVOS.
OBJETIVO DE CONTROL	8.1 Responsabilidad sobre los activos.
CONTROL	*8.1.4 Devolución de activos.*

Artículo 60.- Todo funcionario cesante o aquel servidor que cambie de funciones dentro la institución, deberá realizar la entrega formal, de todos los activos de información que le fueron asignados, considerando lo mencionado en el apartado: *7.3.1 Cese o cambio de puesto de trabajo.*

DOMINIO	8. GESTIÓN DE ACTIVOS.
OBJETIVO DE CONTROL	8.2 Clasificación de la información.
CONTROL	*8.2.1 Directrices de clasificación.*

Artículo 61.- Cada Unidad Organizacional deberá clasificar la información que manejan dentro de sus competencias, de manera autónoma y en base a los niveles de confidencialidad definidos por la institución.

Artículo 62.- La clasificación de la información perteneciente al Ministerio del Trabajo (Ibarra), obedecerá a los siguientes criterios de confidencialidad:

- Información Reservada: aquella usada por un grupo específico de servidores. Su divulgación, puede suponer un fuerte impacto a la entidad.
- Información Clasificada: aquella usada por todos los servidores, con autorización de su propietario.
- Información Pública: aquella que puede ser conocida por todos los servidores y ciudanía general.
- Información No clasificada: aquella que forma parte de los inventarios institucionales, pero cuya clasificación se encuentra en estado pendiente.

DOMINIO	8. GESTIÓN DE ACTIVOS.
OBJETIVO DE CONTROL	8.2 Clasificación de la información.
CONTROL	*8.2.2 Etiquetado y manipulado de la información.*

Artículo 63.- Los servidores del Ministerio del Trabajo (Ibarra) no podrán acceder a la información a la que no estén autorizados.

Artículo 64.- Todo Jefe o responsable de cada Unidad Organizativa, deberá asegurar que las directrices relacionadas al acceso y uso de la información, sean comunicadas eficaz y oportunamente a los funcionarios que están a su cargo.

Artículo 65.- Todo Jefe o responsable de cada Unidad Organizativa, deberá asegurar que el personal que tiene bajo su responsabilidad, conozca los niveles criticidad de los datos que se maneja en su área, y que se cumplan con las medidas de seguridad establecidas.

Artículo 66.- Todo servidor deberá garantizar que la información reservada que utiliza dentro de sus competencias, sea manipulada y almacenada de manera segura, garantizando su confidencialidad e integridad.

Artículo 67.- Todo funcionario deberá destruir cualquier información de carácter reservado, contenida en medios físicos (documentos, notas, informes, fichas, registros) o soportes de almacenamiento (Memorias Flash USB, CDs, DVDs), antes de que ésta sea descartada.

Artículo 68.- Todo servidor es responsable de notificar oportunamente, sobre cualquier actividad sospechosa o mal intencionada, que pueda poner en riesgo la información institucional.

Artículo 69.- Se deberá etiquetar la información institucional, tanto impresa como digital, usando la sintaxis: *Nivel de Confidencialidad (reservada, clasificada o pública) /Unidad Organizacional /Custodio.*

Artículo 70.- Todo funcionario que, dentro de sus funciones, maneje información del tipo "reservada", deberá respaldarla de forma continua y permanente.

Artículo 71.- Las copias o respaldos de la información considerada como reservada, deberán almacenarse en sitios seguros, fuera del alcance de personas no autorizadas.

DOMINIO	8. GESTIÓN DE ACTIVOS.
OBJETIVO DE CONTROL	8.3 Manejo de los soportes de almacenamiento.
CONTROL	*8.3.1 Gestión de soportes extraíbles.*

Artículo 72.- Todo servidor deberá manipular adecuadamente los soportes de almacenamiento que le han sido entregados, manteniendo su correcto funcionamiento y preservando su información.

Artículo 73.- Todo servidor deberá activar el escaneo automático del antivirus institucional en su ordenador, para el análisis de los soportes de almacenamiento autorizados. Si es necesario, deberá solicitar asistencia a la Unidad de TIC.

Artículo 74.- Todo funcionario evitará conectar en sus equipos asignados, soportes de almacenamiento perteneciente a terceras personas, sin la revisión y autorización del personal de la Unidad de TIC.

Sección para la Unidad de TIC:

Artículo 75.- Los soportes de almacenamiento deberán ser resguardados en sitios seguros y en condiciones ambientales óptimas, las cuales son determinadas por el fabricante para evitar su degradación.

Artículo 76.- Los soportes de almacenamiento que contengan información reservada, utilizarán técnicas criptográficas, y deberán resguardarse en varias locaciones, para asegurar la integridad y confidencialidad de sus datos.

Artículo 77.- Se deberá utilizar técnicas de borrado de seguro en los dispositivos de almacenamiento asignados a funcionarios cesantes y en los soportes de almacenamiento que requieran ser dados de baja.

DOMINIO	9. CONTROL DE ACCESO
OBJETIVO DE CONTROL	9.1 Requisitos de negocio para el control de acceso
CONTROL	*9.1.1 Política de control de acceso*

Artículo 78.- El Ministerio del Trabajo (Ibarra) deberá garantizar que sus activos de información, sean protegidos de accesos no autorizados, mediante la implementación de medidas físicas y lógicas.

Artículo 79.-El uso de los recursos institucionales, estará condicionado por los niveles de privilegios asignados a cada uno de los funcionarios para el cumplimiento de sus labores.

DOMINIO	9. CONTROL DE ACCESO
OBJETIVO DE CONTROL	9.1 Requisitos de negocio para el control de acceso
CONTROL	*9.1.2 Control de acceso a las redes y servicios asociados.*

Artículo 80.-Los niveles de privilegio serán establecidos por la Unidad de TIC, de acuerdo a los roles asignados desde Talento Humano.

Artículo 81.- Todo funcionario deberá respetar los privilegios asignados, y hacer uso de los servicios para los que fue autorizado.

Sobre el uso de Internet

Artículo 82.- El uso del servicio de Internet institucional, deberá regirse a los siguientes niveles de acceso:

- Básico: concede permisos para acceder a la intranet y sistemas institucionales, así como a portales gubernamentales y sitios web para consultas legales.
- Intermedio: lo dispuesto en el nivel básico, sumado el acceso a sitios web bancarios, para consultas sin descarga, y portales de noticias.
- Avanzado: lo dispuesto en el nivel intermedio, y adicionalmente el acceso a redes sociales y sitios web con descargas limitadas.
- Rol de Administrador: libre acceso a la Internet, con excepción de sitios web con contenido sexual, o que expresen racismo, xenofobia, violencia, etc.
- Visitantes: lo dispuesto en el nivel básico, con la posibilidad de que pueda ampliarse, con una previa autorización de la máxima autoridad.

Artículo 83.- Todo nuevo funcionario tendrá asignado el nivel básico de acceso a Internet, el cual podrá ser modificado posteriormente, con la debida justificación y autorización de su jefe inmediato.

Artículo 84. Todo funcionario que goce del servicio de Internet institucional, deberá aceptar las siguientes condiciones:

- El uso del servicio será exclusivo para las actividades propias de sus funciones.
- Las actividades de navegación que los funcionarios realizan en la red institucional estarán sujetas a monitoreo.
- Todo servidor conoce de la prohibición existente, respecto al acceso a sitios web no autorizados y descarga de aplicaciones de páginas desconocidas.
- Todo funcionario conoce de la prohibición existente, respecto a la trasferencia de archivos con información reservada o confidencial.
- Todo servidor conoce de la prohibición existente, respecto al acceso a los servicios de red, desde dispositivos ajenos a la institución, sin la debida autorización.

Artículo 85.-Se evitará hacer uso de este servicio para actividades consideradas ilícitas, cuyo fin sea dejar inutilizados los servicios institucionales o causar afectaciones en sus recursos de información.

Sobre el uso del Correo electrónico institucional

Artículo 86.- Este servicio será utilizado única y exclusivamente por los funcionarios de la entidad autorizados, y la información emitida desde sus cuentas estará bajo su responsabilidad.

Artículo 87.- Todo funcionario deberá usar responsablemente las credenciales de acceso para su cuenta de correo asignada, la cual es personal e intransferible.

Artículo 88.- Todo funcionario deberá reportar oportunamente sobre cualquier suceso que ponga en riesgo la disponibilidad de su cuenta de correo asignada, y solicitará asistencia mediante la plataforma GLPI.

Artículo 89.- Todo funcionario que goce del servicio de correo electrónico institucional, no deberá:

- Usar el servicio para actividades personales.
- Transmitir archivos catalogados como "reservados", de acuerdo a los criterios de categorización estipulados en el apartado: *8.2.1 Directrices de clasificación.*
- Guardar datos personales en los buzones del correo electrónico institucional.
- Abrir links sospechosos o responder correos de dudosa procedencia.
- Transferir información institucional a través de proveedores externos de correo electrónico como: Hotmail, Outlook, Gmail, entre otros.
- Acceder a los buzones de las cuentas de otros funcionarios, excepto con fines de auditoría.
- Hacer uso del servicio para trasmitir software malicioso (virus, troyanos, gusanos, espías, etc.) a otros equipos, servidores y red en general.
- Enviar archivos con contenidos multimedia o con extensiones sospechosas, que generen un riesgo mayor para la difusión de malware.

Artículo 90.- Todo funcionario es responsable de extraer periódicamente, una copia de seguridad de la carpeta "Thunderbird", la cual contiene todos sus correos institucionales. En caso de requerir asistencia, deberá levantar la petición mediante la Plataforma GLPI.

Artículo 91.- Es responsabilidad de cada funcionario, liberar el espacio que le ha sido asignado dentro de su cuenta en la plataforma Zimbra, de modo que le permita recibir correos sin interrupciones ni retrasos.

Artículo 92.-En el caso de acceder al servicio de correo institucional vía web (usando su cuenta en Zimbra), deberá deshabilitar la opción de recordatorio de credenciales en el navegador.

DOMINIO	9. CONTROL DE ACCESO
OBJETIVO DE CONTROL	9.2 Gestión de acceso de usuario.
CONTROL	*9.2.1 Gestión de altas/bajas en el registro de usuarios.*

Artículo 93.- El responsable de cada Unidad Organizacional, deberá levantar el requerimiento para la creación de las credenciales del nuevo personal que está a su cargo, usando el Sistema de Tickets GLPI.

Artículo 94.- En las solicitudes de creación de cuentas para el nuevo personal, deberá constar sus datos personales (número de cédula, nombres completos) y de su cargo (denominación del puesto, número de Acción del Personal).

Artículo 95.- El responsable de cada Unidad Organizacional, deberá levantar el requerimiento para la deshabilitación de las credenciales del personal cesante que estuvo a su cargo, usando el Sistema de Tickets GLPI.

DOMINIO	9. CONTROL DE ACCESO
OBJETIVO DE CONTROL	9.3 Responsabilidades del usuario.
CONTROL	*9.3.1 Uso de información confidencial para la autenticación.*

Artículo 96.- Todo funcionario deberá resguardar adecuadamente sus credenciales, evitando que sean conocidas y utilizadas por terceras personas.

Artículo 97.- Todo funcionario deberá acatar la sintaxis de contraseña robusta definida a nivel institucional. Si desconoce la longitud o tipo de caracteres sugeridos, deberá consultar a la Unidad de TIC.

Artículo 98.- Todo funcionario evitará utilizar las mismas contraseñas, para distintos sistemas o servicios, sean éstos institucionales o externos.

Artículo 99.- Todo funcionario deberá modificar sus contraseñas de forma periódica, evitando la reutilización de las últimas claves de acceso.

Artículo 100.- Las contraseñas de los equipos, servicios y sistemas, no deberán ser exhibidas o almacenadas en notas adhesivas, hojas sueltas, ficheros o archivos de software, y demás repositorios que no garanticen su confidencialidad.

Artículo 101.- Todo funcionario evitará almacenar contraseñas en el navegador y demás sistemas, por lo que deberá ingresarlas manualmente en cada inicio de sesión.

Artículo 102.- Todo funcionario tiene la obligación de eliminar la documentación otorgada por la Unidad de TIC, concerniente a los datos de sus credenciales de acceso para los sistemas institucionales.

Sección para los Administradores de red y Unidad de TIC:

Artículo 103.- Deberán fijar la sintaxis de las contraseñas, con un nivel de complejidad adecuado y deberán definir los tiempos estimados para sus actualizaciones.

Artículo 104.- Deberán modificar las contraseñas que vienen definidas por los fabricantes de equipos o proveedores de software.

DOMINIO	9. CONTROL DE ACCESO
OBJETIVO DE CONTROL	9.4 Control de acceso a sistemas y aplicaciones.
CONTROL	*9.4.1 Restricción del acceso a la información.*

Artículo 105.- Todo servidor deberá acceder a los servicios y sistemas institucionales, única y exclusivamente desde su cuenta asignada, y tendrá que regirse al nivel de acceso otorgado.

Artículo 106.- El servidor deberá cerrar las sesiones de acceso a los servicios y sistemas institucionales, una vez que haya concluido la jornada laboral, o cuando deba ausentarse momentáneamente de su estación de trabajo.

Artículo 107.- Todo funcionario está obligado a reportar sobre cualquier error de configuración del nivel de acceso a los servicios o sistemas instituciones, dado por un exceso o escasez de permisos.

Artículo 108.- Se prohíbe probar o implementar herramientas fraudulentas, para vulnerar los controles de los sistemas y aplicaciones institucionales, buscando acceder de manera no autorizada o con un nivel mayor de privilegios al que fue asignado.

Sección para los Administradores de red y Unidad de TIC:

Artículo 109.- Deberán configurar los accesos de los funcionarios a los sistemas y aplicaciones, cumpliendo fielmente con los niveles de privilegios indicados desde Talento Humano.

Artículo 110.- Deberán brindar el debido control y seguimiento de los permisos entregados, para evitar abusos por parte de los funcionarios.

Artículo 111.- Deberán gestionar los accesos remotos de los funcionarios a los sistemas y aplicaciones, garantizando que los privilegios entregados estén acorde a sus funciones.

DOMINIO	11. SEGURIDAD FÍSICA Y AMBIENTAL
OBJETIVO DE CONTROL	11.1 Áreas seguras.
CONTROL	*11.1.1 Controles físicos de entrada.*

Artículo 112.- El Ministerio del Trabajo (Ibarra) deberá asegurar que los visitantes o usuarios externos, que requieran acceder a sus oficinas administrativas, exceptuando los puntos de atención al público, cuenten con una autorización previa de la máxima autoridad.

Artículo 113.- El Ministerio del Trabajo (Ibarra) deberá asegurar que los visitantes o usuarios externos, que ingresaron a sus oficinas administrativas, exceptuando los puntos de atención al público, hayan sido registrados en una bitácora de datos personales.

Artículo 114.- La bitácora de registro de datos para visitantes y usuarios externos, estará a cargo del personal de seguridad institucional y los funcionarios de recepción.

Artículo 115.- El ingreso a las instalaciones requerirá la presentación de la cédula de identidad para personas externas y de la credencial para todos los funcionarios.

Sección para la Unidad de TIC:

Artículo 116.- Se deberá revisar y monitorear periódicamente el sistema de videocámaras institucional, a fin de mantenerlo operativo en todo momento.

DOMINIO	11. SEGURIDAD FÍSICA Y AMBIENTAL
OBJETIVO DE CONTROL	11.1 Áreas seguras.
CONTROL	*11.1.2 Seguridad de oficinas, despachos y recursos.*

Artículo 117.- Todo Jefe o responsable de cada Unidad, en coordinación con el personal de Seguridad y Salud en el Trabajo de la entidad, deberán identificar las áreas de mayor vulnerabilidad, considerando el valor de los activos que dichas instalaciones albergan.

Artículo 118.- Todo Jefe o responsable de cada Unidad, dispondrá que las áreas vulnerables a su cargo, se mantengan cerradas, principalmente aquellas donde no se dispone del servicio de video vigilancia.

Artículo 119.- El responsable de Seguridad y Salud institucional, deberá garantizar una adecuada señalización de dichos espacios, para evitar el ingreso no autorizado de terceros.

Artículo 120.- El ingreso a las instalaciones correspondientes al archivo pasivo y centro de datos de la entidad, deberá ser limitado y exclusivo únicamente para sus funcionarios responsables.

Artículo 121.- El ingreso a las instalaciones correspondientes al centro de datos institucional, por parte de terceras personas, requerirá de la previa autorización de la máxima autoridad y del debido acompañamiento y seguimiento del personal de la Unidad de TIC.

Artículo 122.- El Jefe de la Unidad Administrativa Financiera deberá delegar a un responsable del equipo encargado de la limpieza de las instalaciones de la entidad, quien asegurará la integridad de los recursos de información mientras se ejecutan las tareas de sanidad.

DOMINIO	11. SEGURIDAD FÍSICA Y AMBIENTAL
OBJETIVO DE CONTROL	11.1 Áreas seguras.
CONTROL	*11.1.3 Protección contra las amenazas externas y ambientales.*

Artículo 123.- El responsable de Seguridad y Salud institucional, deberá garantizar el uso de señalética, para identificar los espacios donde se almacenan materiales inflamables y peligrosos.

Artículo 124.- Se deberá asegurar que dichos espacios, estén físicamente alejados y a un perímetro adecuado de las áreas departamentales.

Artículo 125.- Se deberá disponer de extintores Clase B (incendios por líquidos inflamables) y Clase C (fuego activado por electricidad), necesarios para minimizar el nivel de daño en los recursos.

Sección para la Unidad de TIC:

Artículo 126.- Las instalaciones de red deberán permanecer físicamente alejadas de cualquier tipo de cableado eléctrico o de alimentación, para minimizar las interferencias.

Artículo 127.- Se deberá asegurar la disponibilidad de los equipos del centro de datos, ante desabastecimientos de energía eléctrica, mediante dispositivos UPS.

Artículo 128.- Se deberá gestionar periódicamente, la contratación de personal técnico especializado, para el mantenimiento de los sistemas de enfriamiento y ventilación en el centro de datos institucional.

Artículo 129.- Establecer medidas para mitigar el riesgo proveniente de amenazas comunes, como: interferencias, contaminación por polvo, cortes eléctricos, vibración, entre otros.

DOMINIO	11. SEGURIDAD FÍSICA Y AMBIENTAL
OBJETIVO DE CONTROL	11.2 Seguridad de los equipos.
CONTROL	*11.2.1 Emplazamiento y protección de equipos.*

Artículo 130.- El equipamiento institucional deberá ubicarse en espacios seguros y con el mobiliario apropiado, para evitar su manipulación por parte de terceros.

Artículo 131.- Todo funcionario deberá evitar reubicar el equipamiento institucional de forma arbitraria. Para este efecto, necesitará solicitar asistencia a la Unidad de TIC.

Artículo 132.- Todo funcionario evitará realizar tareas de reparación o instalación de dispositivos adicionales, en su equipamiento asignado. Para este cometido, deberá solicitar asistencia a la Unidad de TIC.

Artículo 133.- Todo funcionario evitará ubicar su equipamiento, fuera de su estación de trabajo, y sin las conexiones respectivas.

Artículo 134.- Todo funcionario aplicará las debidas medidas y precauciones, para transportar su equipamiento a otras locaciones.

Artículo 135.- Todo funcionario deberá notificar oportunamente a la máxima autoridad y Unidad de TIC, en caso de daño, pérdida o robo de su equipamiento asignado.

Sección para los Administradores de red y Unidad de TIC:

Artículo 136.- Se deberá llevar una bitácora para préstamos de equipos para los funcionarios y visitantes. Entre los cuales constan: laptops, proyectores, discos externos, cables, regletas, entre otros).

Artículo 137.- Se tomará en consideración, las siguientes medidas respecto al centro de datos institucional:

- Controles físicos en la entrada
- Ubicación y protección del equipamiento
- Suministro eléctrico y climatización (temperatura/humedad)
- Redundancia de sistemas
- Mantenimiento preventivo y correctivo de equipos de cómputo, comunicaciones y auxiliar.

DOMINIO	11. SEGURIDAD FÍSICA Y AMBIENTAL
OBJETIVO DE CONTROL	11.2 Seguridad de los equipos.
CONTROL	*11.2.2 Mantenimiento de los equipos.*

Artículo 138.- Las tareas de reparación y/o mantenimiento del equipamiento institucional, estará a cargo única y exclusivamente por la Unidad de TIC y proveedores de servicio técnico autorizados

Artículo 139.- Los funcionarios no están facultados para ejecutar tareas de reparación en sus equipos, y deberán solicitar este servicio a la Unidad de TIC institucional, mediante el Sistema GLPI.

Sección para la Unidad de TIC:

Artículo 140.- Deberá organizar y ejecutar los respectivos planes de mantenimiento del equipamiento tecnológico de la entidad, asegurando que se desarrollen cuando menos una vez al año.

Artículo 141.- Deberá llevar un registro de lecciones aprendidas, referente a los problemas o fallos detectados en los procesos de mantenimiento, con sus correspondientes medidas de solución.

DOMINIO	11. SEGURIDAD FÍSICA Y AMBIENTAL
OBJETIVO DE CONTROL	11.2 Seguridad de los equipos.
CONTROL	*11.2.3 Salida de activos fuera de las dependencias de la empresa.*

Artículo 142.- Ningún funcionario deberá trasladar sus equipos asignados fuera de la institución, y en el caso excepcional de requerir realizar esta acción, deberá contar con la autorización de la máxima autoridad.

Artículo 143.- Todo funcionario que cuente con la autorización para utilizar su equipo fuera de las instalaciones, deberá seguir acatando las medidas y lineamientos de seguridad institucionales.

Artículo 144.- Todo funcionario que deba enviar su equipamiento, mediante el servicio de valija institucional, garantizará que el mismo sea correctamente empaquetado y etiquetado de acuerdo a su fragilidad.	
DOMINIO	11. SEGURIDAD FÍSICA Y AMBIENTAL
OBJETIVO DE CONTROL	11.2 Seguridad de los equipos.
CONTROL	*11.2.4 Política de puesto de trabajo despejado y bloqueo de pantalla.*
Artículo 145.- Los servidores que, por distintas razones deban dejar sus estaciones de trabajo por lapsos de tiempo considerables, tendrán que: ▪ Depositar su información reservada en lugares físicos o digitales seguros, evitando dejarla en sitios de fácil acceso. ▪ Mantener cerradas las aplicaciones y las sesiones de los sistemas institucionales. ▪ Cerrar la sesión de su ordenador o apagarlo una vez concluida la jornada de trabajo. *Sección para la Unidad de TIC:* Artículo 146.- Deberán habilitar la opción de bloqueo de pantalla de forma automática, en todos los ordenadores institucionales, y en el mínimo tiempo posible.	
DOMINIO	12. SEGURIDAD EN LA OPERATIVA.
OBJETIVO DE CONTROL	12.1 Responsabilidades y procedimientos de operación.
CONTROL	*12.1.1 Documentación de procedimientos de operación.*
Sección para la Unidad de TIC: Artículo 147.- Deberá gestionar el proceso de adquisición del equipamiento institucional, de acuerdo a sus necesidades, disponibilidad de recursos y en coordinación con la Unidad Administrativa Financiera. Artículo 148.- Deberá gestionar el proceso de aprovisionamiento del software, requerido por el Ministerio del Trabajo (Ibarra). Artículo 149.- Deberá gestionar el proceso de baja de equipamiento, en coordinación con el personal encargado de Bienes. Artículo 150.- Deberá gestionar el proceso de aprovisionamiento de suministros de impresoras, en coordinación con la Unidad Administrativa Financiera.	
DOMINIO	12. SEGURIDAD EN LA OPERATIVA.
OBJETIVO DE CONTROL	12.2 Protección contra código malicioso.
CONTROL	*12.2.1 Controles contra el código malicioso.*

Artículo 151.- Todo servidor evitará comprometer su información, por efecto de la propagación de código malicioso (virus, espías, troyanos, gusanos, etc.) en su ordenador.

Artículo 152.- Todo servidor deberá aplicar las siguientes medidas:

- Mantendrá siempre activo, la protección del antivirus asignado.
- Evitará abrir correos electrónicos de fuentes desconocidas.
- No navegará por sitios web poco confiables.
- Navegará en la web utilizando el protocolo seguro HTTPS.
- Mantendrá sus dispositivos de almacenamiento libres de malware.
- Evitará acceder a redes ajenas, desde los equipos institucionales, entre otras medidas.

Artículo 153.- Todo servidor evitará ejecutar aplicaciones o programas descargados de sitios web desconocidos.

Artículo 154.- El funcionario o tercero, con acceso a la red institucional, no deberá probar o ejecutar software malicioso de forma intencionada, dicha acción será catalogada como un grave incumplimiento.

Artículo 155.- Todo servidor que sospeche de cualquier intromisión de malware en su equipo, o la afectación por algún ataque o acción fraudulenta, deberá solicitar asistencia al personal tecnológico institucional de forma inmediata.

Sección para los Administradores de red y Unidad de TIC:

Artículo 156.- Deberán limitar los permisos de las cuentas de usuario de los ordenadores institucionales, para evitar la libre instalación de software no autorizado.

Artículo 157.- Se llevará un control de las versiones de los sistemas operativos y demás aplicaciones, con el fin de mantenerlos debidamente actualizados.

Artículo 158.- Deberán considerar el uso de herramientas tecnológicas para filtrado de tráfico, las cuales tendrán que ser debidamente configuradas y monitoreadas.

Artículo 159.- Deberán garantizar que todos los equipos de cómputo se encuentren inmersos en las políticas del antivirus institucional.

Artículo 160.- Deberán concientizar a los funcionarios sobre los riesgos generados, a consecuencia de la intromisión de malware en su equipamiento.

Artículo 161.- Deberán instruir a los funcionarios, respecto al buen uso del correo electrónico institucional, siguiendo las directrices del punto: 9*.1.2 Control de acceso a las redes y servicios asociados: Respecto al uso del correo electrónico.*

DOMINIO	12. SEGURIDAD EN LA OPERATIVA.
OBJETIVO DE CONTROL	12.3 Copias de seguridad.
CONTROL	*12.3.1 Copias de seguridad de la información.*

Artículo 162.- Todo servidor deberá almacenar su información (digital) en la partición del disco duro destinada para datos. Solicitará asistencia al área tecnológica si el caso lo amerita.

Artículo 163.- Todo servidor es responsable de replicar o respaldar su información, en base a sus propios criterios de priorización.

Artículo 164.- Todo servidor es responsable de resguardar los soportes de información que le han sido entregados para almacenar sus copias de seguridad o respaldos.

Sección para la Unidad de TIC:

Artículo 165.- Deberá contar con una réplica adicional de los datos respaldados por los funcionarios, para evitar su pérdida o modificación intencionada.

Artículo 166.- Deberá programar o planificar anualmente las tareas de extracción de datos de los funcionarios, de forma tal, que no interrumpa sus actividades diarias.

Artículo167.- Deberá garantizar que los soportes de almacenamiento que contienen los respaldos de los funcionarios, sean almacenados en sitios seguros y bajo condiciones normales de temperatura y/o humedad para minimizar su degradación.

DOMINIO	13. SEGURIDAD EN LAS TELECOMUNICACIONES.
OBJETIVO DE CONTROL	13.1 Gestión de la seguridad en las redes.
CONTROL	*13.1.1 Controles de red.*

Sección para la Unidad de TIC:

Artículo 168.- Deberá mantener un registro de los equipos de redes institucionales, mismo que deberá ser actualizado anualmente, o en caso de cambios considerables en la infraestructura tecnológica.

Artículo 169.- Deberá respaldar los archivos de configuración de los equipos de redes que son administrables, para evitar errores y reducir los tiempos de instalación, reparación o sustitución de dichos dispositivos.

Artículo 170.- Deberá mantener contraseñas con un nivel adecuado de complejidad en sus dispositivos de redes, evitando reutilizar las claves de los fabricantes o proveedores.

Artículo 171.- Deberá garantizar que los equipos de redes se alberguen en espacios seguros y bajo condiciones ambientales adecuadas.

Artículo 172.- Deberá mantener un etiquetado adecuado en las instalaciones de cableado estructurado y dispositivos de red institucionales, de tal manera que facilite la identificación de averías.

Artículo 173.- Deberá asegurar que las instalaciones que albergan los equios de redes, cuenten con una adecuada señalética, que minimice los riesgos de accidentes laborales o accesos indebidos.

Sección para los Administradores de red

Artículo 174.- Deberán garantizar la correcta operación y disponibilidad de los equipos de red y servicios institucionales, y asegurará que el acceso a los mismos, sean condicionados por los privilegios de cada funcionario.

Artículo 175.- Deberán llevar registros de las actividades y accesos de los funcionarios en la red, con el fin de verificar su cumplimiento a la normativa.

DOMINIO	15. RELACIONES CON SUMINISTRADORES.
OBJETIVO DE CONTROL	15.1 Seguridad de la información en las relaciones con suministradores.
CONTROL	*15.1.1 Política de seguridad de la información para suministradores.*

Sección para la Unidad de TIC:

Artículo 176.- Deberá pactar acuerdos de confidencialidad con los suministradores que tienen acceso a las instalaciones, o que manipulan el equipamiento institucional

Artículo 177.- Deberá pactar acuerdos de confidencialidad con los suministradores que tienen frecuente acercamiento con los funcionarios y sus datos.

Artículo 178.- Deberá establecer contratos con los suministradores, con cláusulas que aseguren la debida recepción de sus bienes o servicios.

Artículo 179.- Deberá brindar un adecuado seguimiento a las labores ejercidas por los suministradores, para verificar el estricto cumplimiento de la normativa y términos contractuales.

DOMINIO	16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
OBJETIVO DE CONTROL	16.1 Gestión de incidentes de seguridad de la información y mejoras.
CONTROL	*16.1.1 Responsabilidades y procedimientos.*

Artículo 180.- Todo servidor deberá informar al personal de TIC, sobre la presencia de cualquier incidente o evento de seguridad, que pueda afectar los recursos de información de la entidad. Entre otros incidentes, se citan los siguientes:

- Medidas de protección deficientes o desactualizadas.
- Errores no intencionados de los funcionarios, respecto a la gestión de la seguridad de la información.
- Violaciones a la normativa vigente.
- Fallas en la operación del equipamiento, sistemas o aplicaciones.
- Abusos de privilegios.
- Otros eventos que impliquen la vulneración de los recursos de información del Ministerio del Trabajo (Ibarra).

Sección para la Dirección de TIC, Unidad de TIC y Comité de Gestión de la Seguridad de la Información Institucional:

Artículo 181.- Se deberá mantener la confidencialidad de las notificaciones reportadas por los funcionarios.

Artículo 182.- Los incidentes que supongan acciones maliciosas y fraudulentas graves, originadas por entes externos o internos a la institución, deberán ser escalados a la Dirección de TIC de planta central.

Artículo 183.- La Dirección de TIC de planta central deberá atender de manera inmediata los incidentes relacionados a delitos informáticos que le han sido asignados, preservando la disponibilidad de los servicios de sus requirentes.

Artículo 184.- La Unidad de TIC en coordinación con el Comité de Gestión de la Seguridad de la Información Institucional, también deberán:

- Recopilar, documentar y priorizar las incidencias detectadas.
- Adoptar medidas para mitigar las secuelas de los incidentes producidos, de acuerdo a su nivel de prioridad.
- Mantener un registro de lecciones aprendidas, con el fin de conocer los antecedentes relacionados con un determinado evento y el procedimiento a seguir para gestionarlo.

Artículo 185.- Deberán gestionar canales de comunicación con los funcionarios, para mantenerlos informados respecto a los incidentes detectados.

Artículo 186.- Deberán informar a los funcionarios, sobre las acciones o mecanismos implementados, para gestionar los incidentes detectados.

DOMINIO	17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
OBJETIVO DE CONTROL	17.1 Continuidad de la seguridad de la información.
CONTROL	*17.1.1 Planificación de la continuidad de la seguridad de la información.*

Sección para la Dirección de TIC, Unidad de TIC y Comité de Gestión de la Seguridad de la Información Institucional:

Artículo 187.- Deberán ejecutar Planes de Continuidad y de Recuperación ante desastres, con las siguientes consideraciones:

- Deberán sustentarse en un proceso previo de Análisis de Riesgos.
- Deberá priorizarse los recursos de información de acuerdo a su nivel de riesgo.
- Se deberá definir la mejor estrategia para preservar la continuidad de los servicios.
- Los Planes de Continuidad y Recuperación, deberán obedecer a la estrategia elegida.
- Los planes ejecutados deberán ser debidamente documentados y socializados.
- Los planes ejecutados deberán ser revisados periódicamente, para evaluar la vigencia de su estrategia.

DOMINIO	18. CUMPLIMIENTO.
OBJETIVO DE CONTROL	18.1 Cumplimiento de los requisitos legales y contractuales.
CONTROL	*18.1.1 Cumplimiento de las políticas y normas de seguridad.*

Artículo 188.- Los lineamientos de la presente guía, deberán ser cumplidos y acatados a cabalidad y sin excepciones, por parte de todos los funcionarios y terceros relacionados con la institución.

Artículo 189.- La violación de las directrices establecidas, supondrá acciones disciplinarias conforme los Reglamentos y Leyes correspondientes.

Artículo 190.- Los servidores cuentan con la autorización para informar o reportar a las autoridades, sobre las acciones de incumplimiento a la presente normativa.

Sección para la Unidad de TIC y Comité de Gestión de la Seguridad de la Información Institucional:

Artículo 191.- Deberán supervisar las acciones de los funcionarios y terceros, de tal forma que no interrumpa sus actividades laborales, con la finalidad de detectar incumplimientos a la normativa.

Artículo 192.- Deberán documentar las acciones de incumplimiento detectadas, como sustento para los procesos correctivos y de penalización.

DOMINIO	18. CUMPLIMIENTO.
OBJETIVO DE CONTROL	18.1 Cumplimiento de los requisitos legales y contractuales.
CONTROL	*18.1.2 Identificación de la legislación aplicable.*

Artículo 193.- Las penalizaciones por el incumplimiento a la normativa, corresponderán a llamados de atención de manera verbal o escrita por parte de la máxima autoridad y en caso de reincidencias, se basarán en las sanciones estipuladas en el Reglamento interno institucional.

Las Políticas expuestas se basaron en los datos extraídos del proceso de evaluación del riesgo ejecutado previamente, respecto a los servicios relevantes, tipo de información manejada, recursos críticos y amenazas resultantes, en concordancia con las necesidades institucionales y bajo los criterios de los responsables de los activos, autoridades y funcionarios con mayor nivel de experticia.

Mediante los Controles propuestos, se ha podido considerar y abarcar gran parte de las preocupaciones institucionales en relación al resguardo de su información, y mediante su adopción, se pretende formalizar las actividades y procesos del ámbito de TI organizacional.

4.4.Evaluación

En este apartado se desplegará un resumen de los resultados y principales impresiones obtenidas en cada una de las etapas que conforman el presente estudio, y se recogerán algunas propuestas, que a criterio de los expertos y en base a los resultados obtenidos, fueron consideradas para complementar el enfoque de este trabajo investigativo.

Tabla 28.Resumen de resultados (Etapa 1)

Etapa 1: Análisis del entorno	
Entregable	Listado de servicios relevantes *Referencia en el documento: Tabla 8 y Figura 2*

- Con la finalidad de conocer estructuralmente la institución y sus principales servicios, se ejecutaron entrevistas a los responsables de cada Unidad Organizacional de manera virtual, y adicionalmente, se procedió con la revisión de su documentación interna, con la previa autorización del Director Regional.
- Esta etapa inicial, contribuyó con la comprensión del entorno de estudio que requiere ser protegido y de las necesidades en materia de seguridad que demanda su personal y recursos.
- La identificación de los servicios prestados que generan mayor impacto en la institución, contribuyó con la tarea de identificación sus recursos de información con mayor nivel de sensibilidad.

Elaboración Propia

Tabla 29.Resumen de resultados (Etapa 2)

Etapa 2: Análisis del Riesgo	
Entregables	Listado de activos críticos *Referencia en el documento: ANEXO 3- ActCríticovsResp*
	Listado de amenazas resultantes *Referencia en el documento: ANEXO 3- AmeResul*

- La identificación de activos, requirió de la revisión de los inventarios de equipos y su constatación in situ.
- La valoración de activos y amenazas, así como las tareas de estimación de impacto y riesgo, requirieron la ejecución de reuniones virtuales para la ejecución de debates controlados.
- Se obtuvo a final, un listado de activos críticos con sus responsables, y un compendio de amenazas relacionadas.

Elaboración Propia

Tabla 30.Resumen de resultados (Etapa 3)

Etapa 3: Gestión del Riesgo	
Entregables	Manual de Políticas *Referencia en el documento: 4.3.7. Definición de Políticas de Seguridad de la Información basadas en la Norma ISO/IEC 27002 para el Ministerio del Trabajo (Ibarra)*
	Matriz RACI *Referencia en el documento: ANEXO 4* Hoja de Ruta *Referencia en el documento: ANEXO 5*

- Los controles de la Norma ISO/IEC 27002:2013 fueron seleccionados conforme el criterio del personal técnico competente, y en concordancia con los objetivos de la entidad.
- Como requisito inicial del documento de Políticas, también fue necesario el establecimiento del Comité de Gestión de Seguridad de la Información, representado actualmente por el encargado de la Unidad de TIC y un representante de cada Unidad Organizacional.

- Las políticas están dirigidas a los servidores y terceros, para modelar sus tareas de gestión de la información institucional y sus recursos, así como el afinamiento de los procesos relacionados con la adquisición, baja o mantenimiento de su equipamiento.
- En vista del actual estado de emergencia sanitaria, la presente guía fue difundida a través de canales de comunicación tecnológicos como: mail institucional y Sistema de Gestión Documental Quipux.
- Finalmente, por petición del personal institucional, se procedió con la realización de un Modelo de Hoja de Ruta y Matriz RACI, con el objetivo de obtener una planificación de las tareas y recursos humanos, necesarios para la implementación de la Metodología propuesta.

  Mediante estas herramientas, se podrá realizar el lanzamiento del proyecto de forma mucho más ágil, garantizando un control y seguimiento adecuado de sus recursos, y permitiendo su réplica o extrapolación en nuevos escenarios.

Elaboración Propia

5. Conclusiones y Trabajo Futuro

5.1.Conclusiones

- La evaluación del riesgo previa, fue vital para conocer los recursos sensibles que ameritan ser protegidos de manera prioritaria y fue necesaria para identificar los factores que desencadenan ese estado de vulnerabilidad.
- Como medida inicial, se procedió con la asignación de custodios para los recursos sensibles, quienes velarán por su integridad, en apoyo constante al Comité de Seguridad de la Información Institucional y Unidad de TIC.
- Se pudo determinar que las principales incidencias de seguridad se originan de los errores involuntarios de sus funcionarios, en el ejercicio de sus actividades laborales diarias.
- Se pudo evidenciar falencias en los procesos de TI, por parte de sus administradores, principalmente en las tareas de mantenimiento, adquisición y baja de equipamiento.

- En un inicio, se detectó exceso de confianza y desestimación de los riesgos en sus autoridades, lo cual se fue modificando en el transcurso del desarrollo del proyecto, hasta la obtención de su compromiso y apoyo total.
- Se corroboró el valor de la información institucional, la cual arrojó un alto grado de sensibilidad, demostrando su importancia de cara a la preservación de los niveles de confianza e imagen institucional.
- Los Dominios y Controles seleccionados abarcaron todos los ámbitos que ameritaban ser regulados, y con un nivel de granularidad adecuado. En este sentido, se obtuvo una solución integral, y adaptada a los requerimientos y metas de la organización.
- La presente guía amerita ser revisada de manera periódica, con la finalidad de garantizar su vigencia y valía, frente a los cambios constantes del entorno de riesgos, infraestructura tecnológica y requerimientos emergentes.
- Una debida difusión del documento y la oportuna capacitación a sus funcionarios, será factor esencial para el éxito del proyecto; si bien no será la solución definitiva, sin embargo, apoyará enormemente las tareas de concientización del personal y la creación de una cultura organizacional.
- En síntesis, se pudo obtener una solución integral, que combina medidas técnicas y administrativas, mediante el acoplamiento de dos Normas/Metodologías reconocidas como MAGERIT e ISO 27002.

Para culminar el presente apartado, se presenta un resumen del problema que ha sido abordado dentro del ámbito de aplicación propuesto, y de los resultados obtenidos tras la ejecución de las distintas etapas del proyecto, los cuales guardan relación con los objetivos planteados inicialmente.

Tabla 31.Conclusiones

Problema tratado	Etapa	Resultado obtenido	Relación
Desconocimiento de lo que se necesita proteger	Análisis del Riesgo	• Activos de información identificados, valorados y tipificados. • Información debidamente clasificada. • Inventariado de equipos actualizados.	*Objetivo 1*

Desconocimiento de las potenciales amenazas		• Amenazas identificadas, valoradas y clasificadas. • Concientización del impacto. • Salvaguardas actuales identificadas y valoradas. • Recomendaciones de nuevas salvaguardas.	*Objetivo 2*
Desconocimiento del Riesgo		• Valores cualitativos de Impacto y Riesgo • Lista de Activos críticos • Custodios de activos críticos • Lista de Amenazas resultantes • Concientización del riesgo.	
Gestión de la Seguridad de la información, fuera de los objetivos institucionales	Gestión del Riesgo	• Compromiso de las autoridades con la gestión de la seguridad de la información institucional. • Aplicación de procesos de análisis y gestión del riesgo. • Manual de Políticas de Seguridad de la Información. • Difusión de las Políticas. • Apertura a nuevas propuestas o proyectos futuros.	*Objetivo 3*
Personas no involucradas, desatendidas y sin responsabilidades en temas de seguridad.		• Establecimiento del Comité de Gestión de la Seguridad de la información institucional. • Definición de roles y responsabilidades dentro del Comité. • Asignación de custodios o responsables para los activos. • Cumplimiento de las Políticas por parte de los funcionarios. • Participación activa del personal, para notificación de incidentes. • Establecimiento de una Cultura organizacional.	
Requerimientos y preocupaciones del personal institucional.		• Políticas de seguridad revisadas y validadas por personal experto. • Matriz RACI y Hoja de ruta para organizar la implementación de la propuesta.	*Objetivo 4*

Elaboración Propia

5.2.Recomendaciones

- Una adecuada gestión de riesgos asociados a TI, debe sustentarse en los lineamientos y directrices de metodologías o normativas reconocidas y aceptadas por las organizaciones a nivel internacional, para garantizar que sus procesos sean homologados y sus resultados sean fiables.
- Es indispensable mantener contacto frecuente con los "dueños" de la información y recursos, puesto que su experticia, y criterio serán clave para conocer la realidad del ámbito de estudio.
- La ejecución de charlas de capacitación y sensibilización destinadas al personal objetivo, son requisito indispensable para que una normativa proporcione el efecto y resultados esperados. Es recomendable que sean ejecutadas con una periodicidad adecuada, en lapsos de tiempo prudenciales, y en ambientes distendidos, de modo que se mantenga el compromiso y motivación de las personas.
- La normativa deberá ser revisada y actualizada, conforme los nuevos criterios y requerimientos institucionales. Será preciso, la ejecución de nuevas versiones que evolucionen a la par de los riesgos asociados a las nuevas tecnologías.
- Es recomendable que las entidades de la Administración Pública ecuatoriana, también se adhieran a los lineamientos del Esquema Gubernamental de Seguridad de la Información (EGSI) según el Acuerdo Ministerial No. 166, para estar en total conformidad con las leyes vigentes.

5.3.Líneas de Trabajo Futuro

- En vista de los recurrentes incidentes de seguridad originados por errores no intencionados de las personas, en el desarrollo de sus actividades laborales diarias, es recomendable la elaboración de un Manual de procedimientos institucional, que permita formalizar y estandarizar sus tareas y que complemente el campo de acción de las Políticas propuestas.
- En esta misma línea, con el propósito de aportar con la optimización de la gestión de dichas incidencias tecnológicas, y la necesidad de asistir adecuadamente a los funcionarios para minimizar sus errores en el manejo de

los recursos, se recomienda automatizar el Servicio de Mesa de Ayuda institucional, a través de herramientas de machine learning, como chatbots personalizados, los cuales permitan brindar un servicio de asistencia virtual de forma inmediata, acorde al perfil del funcionario, y con la capacidad de generar una base de conocimientos para predecir incidentes futuros.

- Para complementar la acción de sus herramientas técnicas para filtrado de tráfico, como su antivirus y firewall institucional, se podría implementar un Sistema de Prevención de Intrusos basado en software libre, el cual permita filtrar los paquetes de datos a nivel interno y externo, basado en el análisis de su contenido y no únicamente en los puertos o protocolos usados, como lo hacen las herramientas tradicionales antes mencionadas.
- En virtud de que la institución, cuenta actualmente con un programa de evaluación de riesgos vigente, podría optar como proyecto complementario, el desarrollo de un Plan de Contingencias y un Plan de Recuperación ante desastres informáticos, que le permitan cambiar su estrategia a un enfoque de riesgos proactivo, para que pueda anticiparse y reaccionar efectivamente ante la materialización de alguna amenaza.
- Con la finalidad de mantener un control y seguimiento adecuado de los riesgos de TI, será necesaria su evaluación permanente y periódica a través del tiempo, por lo que la institución deberá considerar que el proceso deberá seguir un camino iterativo. Bajo esta premisa, la organización podría optar a futuro por la implementación de programas de evaluación con enfoques probabilísticos basados en modelos matemáticos como fuzy logic, para determinar los niveles de riesgos con mayor precisión respecto a los modelos cualitativos basados en criterios de expertos. Sin embargo, mucho tendrá que ver el nivel de madurez en el que la institución se encuentre, respecto a la experticia de su personal y la ruptura de su enfoque tradicional.

REFERENCIAS BIBLIOGRÁFICAS

Altamirano, J. y Bayona, S. (2017). Políticas de Seguridad de la Información: Revisión Sistemática de las Teorías que Explican su Cumplimiento. *Revista Ibérica de Sistemas y Tecnologías de Información*, *25*(10), 112-134. http://www.scielo.mec.pt/pdf/rist/n25/n25a09.pdf.

Arévalo, F., Cedillo, I. y Moscoso, S. (2017). Metodología Ágil para la Gestión de Riesgos Informáticos. *Revista Killkana Técnica*, *1*(2), 31-42. https://killkana.ucacue.edu.ec/index.php/killkana_tecnico/article/view/81/122

Contero, W. (2019*). Diseño de una Política de Seguridad de la Información basada en la Norma ISO 27002:2013, para el Sistema de Botones de Seguridad del Ministerio del Interior.* [Tesis de maestría, SEK]. Repositorio digital de la Universidad Internacional SEK. https://repositorio.uisek.edu.ec/handle/123456789/3345

Crespo, E. y Cordero, G. (2018). Estudio comparativo entre las Metodologías CRAMM y MAGERIT para la gestión de riesgo de ti en las MPYMES. *UDA AKADEM,* (1). http://udaakadem.uazuay.edu.ec/article/view/129

Domínguez, H., Maya, E., Peluffo, D. y Crisanto, C. (2017). Aplicación de técnicas de fuerza bruta con diccionario de datos, para vulnerar servicios con métodos de autenticación simple “Contraseñas”, pruebas de concepto con software libre y su remediación. *Revista MASKANA*, *7*(Supl.), 87-95. https://publicaciones.ucuenca.edu.ec/ojs/index.php/maskana/article/view/1079

Gantiva, L. (2020). Gestión de Riesgos en el Internet de las Cosas (IOT). Universidad Piloto de Colombia. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6868/Risk%20management%20IoT_LAGH%20V5.pdf?sequence=1&isAllowed=y

Holguín, F. (2018). *Modelo de Madurez para el Análisis de Riesgos de los Activos de Información basado en las Metodologías MAGERIT, OCTAVE y MEHARI; con enfoque a Empresas Navieras*. [Tesis de maestría, UEES]. Repositorio digital de la Universidad Espíritu Santo.http://repositorio.uees.edu.ec/bitstream/123456789/2763/1/HOLGUIN%20GARCIA%20FRESIA%20YANINA.pdf

Ministerio del Trabajo. (2019). *Plan Estratégico Institucional 2019 – 2021*. https://www.trabajo.gob.ec/wp-content/uploads/2020/12/Plan-Estrategico-2019-2021.pdf?x42051

Ministerio del Trabajo. (2021). *Informe de Gestión-2020*. https://www.trabajo.gob.ec/wp-content/uploads/2021/04/INFORME-DE-GESTION-DIRECCION-REGIONAL-IBARRA_compressed1.pdf?x42051&x42051

Muñoz, J. y Ponce, D. (2017). Metodología para seleccionar políticas de seguridad informática en un establecimiento de educación superior. *Revista MASKANA*, *8*(1), 1-8. https://publicaciones.ucuenca.edu.ec/ojs/index.php/maskana/article/view/1961/

Parra, J. (2019). *Amenazas persistentes avanzadas y su impacto en Latinoamérica ¿cómo estar preparados?.* Universidad Piloto de Colombia. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6285/00005219.pdf?sequence=1&isAllowed=y

Pérez, B. (2020). *Importancia de un sistema de gestión de seguridad de la información para empresas de tecnología.* Universidad Piloto de Colombia. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6841/Articulo.pdf?sequence=1&isAllowed=y

Recalde, J. (2019). *Plan de implementación de un SGSI y aplicación de controles críticos en el Centro de Operaciones de Seguridad en la Empresa GMS.* [Tesis de pregrado, Escuela Politécnica Nacional]. Repositorio Digital Institucional de la Escuela Politécnica Nacional. https://bibdigital.epn.edu.ec/bitstream/15000/20530/1/CD%2010022.pdf

Santonja, J. (2019). *Análisis y correlación entre probabilidad e impacto de los riesgos.* [Tesis de maestría, Universidad de Alicante]. Repositorio institucional de la Universidad de Alicante. https://rua.ua.es/dspace/bitstream/10045/93271/1/Analisis_y_correlacion_entre_probabilidad_e_impacto_de_l_Santonja_Lillo_Juan.pdf

Urgilés, C. y Caiza, E. (2017). La concientización como factor crítico para la gestión de la seguridad de la información. *Revista Killkana Técnica*, *1*(3), 1-8. https://killkana.ucacue.edu.ec/index.php/killkana_tecnico/article/view/109/145

Ministerio de Hacienda y Administraciones Públicas. (2012). *MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Portal de Administración Electrónica. https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.htmlInternational Organization for Standardization (ISO). (2013). *Information technology — Security techniques — Information security management systems — Requirements* (estándar ISO/IEC 27001:2005). https://www.iso.org/standard/42103.html

International Organization for Standardization (ISO). (2013). *Information technology — Security techniques — Code of practice for information security controls* (estándar ISO/IEC 27002:2013). https://www.iso.org/standard/54533.html

Central Communication and Telecommunication Agency (CCTA). (s.f.). *CRAMM.* ENISA. https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html

Carnegie Mellon University (CMU). (2001). *OCTAVE Method Implementation Guide Version 2.0 Volume 1: Introduction.* Software Engineering Institute. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=51558

Carnegie Mellon University (CMU). (2009). *CMMI: A Short History.* Software Engineering Institute. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=28414

Club de la Sécurité de l'Information Français (CLUSIF). (s.f.). *Espace Risques et Méthodes.* Groupes et espaces de travail. https://clusif.fr/les-groupes-de-travail-du-clusif/risques-et-methodes/

Central Communication and Telecommunication Agency (CCTA). (s.f.). *ITIL.* ENISA. https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/business-process-integration/operational-it-processes/itil

ANEXO 1. ESTIMACIÓN DEL RIESGO EN LOS ACTIVOS DEL MINISTERIO DEL TRABAJO (IBARRA).

ANEXO 2. RELACIÓN AMENAZA-TIPO DE ACTIVO AFECTADO

ANEXO 3. RESULTADOS DEL ANÁLISIS DEL RIESGO

ANEXO 4. MATRIZ RACI

ANEXO 5. HOJA DE RUTA