OFICINA DE POSGRADOS

Tema:

GUÍA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL GOBIERNO PROVINCIAL DE TUNGURAHUA

Proyecto de Investigación y Desarrollo previo a la obtención del título de Magister en Ciberseguridad

Línea de Investigación:

Seguridad de la Información

Autor:

Víctor Félix Barrezueta Bermeo

Director:

Mg. Jaime Gabriel Llumiquinga Veintimilla

Ambato - Ecuador

Junio 2023

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE AMBATO

APROBACIÓN DEL TRIBUNAL DE GRADO

Tema:

GUÍA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL GOBIERNO PROVINCIAL DE TUNGURAHUA

Línea de investigación:

Seguridad de la Información

Autor:

Víctor Félix Barrezueta Bermeo

Jaime Gabriel Llumiquinga Veintimilla, Ing. Mg. f._____

CALIFICADOR

Ricardo Patricio Medina Chicaiza, Ing. PhD. .f._____

CALIFICADOR

Enrique Xavier Garcés Freire, Ing. Mg. f._____

CALIFICADOR

Juan Carlos Acosta Teneda, P. PhD. f._____

COORDINADOR OFICINA DE POSGRADOS

Hugo Rogelio Altamirano Villarroel, Dr. f._____

SECRETARIO GENERAL PUCESA

Ambato – Ecuador

Junio 2023

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo: **VÍCTOR FÉLIX BARREZUETA BERMEO**, con CC **1803838851**, autor del trabajo de grado intitulado: "GUÍA DE GESTIÓN DE SEGURIDAD DE LA INFORMACION PARA EL GOBIERNO PROVINCIAL DE TUNGURAHUA", previa a la obtención del título profesional de **MAGISTER EN CIBERSEGURIDAD**, en la **OFICINA DE POSGRADOS**.

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

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

Ambato, junio 2023

Víctor Félix Barrezueta Bermeo
CC. 1803838851

DEDICATORIA

A Dios por bendecirme cada día y permitirme soñar y seguir haciendo esos sueños realidad. A mi madre y mi hermosa familia por su motivación quienes con su amor me han dado tanta felicidad.

AGRADECIMIENTO

A Dios, mi más grande amor e inspiración; contigo todo, sin ti nada, por ser el forjador de esta meta. A mi madre luchadora incansable y a mi hermosa familia por su apoyo incondicional sin importar el tiempo y el espacio del trayecto, los amo con todo mi corazón.

A mi tutor Mg. Gabriel Llumiquinga quien fue el artífice de lograr este trabajo, sin su experiencia, paciencia, tiempo no lo hubiera logrado, mi agradecimiento sincero.

RESUMEN

Actualmente uno de los activos con más valor en las organizaciones públicas como privadas es la información, la cual necesita ser protegida ante cualquier eventualidad de riesgo a la que estaría expuesta. De esta forma el objetivo del presente proyecto es establecer una Guía de Gestión de Seguridad de la Información que permita desarrollar criterios y lineamientos que garanticen la seguridad de los activos de información más críticos de la institución, mitigue los riesgos y permita establecer políticas, normas y procedimientos adecuados, de tal manera para la realización de esta guía se ha utilizado como base la Metodología Magerit para la evaluación de riesgos, las directrices establecidas en la Norma Internacional ISO/IEC 27005:2018 y el Esquema Gubernamental de Seguridad de la Información (EGSI), el cual está basado en las normas técnicas ecuatorianas INEN ISO/IEC 27000 para la Gestión de la Seguridad de la Información. Al utilizarlos de forma conjunta brindan los lineamientos necesarios para conformar la presente guía de Seguridad de la Información para el Gobierno Provincial de Tungurahua.

Palabras Claves: riesgos, seguridad, información, esquema gubernamental.

ABSTRACT

Currently, one of the most valuable assets in public and private organizations is information, which requires protection against any eventual risk under it may be exposed. Thus, this study objective is to establish an Information Security Management Guide that allows the development of criteria and guidelines to ensure the institution security of its most critical information assets, mitigate risks and allow the establishment of policies, standards and appropriate procedures. Consequently, the Magerit Methodology for risk assessment, the guidelines established in the International Standard ISO/IEC 27005:2018 and the Governmental Information Security Scheme (EGSI), which is based on the Ecuadorian technical standards INEN ISO/IEC 27000 for Information Security Management, were used. When combined, they provide the necessary guidelines to create this Information Security Guide for the Provincial Government of Tungurahua.

Keywords: risk, security, information, governmental scheme.

ÍNDICE

PRELIMINARES

INTRODUCCIÓN

Hoy en día, las instituciones públicas han experimentado un sin número de cambios tecnológicos, al implementar infraestructura tecnológica que les permita ofrecer a sus funcionarios la posibilidad de conectarse al mundo, con el propósito de brindar una calidad de servicio óptima, y de esta forma mejorar los niveles de competitividad. Un aspecto importante, que se resguarda en una institución ya sea esta pública o privada es sin duda alguna la información. La información, en todas sus formas, son uno de los principales activos de cualquier institución.

El 16 de septiembre de 2019, un artículo publicado por la BBC titulado "Filtración de datos en Ecuador: la 'grave falla informática' que expuso la información personal de casi toda la población del país sudamericano", menciona sobre la filtración de información personal de millones de personas a través de una empresa ecuatoriana de marketing, análisis de datos y desarrollo de software Novaestrat, sin duda una noticia alarmante para los Ecuatorianos, debido a que dicha información contenía nombres, información financiera, datos civiles, registros del Gobierno, datos del Instituto Ecuatoriano de Seguridad Social (IESS), Servicio de Rentas Internas (SRI), Banco del Instituto Ecuatoriano de Seguridad Social (BIESS), entre otros.

De acuerdo con la empresa de seguridad informática vpnMentor, la empresa que administraba todos estos datos no contaba con los requisitos de seguridad mínimos establecidos, lo cual representa como una de las mayores filtraciones en línea de información personal sufridas en el país y a nivel de Latinoamérica, dado por el número de personas expuestas (BBC News Mundo, 2019).

En el sector público Ecuatoriano grandes empresas públicas han sufrido enormes y cuantiosas pérdidas económicas debido a ciberataques, hackeo con ransomware a CNT (Agosto 2021), ataque digital en el sistema AXIS a la Agencia Nacional de Tránsito (Octubre 2021), hackeo a la infraestructura tecnológica al Municipio de Quito (Abril 2022), estos ataques presumen una deficiente gestión de riesgos de seguridad de la información. Además, cabe

indicar que este tipo de incidentes, no se puntualiza únicamente en el tema económico, también se enfoca en la interrupción y caídas de servicio lo que provoca una avalancha de consecuencias para los usuarios que dependen o necesitan de estos servicios.

Como lo cita Luis Enrique (Coordinador del Observatorio de ciberderechos y tecnosociedad de la Universidad Andina Simón Bolívar) “Los altos funcionarios no entienden la importancia del Valor al Riesgo en la ciberseguridad, y mucho menos el costo de la pérdida de confidencialidad, integridad y disponibilidad en los datos personales de los ciudadanos. Esta omisión conduce a la toma de decisiones desinformadas y una mala gestión en la inversión de medidas de seguridad organizacionales y técnicas de seguridad.

Si se considera que las medidas de tratamiento de riesgos de seguridad son eficaces y rentables, la ausencia de metodologías métricas para medir su rendimiento hace que el Estado siempre termine pagando más dinero por menos resultados” (Enríquez, 2022).

En el artículo profesional de alto nivel elaborado por (Ortiz, 2022) titulado “El control Gubernamental y las amenazas disruptivas en Ecuador”, desde el enfoque de un profesional de auditoría del sector público, se mencionan los desafíos que representan las innovaciones disruptivas en los procesos técnicos de auditorías, así como el enfoque de la gestión de tecnologías de la información.

En base a los hechos ocurridos en el Ecuador y que son de conocimiento público, el enfoque se basa en la necesidad de innovación que surge como respuesta a un ambiente creciente de cambios, los hechos suscitados en el Ecuador, no se deberían ocultar y se muestra tal y como sucedieron, de tal forma que estos hechos sirvan para buscar nuevas alternativas de ciberseguridad y como tal adaptarse a un entorno cambiante de la tecnología.

La realidad es que las instituciones públicas tienen dificultades para afrontar cambios y nuevos desafíos, las reglas que se establecen a nivel de gobierno

muchas veces, no se enmarcan en una realidad institucional, el hecho de tratar de asumir nuevos desafíos también implica asumir nuevas responsabilidades, en un marco jurídico con reglas caducas y difíciles de cambiar, resulta imperioso empezar a trabajar internamente en base a necesidades reales y que permitan hacer frente a las amenazas a las cuales toda institución pública está expuesta.

Los autores (Ramírez & Rinconc, 2022) afirman que las instituciones públicas tienen la obligación constitucional de proteger la información, que se maneja de los ciudadanos. Así mismo mencionan que la información es un activo vital dentro de cualquier institución, la seguridad de la información y la ciberseguridad están definidas por un compuesto de instrucciones y elementos, que tienen como misión brindar las tres características fundamentales de la misma como son: disponibilidad, confidencialidad, integridad; implementar políticas y controles de seguridad de los datos se ha convertido en un proceso de vital importancia para que las organizaciones mantengan salvaguardada sus sistemas de ataques, daños o pérdidas.

No obstante, en el artículo científico desarrollado por los autores (Solarte, Enriquez, & Benavides, 2015), manifiestan que para lograr una adecuada protección de los activos informáticos, los sistemas de información, los datos y la información, es necesaria la intervención de todo el personal de la empresa, que incluye a los directivos que avalan el proyecto y brindan el apoyo a todo el personal que esté involucrado en el manejo de los activos y sistemas informáticos. Estas acciones estarán enmarcadas en un proceso lógico, sistemático, documentado, que se difundirá internamente para garantizar la gestión correcta de la seguridad informática y de la información, y continuar el ciclo de mejora continua (planear, hacer, verificar y actuar – PHVA)

En el mismo sentido la investigación desarrollada por (Abril, Pulido, & Bohada, 2013), argumentan que es de vital importancia que en las empresas se establezcan objetivos empresariales y, a partir de ellos, políticas de seguridad que permitan controlar la realización de los procesos para así optimizar el análisis de riesgos.

Las organizaciones están expuestas día a día a amenazas tanto internas como externas que ocasionan robo de identidad e información, bases de datos, información sensible de clientes, pérdida de credibilidad y daños financieros que afectan la sostenibilidad de la entidad, por lo anterior, se cuestiona si las empresas conocen y aplican metodologías para el análisis de riesgos y protección de los principios de seguridad de la información o por el contrario desconocen los modelos que traigan protección de los principios de seguridad de la información.

Para complementar lo expuesto anteriormente la investigación desarrollada por (Mahecha & Coello, 2016) titulada “Desarrollo de un Sistemas de Información para gestionar la implantación mantenimiento y mejora continua de un sistema de gestión de seguridad de la información basado en la Norma ISO 27001:2013”, realiza un análisis en la que se menciona que la seguridad de la Información en Ecuador todavía no consigue los niveles de reconocimiento a nivel empresarial que tienen otras normas de la misma familia, ISO 9001 y 14001 por ejemplo, sin embargo, se destaca que el gobierno ha tenido una iniciativa interesante al respecto.

La promulgación del Acuerdo Ministerial 166 de la Secretaría Nacional de la Administración Pública (SNAP) que fija las actividades principales que las entidades y empresas públicas deben cumplir para implementar el Esquema Gubernamental de Seguridad de la Información, el cual está basado en la Norma ISO 27001:2005. En el sector financiero la Resolución 3066 de la Junta Bancaria también propugna la implementación de Sistemas para Gestión de la Seguridad de la Información (SGSI) y garantías para la continuidad el negocio en el marco de la gestión de riesgos corporativos.

Por otro lado, el sector privado, de manera gradual e incipiente, también empieza a interesarse en destacar que en sus procesos se tiene un buen manejo de la confidencialidad de la información que maneja, así que la expectativa en el corto y mediano plazo es que exista un aumento de la demanda de organizaciones que buscarán certificarse en la Norma ISO 27001.

Con respecto al enfoque normativo legal que rige la legislación Ecuatoriana existe una tesis de investigación elaborada por (Gaibor, 2008) que manifiesta que la legislación ecuatoriana contempla sanciones y tipifica delitos como la omisión de responsabilidades en la difusión de información, el perder o difundir información no autorizada, el vulnerar información confidencial, etc.

La legislación ecuatoriana y los convenios internacionales firmados por el Ecuador evidencian la necesidad de elaborar Políticas de Seguridad de la Información que permitan garantizar la integridad, confidencialidad y disponibilidad de la información. La elaboración de dichas políticas se, ceñirá a normas internacionales que garanticen su éxito, estas políticas estarán elaboradas a medida, es decir, a la realidad de la institución, además de definir las responsabilidades de la misma, fijar objetivos y evaluar continuamente el correcto funcionamiento de dichas políticas.

En el ámbito local desde un enfoque Institucional el Gobierno Provincial de Tungurahua (GPT) es una institución pública que pertenece a los Gobiernos Autónomos Descentralizados del País, lo cual se constituye como la clave para el desarrollo de la provincia, en su condición de referente en impulsar iniciativas para el desarrollo económico, social, ambiental y territorial en Tungurahua.

En el GPT no existe un área específica, unidad de apoyo o sección departamental que gestione la seguridad de la información y los riesgos asociados. En este contexto, resulta importante desarrollar una guía que garantice la seguridad de los activos de información más críticos de la institución, mitigue los riesgos y permita establecer políticas, normas y procedimientos adecuados.

El propósito del presente trabajo de investigación es desarrollar una guía para la gestión de seguridad de la información en el Gobierno Provincial de Tungurahua en base a un análisis a través de la metodología de gestión de riesgos Magerit, las directrices establecidas en la Norma Internacional ISO/IEC 27005:2018 y el Esquema Gubernamental de Seguridad de la Información

EGSI el cual está basado en las normas técnicas ecuatorianas INEN ISO/IEC 27000 para la Gestión de la Seguridad de la Información.

El EGSI establece recomendaciones y ofrece un conjunto de lineamientos para la Gestión de la Seguridad de la Información y ejecuta un proceso de mejora continua. La metodología de gestión de riesgos propuesta servirá para determinar los riesgos y establecer las contramedidas que sean necesarias en torno a la realidad del Gobierno Provincial de Tungurahua.

Una vez aplicada la evaluación de riesgos, la Norma Internacional, la metodología de gestión de riesgos y el Esquema Gubernamental de Seguridad de la Información EGSI se propondrá el desarrollo de una guía para gestionar la seguridad de la información en el Gobierno Provincial de Tungurahua.

Actualmente uno de los inconvenientes a los que se enfrentan las instituciones gubernamentales es la seguridad de la información, y resulta un riesgo inminente el hecho de no contar con un área específica, que se encargue de analizar, gestionar e implementar mejoras continuas para mitigar riesgos que afecten a la seguridad de la información.

Adicionalmente es imprescindible contar con una Guía que gestione la Seguridad de la Información, la cual estará adaptada al entorno específico y a la realidad de cada organización.

La seguridad de la información tiene como propósito la protección de la información contra una amplia gama de amenazas; para minimizar los daños, ampliar las oportunidades del negocio, maximizar el retorno de las inversiones y asegurar la continuidad del negocio. Todo esto se logra mediante la implementación de un conjunto adecuado de políticas, procesos, procedimientos, organización, controles, hardware y software y, lo más importante, mediante comportamientos éticos de las personas (Baldecchi, 2014).

Actualmente dentro del Departamento de Sistemas del Gobierno Provincial de Tungurahua, no se cuenta con la documentación y lineamientos específicos para el tratamiento de eventualidades asociados con la seguridad de la información, no se han determinado niveles de seguridad y tampoco se han establecido contramedidas que contribuyan al control y mitigación de los riesgos que desencadenaría un posible ataque, robo o pérdida de información.

De acuerdo con lo expuesto la idea a defender es: contar con una guía que gestione la seguridad de la información en el Gobierno Provincial de Tungurahua, conocer los activos de mayor, menor relevancia y sensibilidad con respecto a la información, de igual forma contar con lineamientos y políticas en base a normativa internacional que permita gestionar los riesgos asociados a la seguridad de la información.

El objetivo del presente proyecto es elaborar una guía de gestión de seguridad de la información para el Gobierno Provincial de Tungurahua que permitirá gestionar activos y riesgos de seguridad de la información con el cumplimiento de los siguientes objetivos específicos:

1. Analizar la situación actual de seguridad de la información del Gobierno Provincial de Tungurahua.
2. Identificar los activos de mayor riesgo y grado de criticidad con respecto a la seguridad de la información dentro del Gobierno Provincial de Tungurahua.
3. Definir el alcance del Esquema Gubernamental de Seguridad de la Información (EGSI) aplicable dentro del Gobierno Provincial de Tungurahua.

El tipo de investigación del presente proyecto de investigación es no experimental, partiendo de un entorno en donde los hechos ya se han suscitado, el estudio está basado en el análisis de gestión de riesgos Magerit, las directrices de la Norma Internacional ISO/IEC 27005:2018 que brinda los lineamientos de las mejores técnicas de seguridad para la gestión de riesgos de seguridad de la información y el Esquema Gubernamental de Seguridad de

la Información V2.0 EGSI, el cual está basado en las normas técnicas ecuatorianas “INEN ISO/IEC 27000”, para la Gestión de la Seguridad de la Información.

La metodología de desarrollo del presente trabajo de investigación tiene como punto de partida la Metodología para el análisis de gestión de riesgos Magerit, de igual forma se toma como referencia las directrices de la Norma Internacional ISO/IEC 27005:2018 y el Esquema Gubernamental de Seguridad de la Información V2.0 EGSI, el cual está basado en las normas técnicas ecuatorianas “INEN ISO/IEC 27000”.

Entre los beneficios que proporciona un SGSI, están la de establecer una metodología de gestión de seguridad, se garantiza la continuidad del negocio, después de enfrentar un incidente de seguridad considerable, garantiza el cumplimiento del marco legal en el Ecuador, mejora e implementa nuevos procesos, lo cual incide directamente en el aumento de la seguridad en base a la gestión de procesos. La implantación de un Sistema de Gestión de Seguridad de la Información es una decisión estratégica que involucra a toda la organización y que se apoyará y dirigirá desde la dirección (Frayssinet, 2014).

Con el incremento de ataques informáticos, sobre todo en el Ecuador se ha creado un marco legal para las Instituciones Públicas, que establece un conjunto de recomendaciones para la Gestión de la Seguridad de la Información y ejecuta un proceso de mejora continua como es el Esquema Gubernamental de Seguridad de la Información EGSI, de tal forma que al complementar estas recomendaciones con una metodología de análisis de gestión de riesgos y las directrices de la Norma Internacional ISO/IEC 27005:2018, se propone una guía de Gestión de Seguridad de la Información para el Gobierno Provincial de Tungurahua que permita mantener la integridad, confidencialidad y disponibilidad de la información y salvaguardar sus activos.

A raíz de la pandemia, el rol de la ciberseguridad tomó mucha relevancia y protagonismo en función de las medidas de protección de datos personales ante posibles manipulaciones o amenazas a la integridad de la información en

empresas públicas y privadas del Ecuador, han tenido que volcar sus esfuerzos en el trabajo remoto sin embargo esto implica mayor riesgo en el tratamiento de los datos y mayor atención en el tema de la gestión de la seguridad de la información.

Uno de los objetivos de las empresas públicas como privadas es precautelar la información y datos personales; la pandemia aceleró en gran medida este proceso, muchas empresas observaron que al aplicar tecnología para la conectividad no era suficiente, el reto es garantizar que esa conectividad sea segura, confiable y sobre todo que la información de la empresa esté protegida.

La falta de directrices y un área específica dedicada a la ciberseguridad también es una falencia que enfrentan empresas públicas y privadas del Ecuador. La falta de procesos, la falta de lineamientos, la falta de guías y políticas que gestionen la seguridad de la información dentro de las empresas se ha marcado cada vez más sobre todo en pandemia, y con ello los riesgos que representa, es por ello que la ciberseguridad dentro de una empresa recibiría mayor atención y mayor apoyo por parte de la alta gerencia, con el fin de obtener mayores y mejores resultados.

De la misma forma cabe mencionar que un modelo de auditoría de ciberseguridad aportaría elementos en función de mejorar la seguridad de la información y al mismo tiempo establecer un marco de trabajo para concientizar sobre la seguridad de la información en los diferentes roles, que se desempeñan dentro de una empresa, institución u organización.

Un ataque por ransomware, es la principal preocupación para las entidades públicas y privadas del Ecuador, según lo detalla Deloitte en un estudio realizado en el año 2021, la filtración de datos y robo de información es considerado como la segunda amenaza de mayor atención. Cabe indicar que en el Ecuador un ataque por ransomware está considerado como secuestro de información tipificado en el Código Orgánico Integral Penal COIP como delito, sancionado con pena privativa de libertad de tres a cinco años.

Con fecha 26 de mayo de 2021 en el Registro Oficial se publicó la Ley Orgánica de Protección de Datos Personales, la cual establece derechos y principios para los titulares de los datos, hace referencia a aquellos datos que permite la identificación de una persona y de alguna manera brinda a los ciudadanos el derecho a la privacidad en el ámbito legal. Se establece un régimen sancionatorio por la vulneración y hechos que afecten el tratamiento y correcto uso de datos personales.

En lo que respecta a una medida de control de seguridad que garantice la privacidad de datos personales, surge la necesidad de un análisis de riesgos y una evaluación de un posible impacto de dichos riesgos; dicho análisis y evaluación dependerá del tipo y volumen de datos personales objeto de tratamiento. Los datos personales es una información considerada altamente sensible y de gran valor, en caso de alguna vulneración e infracción a la seguridad, la Autoridad de protección de datos personales, así como la Superintendencia de Control de Datos Personales cumplirá su rol fundamental como ente rector, regulador y sancionador en materia de protección de datos personales.

El presente proyecto de investigación pretende crear lineamientos que gestionen la seguridad de la información en beneficio del Gobierno Provincial de Tungurahua, en base al Esquema Gubernamental de Seguridad de la Información EGSI creado en base al Acuerdo Ministerial Nro. 025-2019, por el Ministerio de Telecomunicaciones y de la Sociedad de la Información, a través del diseño de una guía, debido a que actualmente en el Gobierno Provincial de Tungurahua, no se cuenta con una guía, norma o procedimiento documentado que garantice la seguridad de la información.

Resulta pertinente trabajar en una guía en base a una evaluación de riesgos, determinar activos en mayor y menor grado de vulnerabilidad y sensibilidad con respecto a la información, aplicar los lineamientos establecidos en el Esquema Gubernamental de Seguridad de la Información EGSI y las directrices establecidas en la Norma Internacional ISO/IEC 27005:2018; mismo que al

aplicarlos de forma conjunta brindan las herramientas necesarias para la elaboración de la guía.

La importancia y beneficio que tiene este proyecto radica en garantizar los pilares de la información, disponibilidad, integridad y confidencialidad, además de establecer una política que establezca roles y responsabilidades, definir excepciones, sanciones y desarrollar un plan que permitan proteger y evaluar los activos imprescindibles para el correcto funcionamiento de la planta tecnológica del Gobierno Provincial de Tungurahua.

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

1.1. Antecedentes

Existen varios trabajos de investigación que detallan desde diferentes puntos de vista, metodologías y perspectivas sobre el análisis de la gestión de riesgos y la seguridad de la información, entre los que se relacionan al presente trabajo de investigación se mencionan los siguientes, el trabajo de investigación titulado “propuesta metodológica de gestión de riesgos de tecnología de información y comunicación (TIC) para entidades públicas conforme normativa NTE INEN ISO/IEC 27005” elaborada por (Patiño, 2018).

Se desarrolla una guía en base a un estudio cuali-cuantitativo con un muestreo no probabilístico que describe las etapas y actividades para establecer una adecuada gestión de los riesgos relacionados con las tecnologías de la información y comunicación y su aplicabilidad en el sector público, lo cual establece un punto de partida de lineamientos enfocados a entidades públicas para obtener información paso a paso de cómo llevar a cabo un análisis y evaluación de riesgos enfocados en la seguridad de la información, todo esto dependerá del entorno específico de cada institución en el cual se desarrolle dicha propuesta.

En la “Elaboración de una política de seguridad de la información para una institución pública basado en el esquema gubernamental de seguridad de la información” realizado por (Ávila, 2018), se plantea una política de seguridad de la información se basa en el Esquema Gubernamental de Seguridad de la Información. La institución pública a la cual está dirigido el estudio pertenece al Gobierno Central, razón por la cual resulta imprescindible además de ser obligatorio por ley contar con una política de seguridad de la información, resulta interesante la posición del autor en realizar una comparativa de la metodología de gestión de riesgos y normas ISO utilizadas, lo cual permite extraer lo más importante de cada una de ellas y de esta forma contar con una política de seguridad de la información integral.

El artículo científico denominado “Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios”, presentado por (Castro & Bayona, 2011), aborda una metodología para gestionar riesgos tecnológicos basados en los estándares ISO 31000 e ISO/IEC 27005. Los autores incluyen recomendaciones de cómo se realiza una gestión de riesgos y aseguramiento de la información en tres etapas a nivel físico, nivel lógico y factor humano, desde una perspectiva tecnológica.

En comparación con otros trabajos de investigación resulta muy importante la inclusión del factor humano, factor considerado como amenaza interna dentro de cualquier organización, con una adecuada concienciación sobre la seguridad, con una cultura de seguridad y constante capacitación se mitiga los factores humanos que conducen a riesgos de seguridad de la información para las organizaciones.

En el artículo científico elaborado por (Gómez, Duchimaza, Holguín, & Lindao, 2019) titulado “Plan de contingencia para los equipos y sistemas informáticos utiliza la metodología Magerit” se presenta una investigación basada en análisis, estándares y normas para la elaboración de un plan de contingencia para equipos físicos y sistemas informáticos, esta investigación presenta un resultado bastante interesante en función de resultados que comúnmente arroja el utilizar la metodología MAGERIT.

Los resultados obtenidos en base a esta metodología también incluyen riesgos por desastres naturales, y sectores considerados de alto riesgo, como inundaciones, deslaves, derrumbes, riesgos de robo de equipos por falta de seguridad; la perspectiva de que el análisis de riesgos no solo incluye riesgos de pérdida y robo de información a nivel lógico, la información también está expuesta a nivel físico, aspectos muy importantes a considerar al elaborar un plan de contingencia y sistemas informáticos.

El artículo profesional de alto nivel titulado “Diseño de un sistema de gestión de seguridad de la información para el proceso administrativo de la infraestructura tecnológica de instituciones académicas basado en Magerit” realizado por los

autores (Montalbán, Gómez, & Borré, 2020) proponen una investigación del diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) de una institución educativa ubicada en Cartagena Colombia, al aplicar un proceso administrativo o dicho de otra forma parámetros de evaluación de gestión de una infraestructura tecnológica.

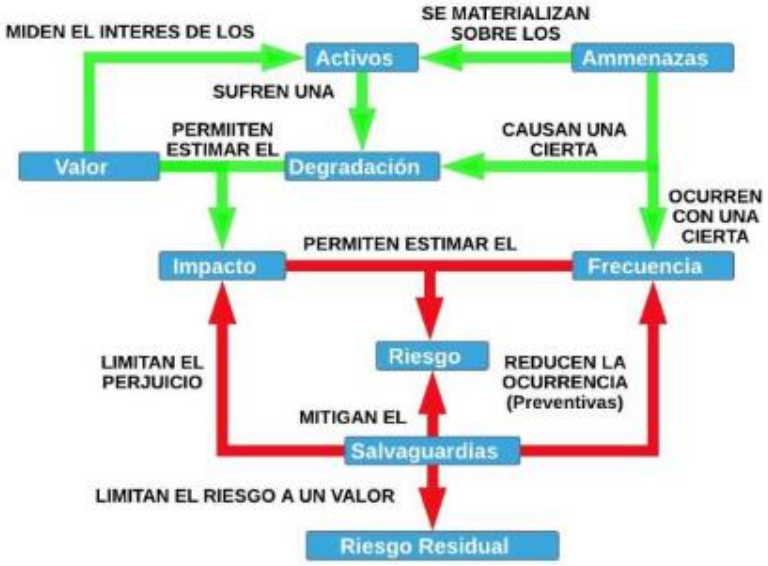
A través de esta investigación se determina la utilización y buenos resultados que brinda la metodología MAGERIT, tanto a nivel de empresas del sector público y privado, como a nivel de instituciones educativas, prueba de ello es el resultado del estudio elaborado en Colombia, con buenos resultados y aprobado por la Universidad de Cartagena.

1.2. Metodología Magerit

Magerit es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, actualmente Comisión de Estrategia TIC, Magerit permite saber cuánto valor está en juego y ayuda a protegerlo. Conocer el riesgo al que están sometidos los elementos de trabajo es simplemente, imprescindible para gestionarlos. Con Magerit se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista (Amutio Gómez, Candau, & Mañas, MAGERIT version 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I Método, 2012).

La razón de ser de MAGERIT está estrechamente relacionada con el uso de las Tecnologías de la Información, lo que supone riesgos, los cuales se reducen al máximo al aplicar medidas de seguridad los cuales garanticen los pilares de la información y proteger el activo más valioso de las empresas o instituciones como es la información, a continuación, se muestra en la Figura 1 el Marco de Trabajo para la Gestión de Riesgos:

Figura 1. Marco de trabajo para la gestión de riesgos Magerit



Fuente: [1]tomado a partir de Amutio, Candau, & Mañas (2012)

Las ventajas de usar la Metodología Magerit son las siguientes:

- En el ámbito de seguridad, es una metodología completa, compatible con la Norma ISO 27005, ISO 31000, ISO 31010 y es adaptable a cualquier tipo de organización.
- El tipo de análisis que brinda esta metodología es de tipo cuantitativo y cualitativo.
- Cuenta con una metodología la cual permite la identificación de recursos informáticos, activos y amenazas.
- Realiza una valoración basada en los tres pilares de la información confidencialidad, integridad, disponibilidad y autenticación lo que permite obtener un análisis integral de riesgos.

La Metodología Magerit está compuesta de tres libros, que brindan una guía para el análisis y gestión de riesgos, los que se detallan a continuación:

- Libro I – Método (Amutio Gómez, Candau, & Mañas, MAGERIT version 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I Método, 2012)

[1] MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método

- Libro II – Catálogo de elementos (Amutio Gómez, Candau, & Mañas, MAGERIT-version 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II - Catálogo de Elementos, 2012)
- Libro III – Guía de técnicas (Amutio Gómez, Candau, & Mañas, MAGERIT-version 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III - Guía de Técnicas, 2012)

Para llevar a cabo el análisis de riesgos se contempla los siguientes elementos:

1. Activos
2. Amenazas
3. Salvaguardas

Con estos elementos se estima:

1. El impacto, que es lo que pasaría en un determinado momento.
2. El riesgo: que es lo que probablemente pase.

Valoración

Cada uno de los activos con los que cuenta una Institución Pública o Privada tiene valor, y el valor de este depende de su importancia dentro de la misma, en este contexto resulta importante señalar que, a mayor importancia del activo, mayor es la necesidad de protegerlo. Magerit establece una valoración cuantitativa y cualitativa para la evaluación y gestión de riesgos, en el presente proyecto de investigación se realizará una valoración cualitativa.

Criterios de valoración

Para realizar una valoración es necesario aplicar una escala y un criterio, de esta forma se obtendrá una comparación del riesgo. En la tabla 2, se muestra los criterios de valoración aplicados y sugeridos por la metodología Magerit.

*T*abla 1. Criterios de valoración de activos

valor		***criterio***
10	extremo	daño extremadamente grave
9	muy alto	daño muy grave
6-8	alto	daño grave
3-5	medio	daño importante
1-2	bajo	daño menor
0	despreciable	irrelevante a efectos prácticos

Fuente: [2]tomado a partir de Amutio, Candau, & Mañas (2012)

Identificación de las amenazas

De acuerdo a la Metodología Magerit, las amenazas típicas son:

- Amenazas de origen natural: como son accidentes naturales, terremotos, inundaciones, entre otros.
- Amenazas del entorno (de origen industrial): como son desastres industriales, fallas eléctricas, contaminación industrial, entre otros.
- Amenazas por defectos de aplicaciones: como son errores no contemplados, fallas de origen técnico con consecuencias negativas sobre el sistema.
- Amenazas causadas por las personas de forma accidental: personal con acceso a los sistemas que causaría problemas no intencionados, por error u omisión o de forma accidental.
- Amenazas causadas por las personas de forma deliberada, como acceso personal a los sistemas que causan problemas mal intencionados: ataques deliberados, causar daños y perjuicios a la institución. Cabe indicar que no todas las amenazas afectan directa o indirectamente a los activos, existe un cierto grado de relación entre el tipo de activo y lo que ocurriría.

[2] MAGERIT version 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I Método

Tabla 2. Probabilidad de ocurrencia

impacto	valor	ocurrencia
MA	100	Muy Frecuente (a diario)
A	10	Frecuente (mensualmente)
M	1	Normal (una vez al año)
B	1/10	Poco frecuente (cada varios años)
MB	1/100	Muy poco frecuente (siglos)

Fuente: [3]tomado a partir de Amutio, Candau, & Mañas (2012)

Riesgo en función del impacto y la probabilidad

El riesgo se incrementa conjuntamente con el impacto y la probabilidad, por lo cual se distinguen una serie de zonas en cuanto al tratamiento del riesgo.

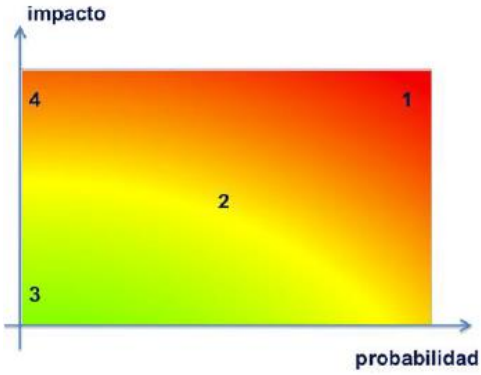
Zona 1 – franja de color rojo: riesgos muy probables y de muy alto impacto.

Zona 2 – franja de color amarillo: comprende un alto rango desde situaciones poco probables e improbables y de impacto medio, hasta situaciones muy probables, pero de impacto bajo o muy bajo.

Zona 3 – franja de color verde: riesgos improbables y de bajo impacto.

Zona 4 – franja de color anaranjado: riesgos improbables, pero de muy alto impacto.

Figura 2. Riesgo en función del impacto y la probabilidad



Fuente: [4]tomado a partir de Amutio, Candau, & Mañas (2012)

[3] MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método

[4] MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método

Estimación del riesgo

Magerit recomienda la siguiente escala en función del impacto, probabilidad y riesgo, para la estimación del riesgo misma que se ejemplificada en la tabla 3:

Tabla 3. Estimación del riesgo

escalas		
impacto	probabilidad	riesgo
MA: muy alto	**MA:** prácticamente seguro	**MA:** crítico
A: alto	**A:** probable	**A:** importante
M: medio	**M:** posible	**M:** apreciable
B: bajo	**B:** poco probable	**B:** bajo
MB: muy bajo	**MB:** muy raro	**MB:** despreciable

Fuente: [5]tomado a partir de Amutio Gómez, Candau, & Mañas (2012)

De esta forma se combina impacto y frecuencia en una tabla para calcular el riesgo.

Tabla 4. Cálculo del riesgo

riesgo		***probabilidad***				
		MB	B	M	A	MA
impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Fuente: [6]tomado a partir de (Amutio Gómez, Candau, & Mañas (2012)

Estimación de salvaguardas

La Metodología Magerit brinda una gran variedad de salvaguardas, para lo cual se plantean las siguientes preguntas:

[5] MAGERIT – version 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III - Guía de Técnicas

[6] MAGERIT – version 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III - Guía de Técnicas

¿Cuáles son los tipos de activos que se van a proteger?
¿Cuáles son los tipos de amenazas a las cuales se está expuesto y existe la necesidad de proteger?
¿Las salvaguardas brindan seguridad?

Estimación del impacto

Para realizar un análisis de riesgos se trabajará con información la cual hay que combinar, ordenar y detallar en base a su importancia. De tal forma la siguiente tabla muestra las escalas para medir el valor según la magnitud del impacto y del riesgo, según la Metodología Magerit.

Tabla 5. Estimación del impacto

impacto		*degradación*		
		1%	10%	100%
valor	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Fuente: [7]tomado a partir de Amutio Gómez, Candau, & Mañas (2012)

Los activos que reciban calificaciones muy altas (MA), se someterán a atención inmediata. Sin embargo, esto no significa que los activos con calificación alta (A) y media (M) no requieran una debida atención, muchas veces este tipo de activos con calificación alta y media representan un alto riesgo a medida que transcurre el tiempo.

Determinación del impacto potencial

La determinación del impacto potencial es el daño causado al activo, esto sucede al materializarse una amenaza, de tal forma las consecuencias son

[7] MAGERIT – version 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III - Guía de Técnicas

indudablemente negativas. Para realizar el cálculo del valor del impacto se aplica la siguiente fórmula:

Impacto = valor del activo x degradación del valor

Fuente: [8]tomado a partir de Amutio Gómez, Candau, & Mañas (2012)

Determinación del riesgo potencial

Para realizar una valoración de riesgos, es necesario identificar cada uno de los activos, para posteriormente identificar las amenazas sobre el activo y finalmente estimar la vulnerabilidad, de que la amenaza probablemente se materialice. Para determinar el riesgo se utiliza la siguiente fórmula:

Riesgo = probabilidad de amenaza x magnitud del daño

Fuente: [9]tomado a partir de Amutio Gómez, Candau, & Mañas (2012)

Tabla 6. Valores representativos para estimar el riesgo

valores representativos	probabilidad de la amenaza	magnitud del daño
5 - Catastrófico	100	10
4 - Crítico	10	8 - 9
3 - Alto	1	6 - 7
2 - Medio	1/10	4 - 5
1 - Bajo	1/100	0 - 3

Fuente: [10]tomado a partir de Amutio Gómez, Candau, & Mañas (2012)

Para realizar un cálculo del riesgo se hace imprescindible realizar una matriz donde se diferencia las zonas de alto riesgo de acuerdo al color, conforme lo indica la Metodología Magerit.

[8] MAGERIT – version 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III - Guía de Técnicas
[9] MAGERIT – version 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III - Guía de Técnicas
[10] MAGERIT – version 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III - Guía de Técnicas

Tabla 7. Matriz de riesgos con colores de acuerdo al impacto

PROBABILIDAD		IMPACTO				
		1	2	3	4	5
Muy Frecuente (a diario)	5	Alto	Alto	Crítico	Crítico	Crítico
Frecuente (mensualmente)	4	Medio	Alto	Alto	Crítico	Crítico
Normal (una vez al año)	3	Bajo	Medio	Alto	Crítico	Crítico
Poco frecuente (cada varios años)	2	Bajo	Bajo	Medio	Alto	Crítico
Muy poco frecuente (siglos)	1	Bajo	Bajo	Medio	Alto	Alto

Fuente: [11]tomado a partir de Amutio Gómez, Candau, & Mañas (2012)

Impacto residual

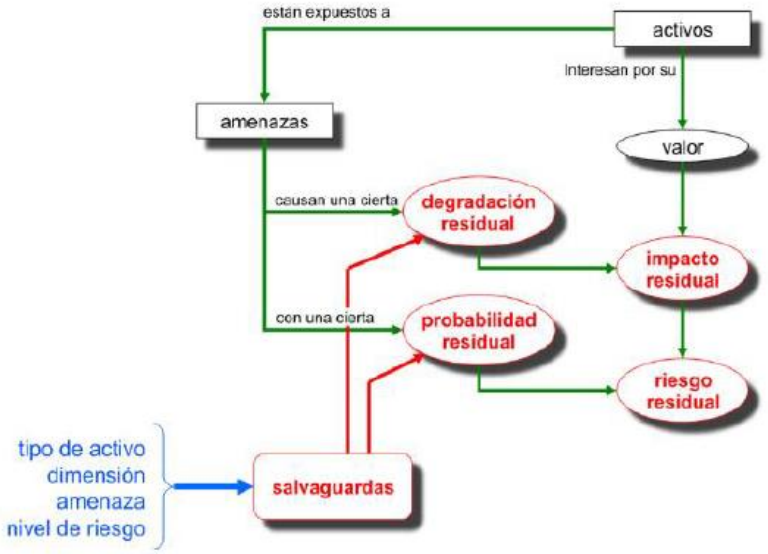
Es el daño ocasionado al activo consecuencia de la materialización de una amenaza, pese a la existencia de salvaguardas (Amutio Gómez, Candau, & Mañas, MAGERIT version 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I Método, 2012) para el cálculo del impacto residual se repite los cálculos del impacto y se suma un nuevo nivel de degradación.

Riesgo residual

Es el riesgo que persiste después de los controles de las salvaguardas (Amutio Gómez, Candau, & Mañas, MAGERIT version 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I Método, 2012). Para el cálculo del riesgo residual se repite los cálculos del riesgo y se utiliza el impacto residual y la probabilidad residual de ocurrencia.

[11] MAGERIT – version 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III - Guía de Técnicas

Figura 3. Elementos de análisis del riesgo residual



Fuente: [12]tomado a partir de Amutio, Candau & Mañas (2012)

Herramienta PILAR

La Herramienta PILAR (Procedimiento Informático y Lógico de Análisis de Riesgos), desarrollada por el Centro Nacional de Inteligencia – Centro Criptológico Nacional, con la colaboración del MAP, tiene librerías que permiten aplicar MAGERIT versión 3 y realizar el análisis y la gestión de los riesgos en el marco de los criterios que establece la metodología (Aldaz Calispa & Pazmiño Sanchez, 2021). Entre los aspectos interesantes de PILAR:

- Facilidad de uso: realización asistida del análisis y la gestión de los riesgos, de manera intuitiva y rápida.
- Flexibilidad: Utilizable a diferentes niveles de profundidad y de conocimiento de los usuarios.
- Adaptación del entorno: Posibilidad de generación y adaptación de bibliotecas (AAP, OTAN).

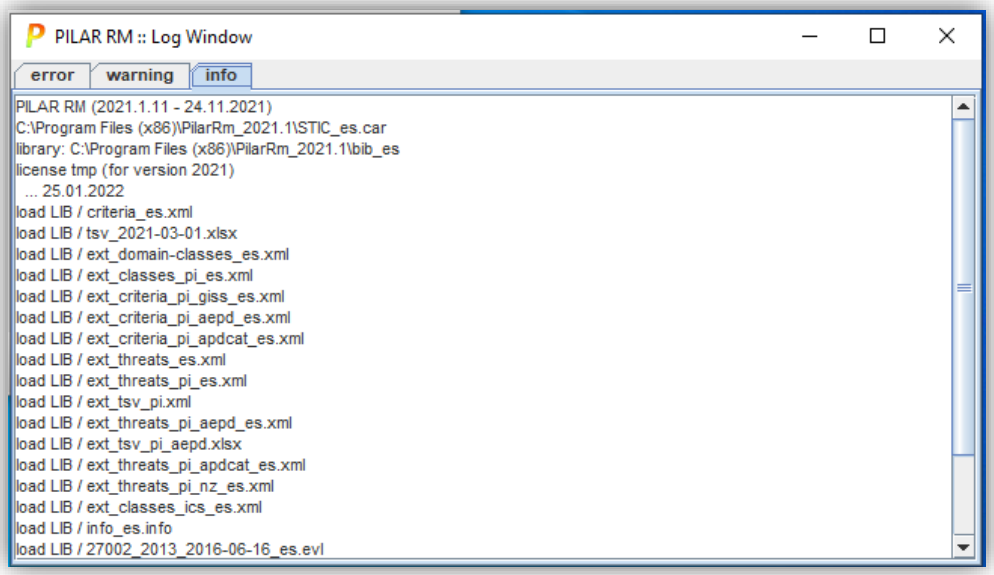
PILAR es una herramienta creada específicamente bajo lineamientos de la metodología MAGERIT, en la cual se describen los siguientes procesos:

- Identificación del activo.
- Establecer dependencias entre los activos.
- Valoración de los activos.

[12] MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método

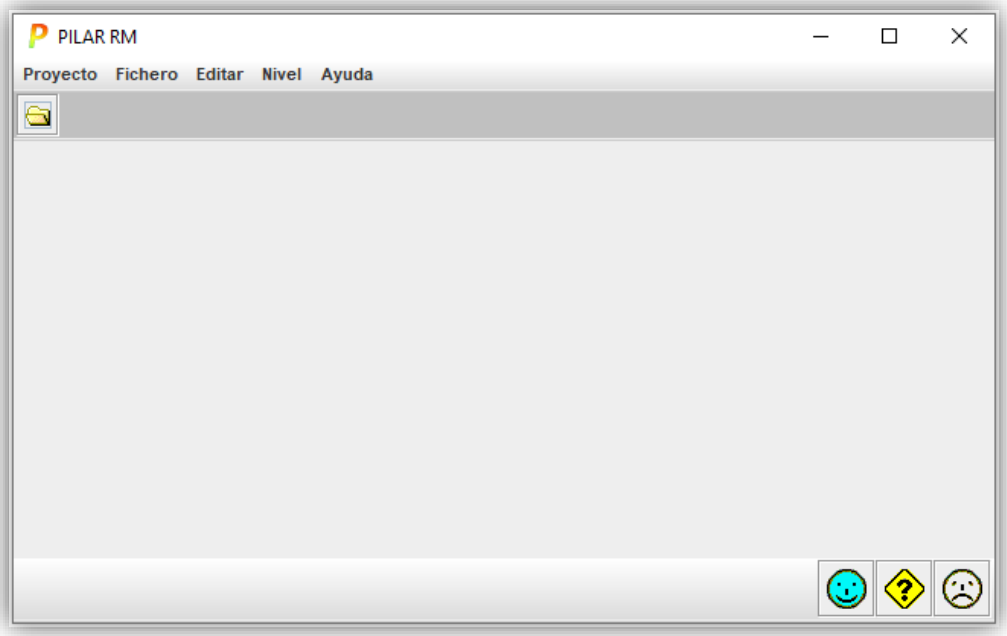
- Identificación de las amenazas, asigna automáticamente amenazas de la biblioteca del programa según las características de cada activo.
- Valoración de amenazas por cada activo, el programa calcula las probabilidades de que una o varias amenazas se materialicen.
- Impacto y riesgo, el programa genera automáticamente estos parámetros.
- Impacto y riesgo residual, el programa lo genera automáticamente.

Figura 4. Pantalla principal de carga PILAR SOFTWARE



Fuente: PILAR – MAGERIT (2021)

Figura 5. Pantalla principal PILAR SOFTWARE



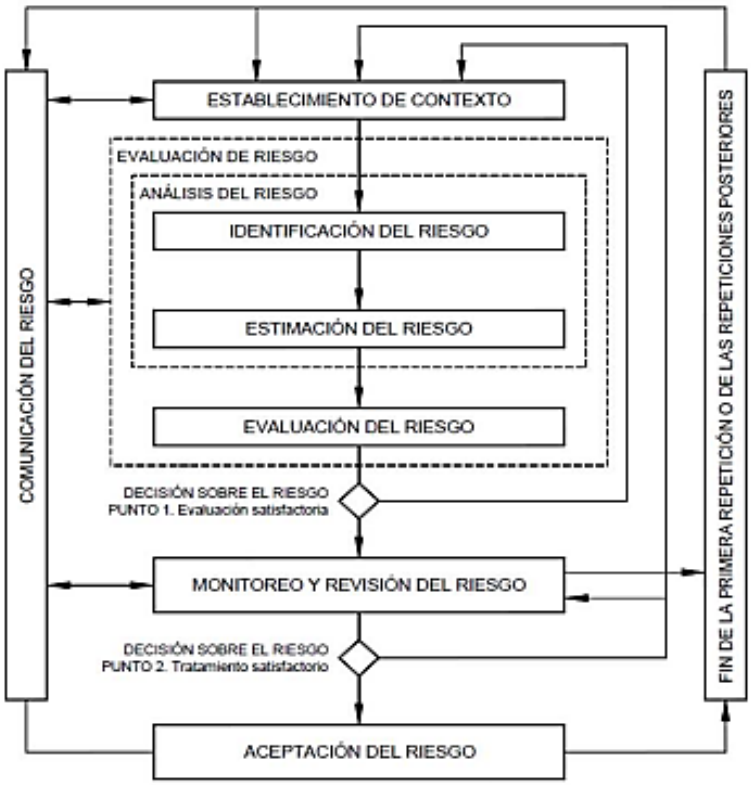
Fuente: PILAR – MAGERIT (2021)

1.3. ISO / IEC 27005:2018

ISO / IEC 27005: 2018, Tecnologías de la información - Técnicas de seguridad - Gestión de riesgos de seguridad de la información, proporciona directrices para la gestión de riesgos de seguridad de la información y respalda los conceptos generales especificados en ISO / IEC 27001: 2005, Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información – Requerimientos (PMG-SSI, 2022).

Es aplicable a organizaciones públicas y privadas, permite gestionar los riesgos asociados a la seguridad de la información e identifica los riesgos de mayor criticidad, la probabilidad de impacto y ocurrencia, de igual forma permite categorizarlos para establecer las medidas adecuadas de control y seguimiento. En la figura 2 se muestra la gestión del riesgo de seguridad de la información propuesta por ISO 27005:

Figura 6. Proceso de gestión del riesgo en la seguridad de la Información



Fuente: tomado a partir de Kowask, Alcántara, Cesar & Boca (2014)

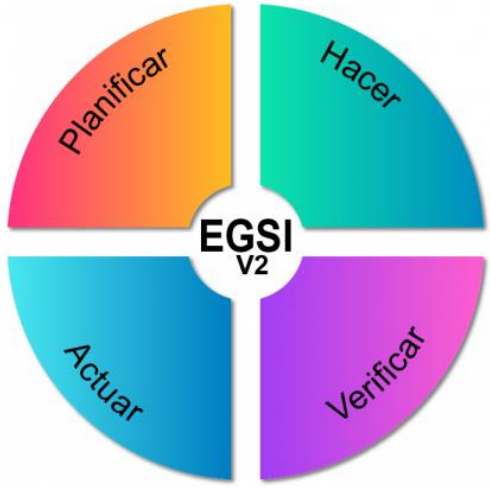
El proceso de gestión de riesgos de seguridad de la información es iterativo, es decir, que se repetirse una o varias veces, para las actividades de evaluación y/o tratamiento de riesgos. Un enfoque iterativo para realizar la evaluación de riesgos aumenta la profundidad y el detalle de la evaluación en cada iteración. El enfoque iterativo proporciona un buen equilibrio entre minimizar el tiempo y el esfuerzo dedicados a la identificación de controles y, al mismo tiempo, garantizar que los riesgos elevados se evalúen adecuadamente (Dirección Nacional de Interoperabilidad Seguridad de la Información e Infraestructura, 2020, pág. 4) .

1.4. Esquema Gubernamental de Seguridad de la Información (EGSI) V 2.0

Es un documento basado en las normas técnicas ecuatorianas “INEN ISO/IEC 27000”, para la Gestión de la Seguridad de la Información y está dirigido a las Instituciones de la Administración Pública Central e Institucional y que depende de la Función Ejecutiva (Ministerio de Telecomunicaciones y de la Sociedad de

la Información, 2020). En la figura 3 se muestra el ciclo de mejora continua propuesto por el EGSI:

Figura 7. Ciclo de mejora continua (PDCA) aplicado al EGSI



Fuente: tomado a partir de Ministerio de Telecomunicaciones y de la Sociedad de la Información (2020)

En este contexto, lo primero en lo cual se enfoca es en la planificación, la cual se evalúa en primera instancia a partir de un análisis de la situación actual de la institución desde la seguridad de la información. La etapa de ejecución (Hacer) prepara un plan, implementa controles y establece lineamientos con carácter formativo y de concienciación enfocado en la seguridad de la información. Posteriormente en la etapa de verificación se realiza una evaluación de la eficacia de los indicadores, controles y lineamientos implementados.

Finalmente, los resultados obtenidos se enmarcarán en un proceso de gestión de seguridad de la información, y alineado a los objetivos institucionales, al cumplir con los principios de confidencialidad, integridad y disponibilidad de la información. Los pasos de un proceso para la gestión del riesgo de seguridad de la información son los siguientes:

- Establecimiento del contexto, lo cual consiste en levantar la información inicial, establecer criterios básicos para gestionar el riesgo, definir alcance y límites y establecer una organización para el SGRSI.

- Valoración del riesgo, consiste en identificar los activos, las amenazas y vulnerabilidades, además de los controles existentes, las consecuencias, valorar los incidentes, determinar el nivel de estimación del riesgo y evaluar el riesgo.
- Tratamiento del riesgo, en esta etapa se seleccionan los controles.
- Aceptación del riesgo, evaluar el aceptar o no un riesgo.
- Comunicación del riesgo, después de la evaluación de un riesgo resulta necesario socializar y comunicar dicho riesgo en función de su aceptación.
- Monitoreo y revisión del riesgo, monitoreo y revisión permanente de los riesgos aceptados.

En la Tabla 9 se muestran las actividades del proceso para la gestión de riesgos dividido en actividades y pasos, que llevados de manera conjunta y ordenada dan como resultado una adecuada gestión de riesgos y asegura los objetivos y metas trazadas por la unidad encargada del proceso en beneficio para toda la institución:

Tabla 8. Proceso para la gestión del riesgo

ACTIVIDADES	PASO
Establecimiento del contexto	*1. Consideraciones Generales - Levantamiento de información inicial* *2. Establecer criterios básicos para la Gestión del Riesgo* *3. Definir alcance y límites de la Gestión del Riesgo* *4. Establecer una organización para la operación del SGRSI*
Valoración del Riesgo	*5. Identificar Activos de Información* *6. Identificar las amenazas y las vulnerabilidades* *7. Identificar los controles existentes* *8. Identificar consecuencias* *9. Valorar las consecuencias* *10. Valorar los incidentes* *11. Determinar el nivel de estimación del riesgo* *12. Evaluar el riesgo*
Tratamiento del Riesgo	*13. Seleccionar controles*
Aceptación del Riesgo	*14. Aceptar el riesgo*
Comunicación del Riesgo	*15. Comunicar el riesgo*
Monitoreo y Revisión del Riesgo	*16. Monitorear y revisar los riesgos*

Fuente: tomado a partir de Ministerio de Telecomunicaciones y de la Sociedad de la Información (2020)

Análisis del riesgo y el sistema de gestión de seguridad de la información

Como lo cita (Gallardo, 2018, pág. 28), en su documento “el enfoque ISO 27001:2005” hace referencia a la implementación de una norma basada en seguridad de la información, misma que necesita determinar los requerimientos básicos y trabajo en conjunto con las autoridades y técnicos relacionados a la seguridad de la información. El propósito fundamental es el de asegurar la información mediante confidencialidad, integridad y disponibilidad en función del análisis realizado por el equipo de trabajo, para establecerlo como guía base en la implementación de los controles, que se ajustan a las necesidades del negocio. En tal virtud, apalanca la elaboración de una política y fundamenta el desarrollo del presente estudio que involucra autoridades, personal técnico y demás funcionarios para cumplir con el objetivo propuesto (Ávila, 2018).

De igual forma como lo afirma (Ávila, 2018) “las normas ISO 27001, plantean una visión de la situación actual de varios estándares y debido a su demanda en función de la seguridad de la información, convergen en un sistema de gestión integrado, mismo que optimiza y cumple con los requisitos específicos de gestión de servicios de TI y de seguridad de la información”. De esta manera, se alinea la aplicación del Esquema Gubernamental de Seguridad de la Información que abarca las mejores prácticas de la norma ISO 27001 e ISO 27002, así como el alineamiento para blindar en primera instancia los aplicativos denominados como críticos.

Terminología

- **Activo de información**

Es cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización, como son procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización (Instituto Nacional de Ciberseguridad, 2017).

- **Amenaza**

Circunstancia desfavorable que ocurriría y que de suceder tiene consecuencias negativas sobre los activos lo que provoca su indisponibilidad, funcionamiento incorrecto o pérdida de valor (Instituto Nacional de Ciberseguridad, 2017).

- **Análisis de Riesgo**

Es un proceso que comprende la identificación de activos de información, sus vulnerabilidades y las amenazas a los que se encuentran expuestos, así como la probabilidad de ocurrencia y el impacto, a fin de determinar los controles adecuados para tratar el riesgo (Instituto Nacional de Ciberseguridad, 2017).

- **Auditoría de seguridad**

Es el estudio que comprende el análisis y gestión de sistemas llevado a cabo por profesionales en tecnologías de la información (TI) con el objetivo de identificar, enumerar y describir las diversas vulnerabilidades que presentarían en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones, servidores o aplicaciones (Instituto Nacional de Ciberseguridad, 2017).

- **Autenticación**

Procedimiento para comprobar que alguien es quien dice ser al acceder a un ordenador o a un servicio online. Este proceso constituye una funcionalidad característica para una comunicación segura (Instituto Nacional de Ciberseguridad, 2017).

- **Confidencialidad**

Es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información. La confidencialidad de la información constituye la piedra angular de la seguridad de la información (Instituto Nacional de Ciberseguridad, 2017).

- **Disponibilidad**

Se trata de la capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por los usuarios o procesos autorizados si estos lo requieran (Instituto Nacional de Ciberseguridad, 2017).

- **Fuga de datos**

La fuga de datos o fuga de información es la pérdida de la confidencialidad de la información privada de una persona o empresa. Información que, a priori, no sería conocida más que por un grupo de personas, en el ámbito de una organización, área de una organización, área o actividad, y que es visible o accesible para otros (Instituto Nacional de Ciberseguridad, 2017).

- **Impacto**

Medida del efecto que produce un incidente, desastre, problema o cambio en los niveles de servicio de una empresa y cómo se ven afectados en el caso de que se materialice dicha amenaza (Instituto Nacional de Ciberseguridad, 2017).

- **Integridad**

Es la propiedad de la información, por la que se garantiza la exactitud de los datos transportados o almacenados, asegura que, no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de software o hardware o por condiciones medioambientales (Instituto Nacional de Ciberseguridad, 2017).

- **Incidente de seguridad**

Cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa, por ejemplo: acceso o intento de acceso a los sistemas, uso, divulgación, modificación o destrucción no autorizada de la información (Instituto Nacional de Ciberseguridad, 2017).

- **No repudio**

El no repudio en el envío de información a través de redes es la capacidad de demostrar la identidad del emisor de esa información. El objetivo que se

pretende es certificar que los datos, o la información, provienen realmente de la fuente que dice ser (Instituto Nacional de Ciberseguridad, 2017).

- **Plan de contingencia**

Un Plan de Contingencia de las Tecnologías de la Información y las Comunicaciones (TIC) consiste en una estrategia planificada en fases, constituida por un conjunto de recursos de respaldo, una organización de emergencia y unos procedimientos de actuación, encaminados a conseguir una restauración ordenada, progresiva y ágil de los sistemas de información que soportan la información y los procesos de negocio considerados críticos en el Plan de Continuidad de Negocio de la compañía (Instituto Nacional de Ciberseguridad, 2017).

- **Política de seguridad**

Son las decisiones o medidas de seguridad que una empresa ha decidido tomar respecto a la seguridad de sus sistemas de información después de evaluar el valor de sus activos y los riesgos a los que están expuestos. Este término también se refiere al documento de nivel ejecutivo mediante el cual una empresa establece sus directrices de seguridad de la información (Instituto Nacional de Ciberseguridad, 2017).

- **Riesgo**

Es la posibilidad de que una amenaza o vulnerabilidad se convierta en un daño real para la empresa, que resulte en una pérdida o robo de información o en una detención de su actividad como consecuencia del daño ocasionado. El riesgo se mitiga mediante políticas de seguridad y continuidad del negocio que suelen prever posibles ataques y proponen soluciones de actuación ante situaciones cuyo riesgo sería elevado (Instituto Nacional de Ciberseguridad, 2017).

- **Vulnerabilidad**

Debilidad o fallo de un sistema que se aprovecha con fines maliciosos (Instituto Nacional de Ciberseguridad, 2017).

CAPÍTULO II. DISEÑO METODOLÓGICO

2.1. Metodología de investigación

El enfoque de investigación del presente trabajo es cualitativo, el diseño de la investigación es no experimental, misma que parte en un entorno en donde los hechos ya se han suscitado.

Al aplicar una investigación de tipo cualitativo se priorizarán los riesgos identificados con el fin de recomendar las acciones pertinentes a ejecutar, con base a los datos arrojados por la metodología Magerit, conjuntamente con el Esquema Gubernamental de Seguridad de la Información.

La metodología cualitativa es el más utilizado para el análisis de riesgo según lo afirma (Molina & Sánchez, 2019).

Método de investigación

Método Inductivo

Mediante este método se observa, estudia y conoce las características genéricas o comunes que se reflejan en un conjunto de realidades para elaborar una propuesta o ley científica de índole general (Abreu, 2014).

Es este el caso para la aplicabilidad en el desarrollo de la guía de gestión de seguridad de la información para el Gobierno Provincial de Tungurahua.

Tipo de investigación

No experimental

El tipo de investigación aplicada en el presente trabajo de investigación es no experimental, inicia en un entorno en donde los hechos ya se han suscitado, sin intervenir en los acontecimientos.

Técnicas e instrumentos

Entrevista

La entrevista es una técnica importante en el presente trabajo de investigación, tiene el propósito de obtener información a profundidad de inicio a fin, a través de encuentros reiterados con el personal técnico de la Dirección de Sistemas del Gobierno Provincial de Tungurahua.

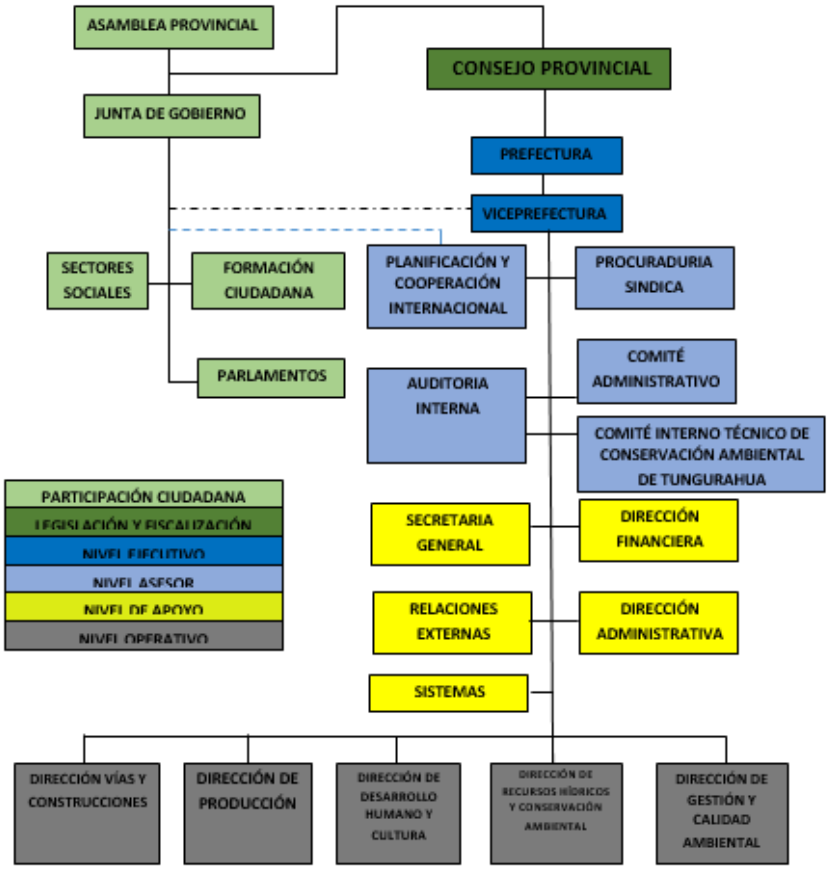
2.2 Caracterización de la institución

El Gobierno Provincial de Tungurahua es una institución pública que pertenece a los gobiernos autónomos descentralizados (GAD) del país, entre sus atribuciones son coordinar, orientar, facilitar, planificar y ejecutar acciones mancomunadas con gobiernos locales, instituciones públicas, privadas y organizaciones sociales, en los niveles; parroquiales, cantonales, provincial, nacional e internacional; con el fin de impulsar las iniciativas de desarrollo económico, social, ambiental y territorial de Tungurahua, bajo los principios de participación, mancomunidad, equidad, ética, efectividad y transparencia (Gobierno Provincial de Tungurahua, 2022).

Visión Institucional

El Gobierno Provincial de Tungurahua se constituye en líder de desarrollo integral de la provincia, en su condición de referente político – técnico, con capacidades para orientar las grandes decisiones de interés provincial (Gobierno Provincial de Tungurahua, 2022).

Figura 8. Estructura Orgánica Funcional del Gobierno Provincial de Tungurahua



Fuente: tomado a partir de Gobierno Provincial de Tungurahua (2022)

En el nivel de apoyo se encuentra la Dirección de Sistemas, la cual tiene como objetivo proveer servicios tecnológicos de calidad a todo el Gobierno Provincial de Tungurahua, a través de herramientas e infraestructura actualizada, para apoyar a los procesos y actividades institucionales.

Dentro de sus atribuciones y responsabilidades están:

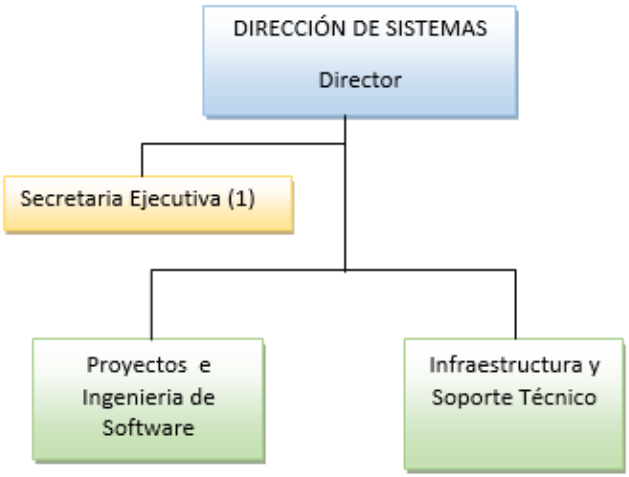
- Realizar el diseño, pruebas, implantación, monitoreo y mantenimiento de aplicaciones según las necesidades del usuario interno.
- Realizar el mantenimiento de los equipos del sistema informático: Software y Hardware.
- Lograr un mejor desempeño mediante la conectividad de todos los equipos informáticos del Gobierno Provincial.
- Vigilar el desempeño, las seguridades y controles de los sistemas informáticos que obtienen recursos de la base de datos principal.

- Capacitar al personal del Gobierno Provincial en el uso y manejo de equipos y sistemas informáticos implementados.
- Mantener un registro y control de los recursos informáticos, así como su respectiva provisión y optimización.
- Dar soporte de hardware y software a los usuarios internos del sistema.
- Evaluar y controlar el buen uso de los recursos informáticos y equipos de comunicación. (Gobierno Provincial de Tungurahua, 2022)

Población y Muestra

El presente trabajo de investigación se centra específicamente en la Dirección de Sistemas del Gobierno Provincial de Tungurahua, la cual cuenta con 10 profesionales, los cuales están divididos de la siguiente forma:

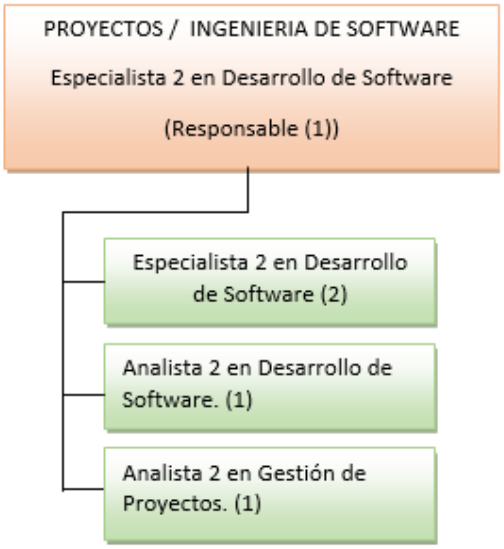
Figura 9. Estructura Dirección de Sistemas del Gobierno Provincial de Tungurahua



Fuente: tomado a partir de Gobierno Provincial de Tungurahua (2022)

Proyectos e Ingeniería de Software

Figura 10. Estructura Proyectos e Ingeniería de Software
Dirección de Sistemas del Gobierno Provincial de Tungurahua

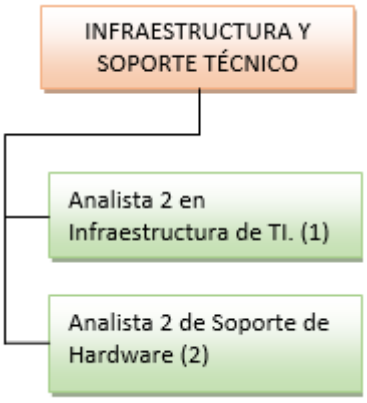


Fuente: tomado a partir de Gobierno Provincial de Tungurahua (2022)

El cual tiene como objetivo definir mecanismos que faciliten la administración de todos los proyectos informáticos que ejecutan las diferentes áreas que conforman la unidad.

Infraestructura y soporte técnico

Figura 11. Estructura Infraestructura y Soporte Técnico
Dirección de Sistemas del Gobierno Provincial de Tungurahua



Fuente: tomado a partir de Gobierno Provincial de Tungurahua (2022)

Se encarga de definir, justificar, implementar y actualizar la infraestructura tecnológica de la institución, establecer mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos (Gobierno Provincial de Tungurahua, 2022).

2.3 Metodología de desarrollo

La metodología de desarrollo empleada en el presente trabajo de investigación es Magerit, la cual brinda los lineamientos para realizar análisis de gestión de riesgos de los Sistemas de Información.

De igual forma se aplica las directrices del Esquema Gubernamental de Seguridad de la Información (EGSI) versión 2.0 emitido mediante acuerdo Ministerial Nro. 025 - 2019 por el Ministerio de Telecomunicaciones y de la Sociedad de la Información y publicado en el Registro Oficial el 10 de enero de 2020.

Figura 12. Método de Análisis de Riesgo de Magerit

Fuente: [13]tomado a partir de Amutio, Candau & Mañas, (2012)

Determinar los activos

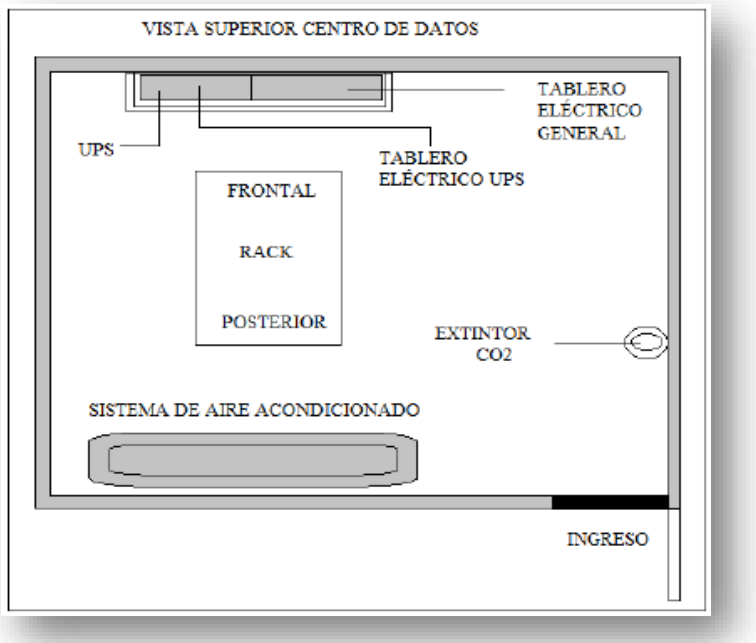
En el Gobierno Provincial de Tungurahua, específicamente en la Dirección de Sistemas se encuentra ubicado e implementado un Data Center, el mismo que

[13] MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método

cuenta con un acondicionamiento especial por temas de temperatura y ambiente.

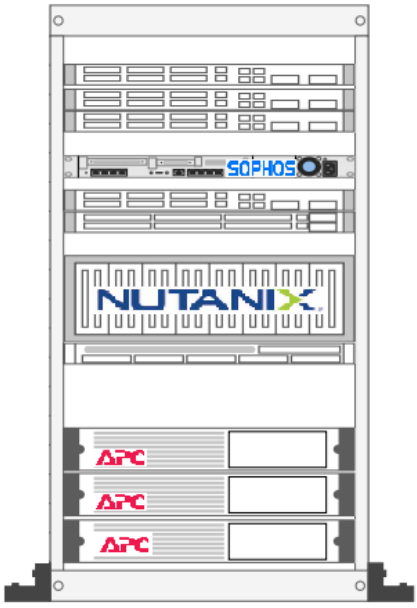
En la figura 9 se muestra un diagrama de la Infraestructura del Data Center.

Figura 13. Infraestructura Data Center



Fuente: elaboración propia

Figura 14. Vista frontal del rack



Fuente: elaboración propia

El Centro de Datos está conformado de los siguientes componentes: sistema eléctrico, sistema de aire acondicionado, estructura que sostiene los equipos físicos (rack), sistema de telecomunicaciones.

El sistema de telecomunicaciones está compuesto por los principales equipos de telecomunicaciones como son: switchs, firewall marca Sophos y servidor físico marca Nutanix.

El servidor físico con el que cuenta el Gobierno Provincial de Tungurahua es un servidor Nutanix, el cual está implementado en una plataforma de hiperconvergencia, configurado para brindar soluciones de almacenamiento para grandes cargas de trabajo y administrar toda la red institucional.

La infraestructura de hiperconvergencia se tomó en consideración para reducir gastos operativos, recursos de espacio y administración de almacenamiento simplificado.

Los activos considerados para el análisis y gestión de riesgos han sido seleccionados en base al grado de relevancia que tienen para el Gobierno Provincial de Tungurahua.

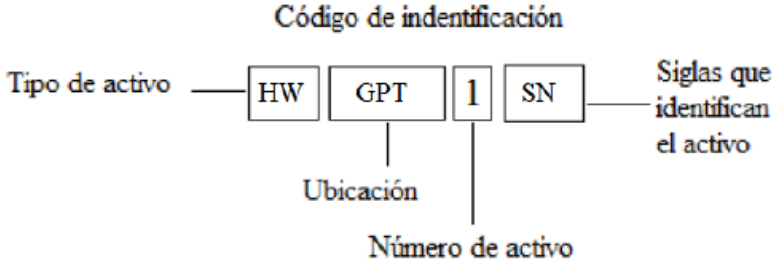
Conforme lo señala la Metodología Magerit, a cada activo se asigna un código el cual lo identifique, el código de asignación está estructurado de la siguiente forma:

Tipo de activo: las dos primeras letras describen el tipo de activo al cual pertenece:

- [HW] HARDWARE
- [SW] SOFTWARE
- [D] DATOS
- [I] INSTALACIONES
- [P] PERSONAL

Ubicación: iniciales de la Institución GPT Gobierno Provincial de Tungurahua.
Número de archivo: numeración de cada uno de los activos.
Siglas de identificación del activo: nombre del activo para su identificación en este caso SN que corresponde a Servidor Nutanix, FS que corresponde a Firewall Sophos.

Figura 15. Código Identificador de activos



Fuente: elaboración propia

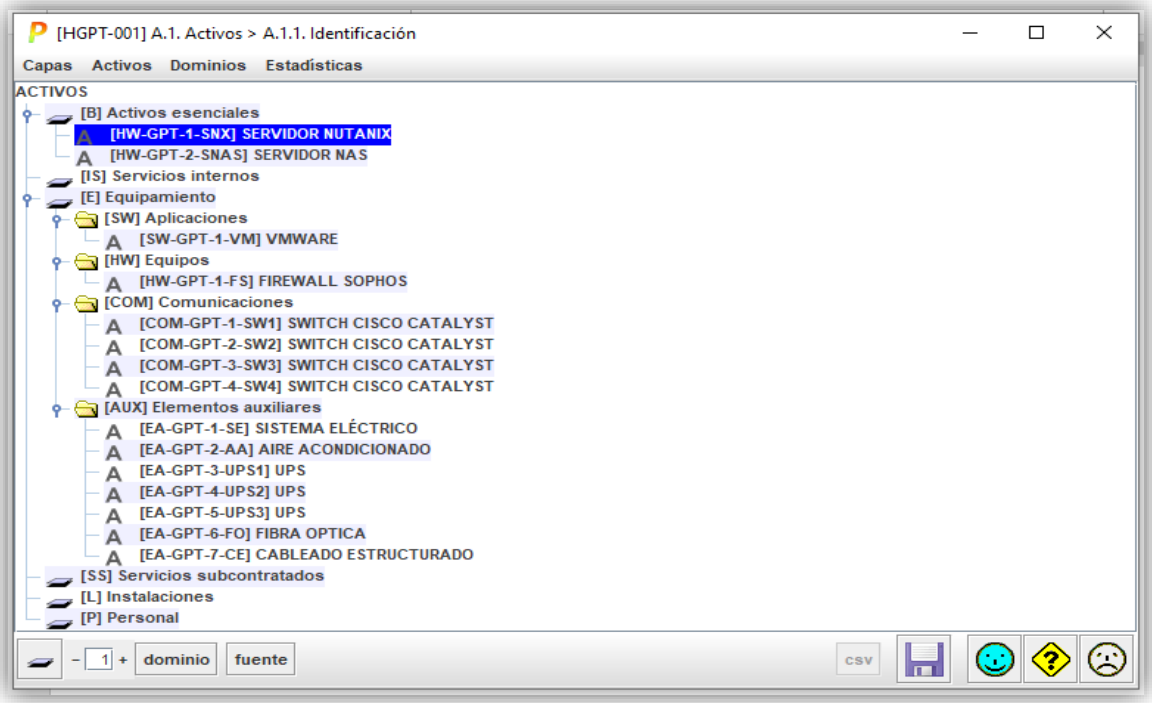
Con la nomenclatura, que se asigna a cada activo, se obtiene un código, dicho código consta de 4 elementos como son: tipo, ubicación, número y siglas, de esta forma se identifica y se divide el tipo de activo en función a la información y grado de vulnerabilidad a las que estaría expuesto, durante todo el proceso de levantamiento de información y análisis de riesgos.

Tabla 9. Proceso para la gestión del proceso de gestión del riesgo

LISTADO DE ACTIVOS DEL DATA CENTER DEL GOBIERNO PROVINCIAL DE TUNGURAHUA		
Esenciales		
Código	**Nombre**	**Detalle**
HW-GPT-1-SNX	SNX	Servidor NUTANIX
HW-GPT-2-SNAS	SNAS	Servidor NAS (Network Attached Storage) Synology
Equipos de red		
HW-GPT-1-FS	FS	Firewall SOPHOS
COM-GPT-1-SW1	SW1	Switch Cisco Catalyst Capa 3
COM-GPT-2-SW2	SW2	Switch Cisco Catalyst Capa 3
COM-GPT-3-SW3	SW3	Switch Cisco Catalyst Capa 3
COM-GPT-4-SW4	SW4	Switch Cisco Catalyst Capa 3
Aplicaciones Informáticas (Software)		
SW-GPT-1-VM	VM	VMWare
Elementos auxiliares		
EA-GPT-1-SE	SE	Sistema Eléctrico
EA-GPT-2-AA	AA	Aire Acondicionado
EA-GPT-3-UPS1	UPS1	UPS APC
EA-GPT-4-UPS2	UPS2	UPS APC
EA-GPT-5-UPS3	UPS3	UPS APC
EA-GPT-6-FO	FO	Fibra Óptica
EA-GPT-7-CE	CE	Cableado Estructurado

Fuente: elaboración propia

Figura 16. Identificación de activos



Fuente: PILAR – MAGERIT (2022)

Dependencia de activos

En base a un análisis de los activos que contienen información sensible, y las entrevistas con el personal de la Dirección de Sistemas del Gobierno Provincial de Tungurahua, se evidenció que existe una dependencia absoluta de los servidores físicos NUTANIX y NAS (almacenamiento conectado a una red), los que administran todos los servicios internos y externos que brinda la Institución.

Valoración de activos

Para establecer una valoración de los activos, se parte de la importancia del activo para la Institución, la metodología Magerit recomienda una escala de 0 (cero) a 10 (diez), donde 0 (cero) significa que la pérdida o daño del activo no afecta ni repercute a la Institución, por el contrario, si la valoración es de 10 (diez) significa una grave afectación y consecuencias negativas para la Institución.

Cabe señalar que la valoración de los activos se realiza en base a la: disponibilidad, integridad de datos, confidencialidad de datos, autenticidad, trazabilidad, valor y datos personales.

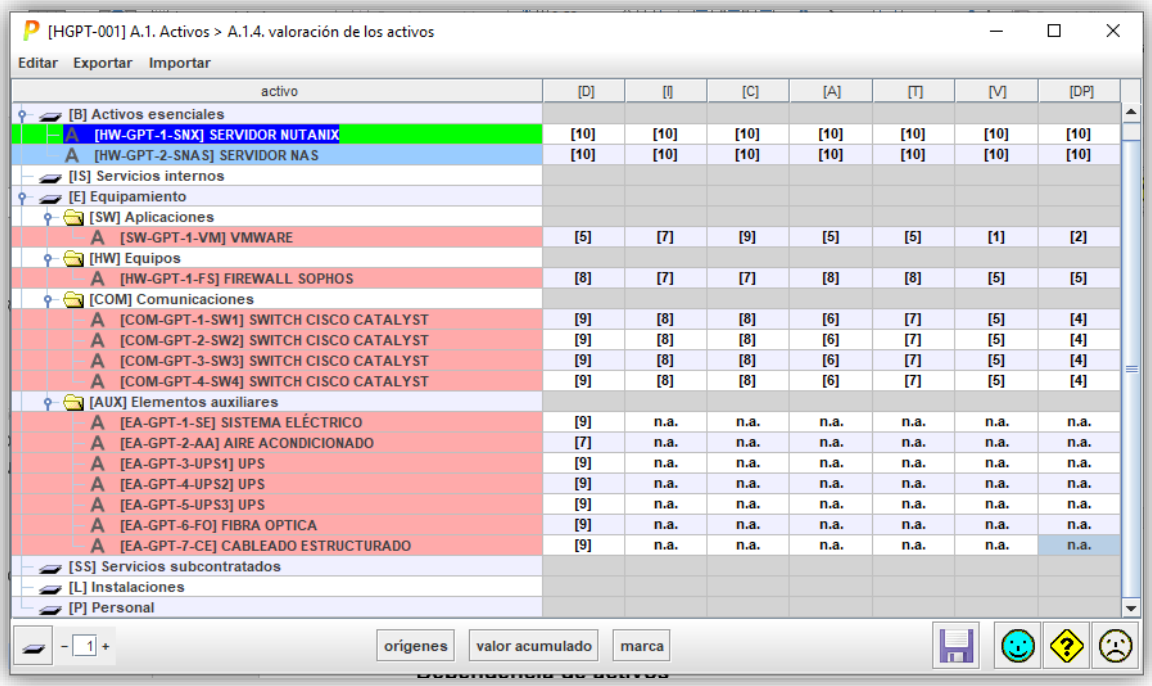
Para la asignación de valores se toma en consideración las siguientes preguntas:

¿Cuál es la importancia del activo y su disponibilidad?
¿Cuáles son las consecuencias de la modificación no autorizada de datos?
¿Cuáles son las consecuencias del acceso a datos sensibles de la Institución y de personas no autorizadas?
¿Cuál es la importancia de la información que es accesible para el personal administrativo de la Institución?

Todas las respuestas a estas preguntas se evaluarán y contestarán en un rango de 0 a 10.

El análisis y respuestas a estas preguntas se las realizó conjuntamente con el área técnica de la Dirección de Sistemas del Gobierno Provincial de Tungurahua. En la imagen a continuación se muestra los resultados:

Figura 17. Valoración de activos



activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[B] Activos esenciales							
[HW-GPT-1-SNX] SERVIDOR NUTANIX	[10]	[10]	[10]	[10]	[10]	[10]	[10]
[HW-GPT-2-SNAS] SERVIDOR NAS	[10]	[10]	[10]	[10]	[10]	[10]	[10]
[IS] Servicios internos							
[E] Equipamiento							
[SW] Aplicaciones							
[SW-GPT-1-VM] VMWARE	[5]	[7]	[9]	[5]	[5]	[1]	[2]
[HW] Equipos							
[HW-GPT-1-FS] FIREWALL SOPHOS	[8]	[7]	[7]	[8]	[8]	[5]	[5]
[COM] Comunicaciones							
[COM-GPT-1-SW1] SWITCH CISCO CATALYST	[9]	[8]	[8]	[6]	[7]	[5]	[4]
[COM-GPT-2-SW2] SWITCH CISCO CATALYST	[9]	[8]	[8]	[6]	[7]	[5]	[4]
[COM-GPT-3-SW3] SWITCH CISCO CATALYST	[9]	[8]	[8]	[6]	[7]	[5]	[4]
[COM-GPT-4-SW4] SWITCH CISCO CATALYST	[9]	[8]	[8]	[6]	[7]	[5]	[4]
[AUX] Elementos auxiliares							
[EA-GPT-1-SE] SISTEMA ELÉCTRICO	[9]	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.
[EA-GPT-2-AA] AIRE ACONDICIONADO	[7]	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.
[EA-GPT-3-UPS1] UPS	[9]	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.
[EA-GPT-4-UPS2] UPS	[9]	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.
[EA-GPT-5-UPS3] UPS	[9]	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.
[EA-GPT-6-FO] FIBRA OPTICA	[9]	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.
[EA-GPT-7-CE] CABLEADO ESTRUCTURADO	[9]	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.
[SS] Servicios subcontratados							
[L] Instalaciones							
[P] Personal							

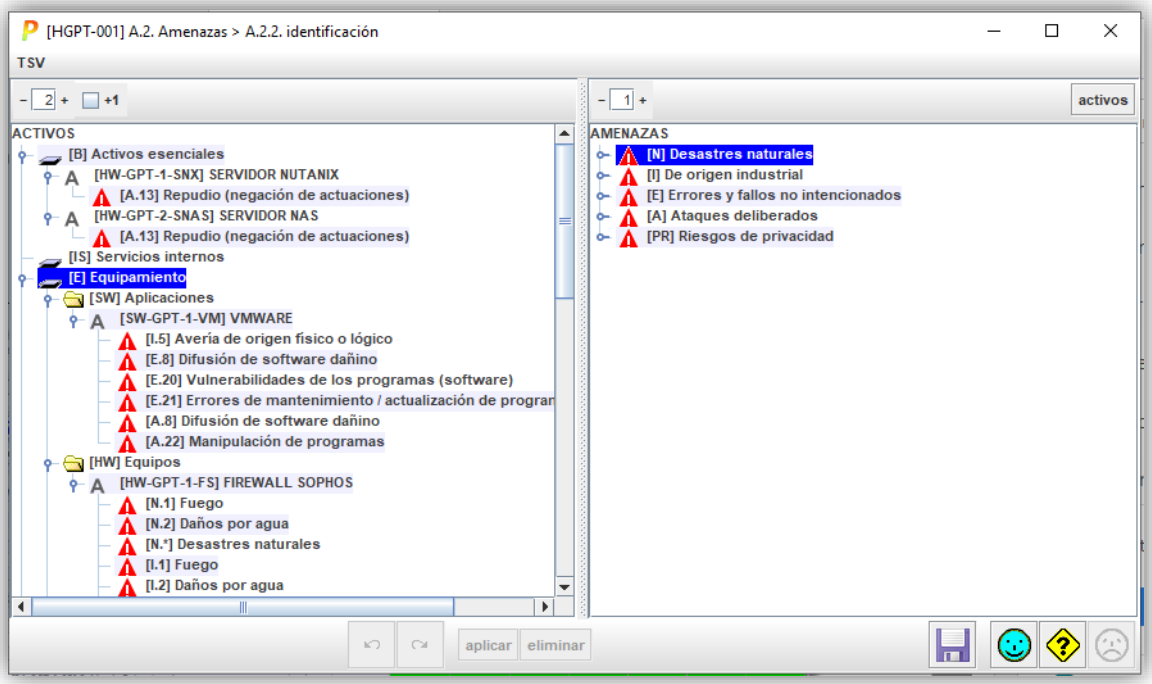
Fuente: PILAR – MAGERIT (2022)

Determinar las amenazas

A través de la herramienta PILAR, se identifican las amenzas en base a la biblioteca de amenazas incorporadas en la herramienta, por cada uno de los activos.

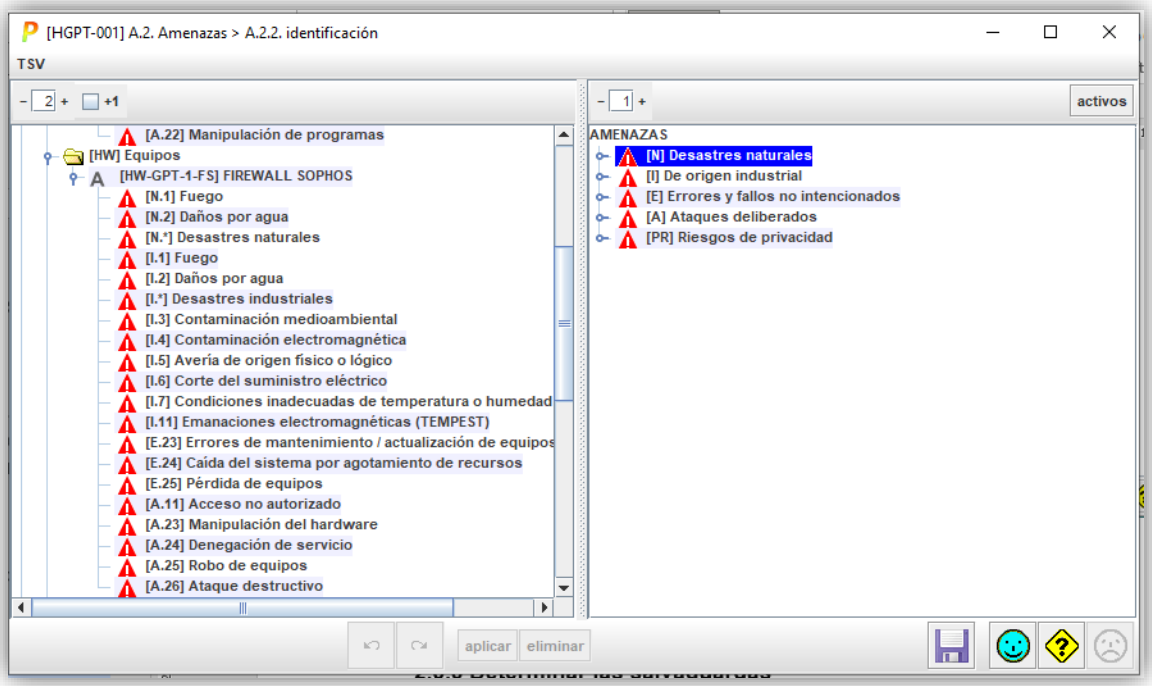
A continuación se muestran todas los posibles amenazas que proporciona PILAR sobre los activos:

Figura 18. Identificación de amenazas activos esenciales



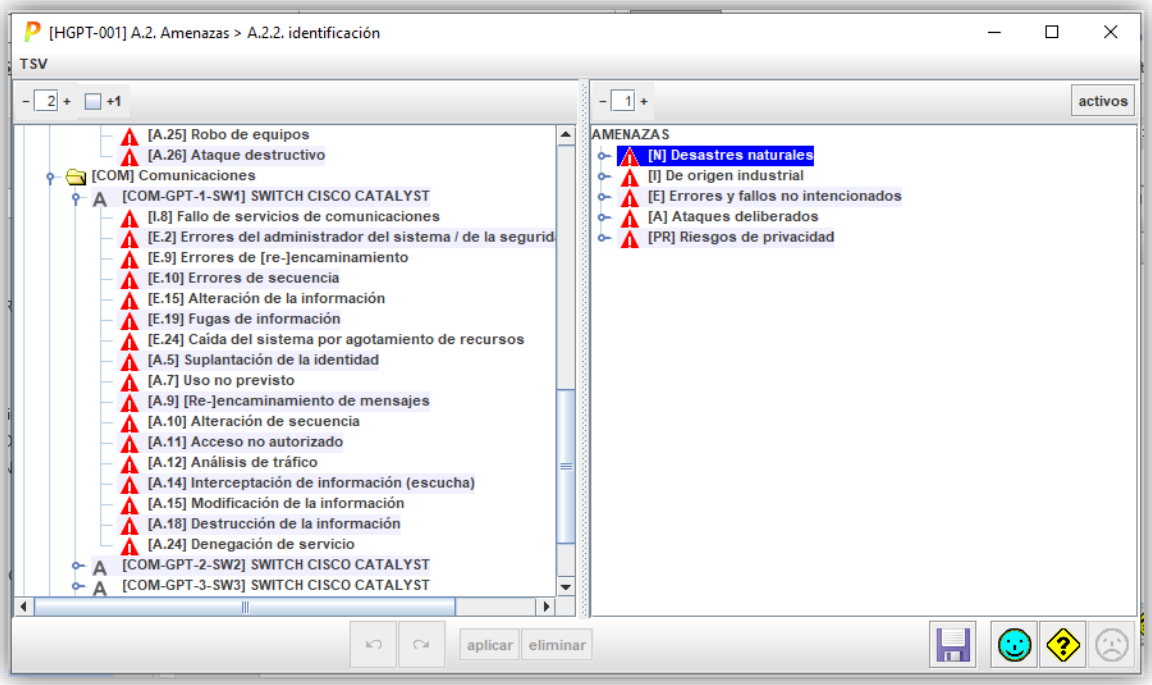
Fuente: PILAR – MAGERIT (2022)

Figura 19. Identificación de amenazas equipos



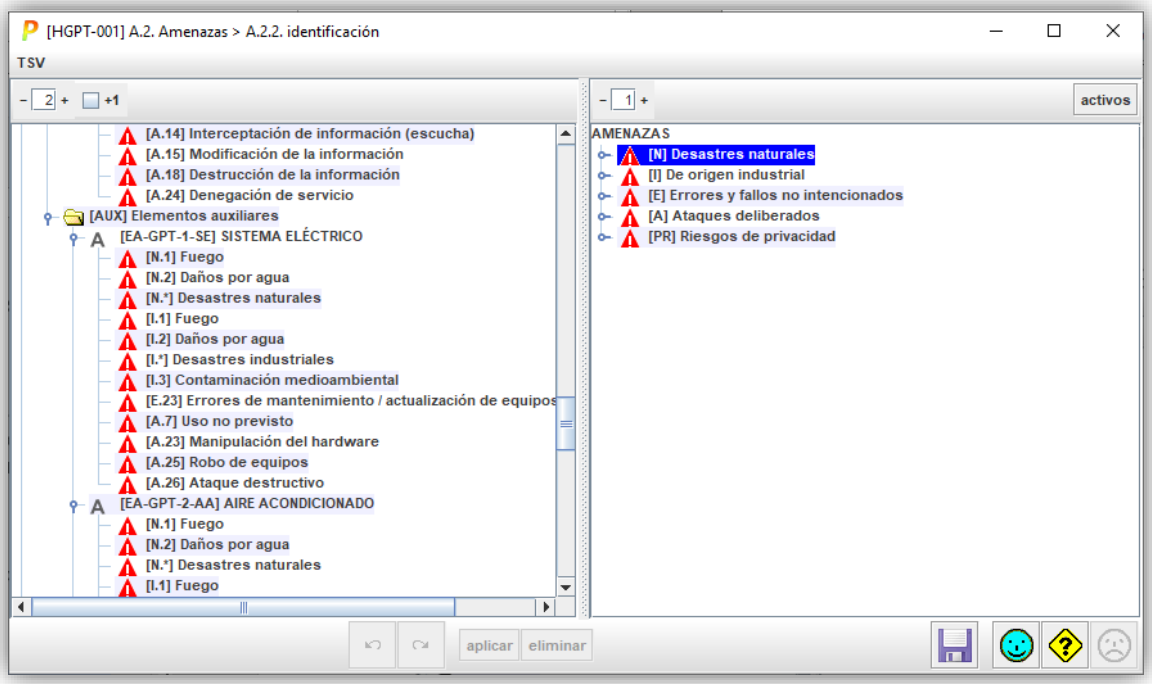
Fuente: PILAR – MAGERIT (2022)

Figura 20. Identificación de amenazas equipos de comunicaciones



Fuente: PILAR – MAGERIT (2022)

Figura 21. Identificación de amenazas elementos auxiliares



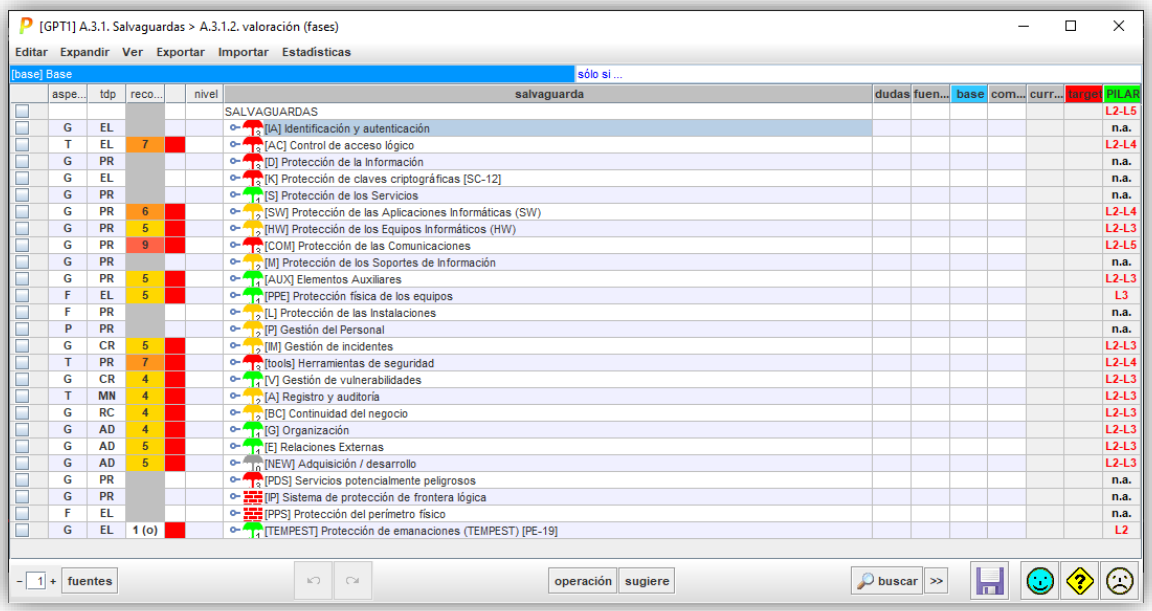
Fuente: PILAR – MAGERIT (2022)

Determinar las salvaguardas

A través de una inspección física realizada al Centro de Datos del Gobierno Provincial de Tungurahua, se determinó la existencia de las siguientes salvaguardas.

- Sistema de alimentación eléctrica ininterrumpida, en el caso de fallos eléctricos.
- Sistema de control de temperatura, el cual está configurado para alertar en el caso de elevaciones demasiado altas de temperatura.
- Firewall marca Sophos con licenciamiento de software, el cual controla la seguridad de la red de toda la Institución.
- Y, por último, pero no menos importante un extintor de CO_2 en el caso de incendio.

Figura 22. Identificación de salvaguardas

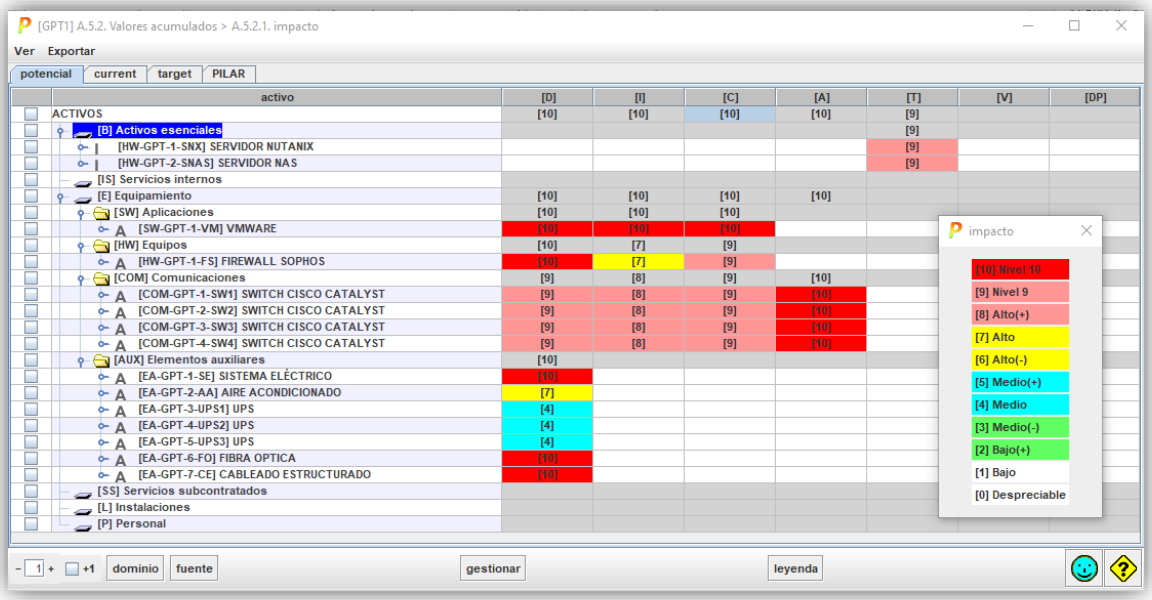


Fuente: PILAR – MAGERIT (2022)

Estimar el impacto

El impacto es el daño, que se origina sobre el activo derivado de la materialización de las amenazas. El cuadro de colores representa el nivel de impacto en base a una numeración de 0 a 10, mientras más alta sea la estimación del impacto la herramienta PILAR asignará un nivel de criticidad y pintará las alertas de cada activo.

Figura 23. Estimación del impacto

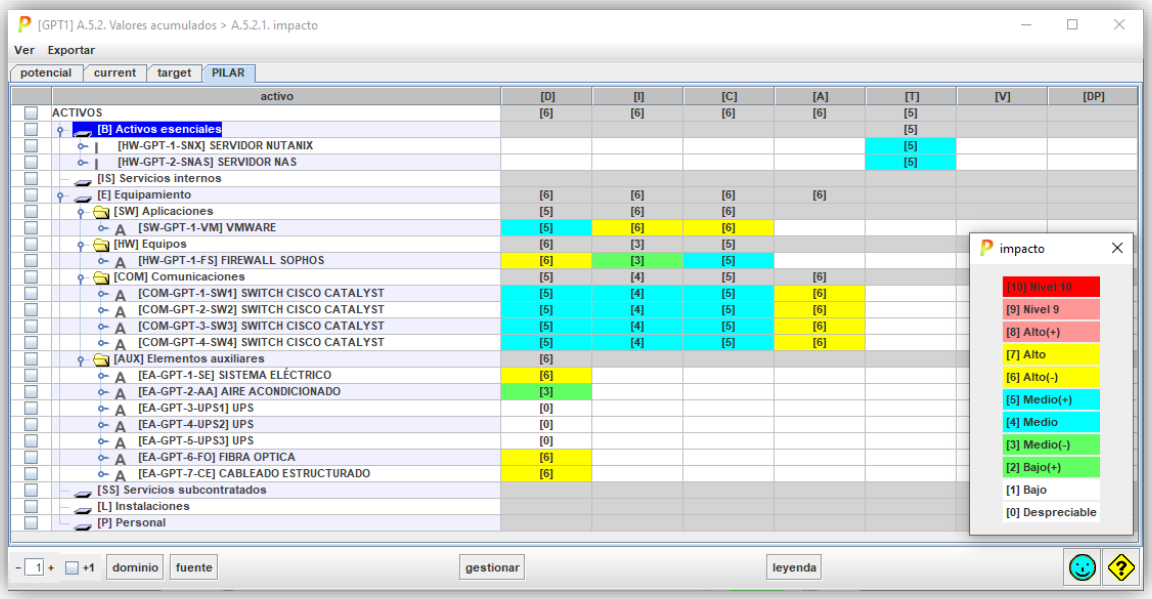


Fuente: PILAR – MAGERIT (2022)

De la misma forma PILAR brinda la posibilidad de realizar un análisis con la implementación de salvaguardas, las más apropiadas conforme el presente análisis, luego de lo cual es notorio que los valores y colores cambian considerablemente.

A continuación, se muestran los resultados:

Figura 24. Estimación del impacto después de la implementación de salvaguardas

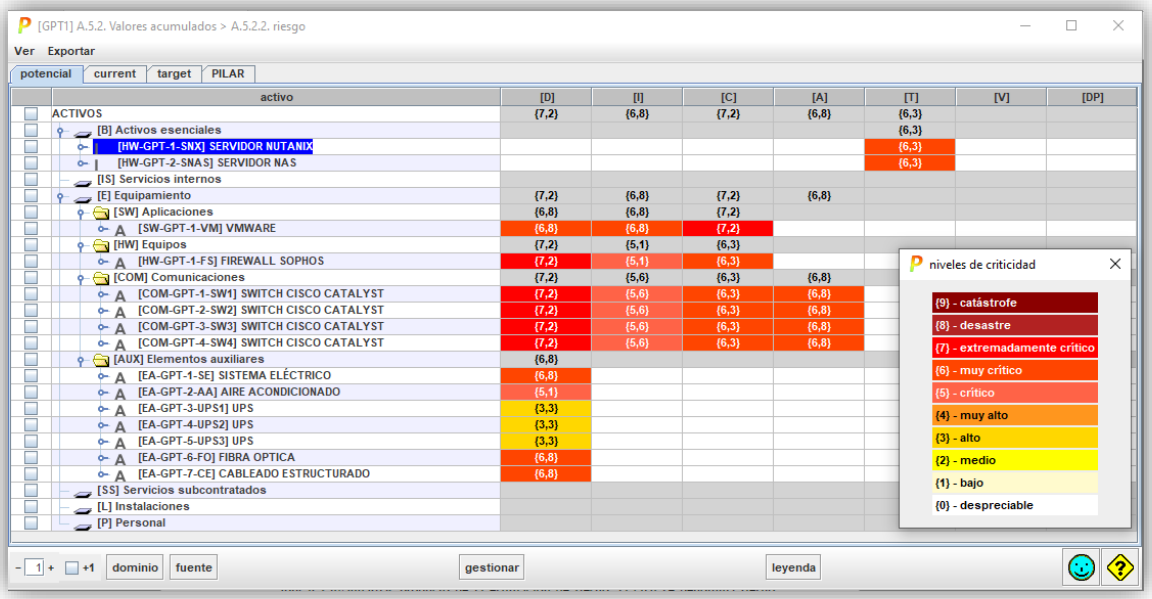


Fuente: PILAR – MAGERIT (2022)

Estimar el riesgo

La estimación del riesgo es el resultado de la relación entre la probabilidad que el riesgo ocurra, frente al impacto causado producto de la ocurrencia del riesgo. A continuación, se muestran los riesgos por activos:

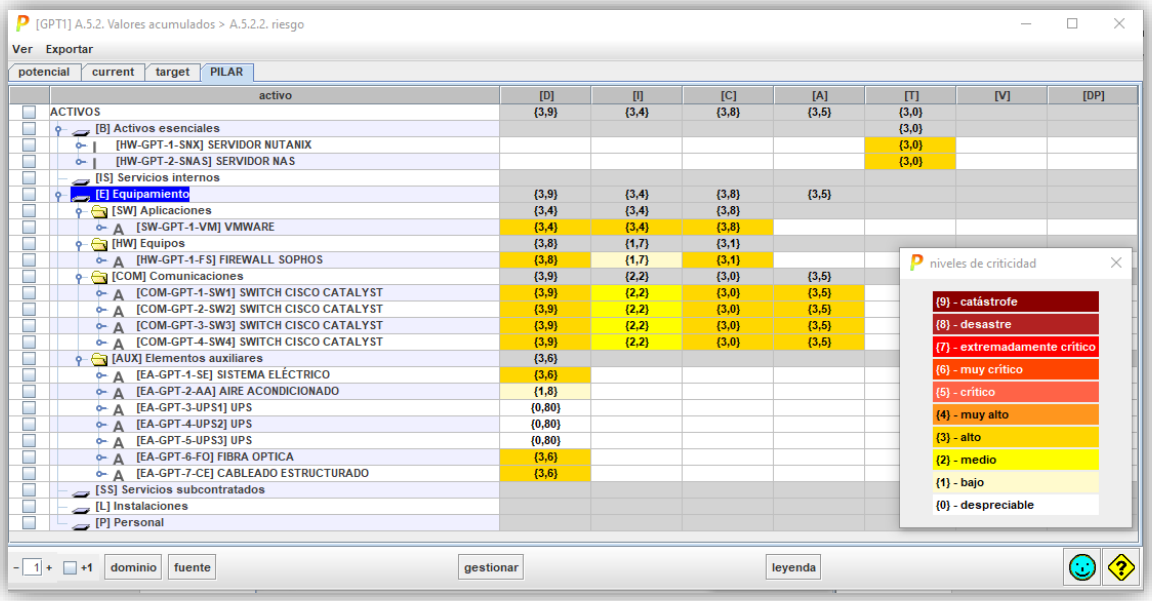
Figura 25. Estimación del riesgo



Fuente: PILAR – MAGERIT (2022)

PILAR proporciona los resultados de la interpretación de aplicar salvaguardas producto de la estimación del riesgo, la cual se denomina riesgo residual, es decir se ha modificado el riesgo de un valor potencial a un valor residual, lo cual claramente tiene un efecto significativo, sin embargo, aunque disminuye el riesgo no elimina en su totalidad dicho riesgo, o a su vez se considera la eficacia de las salvaguardas aplicadas.

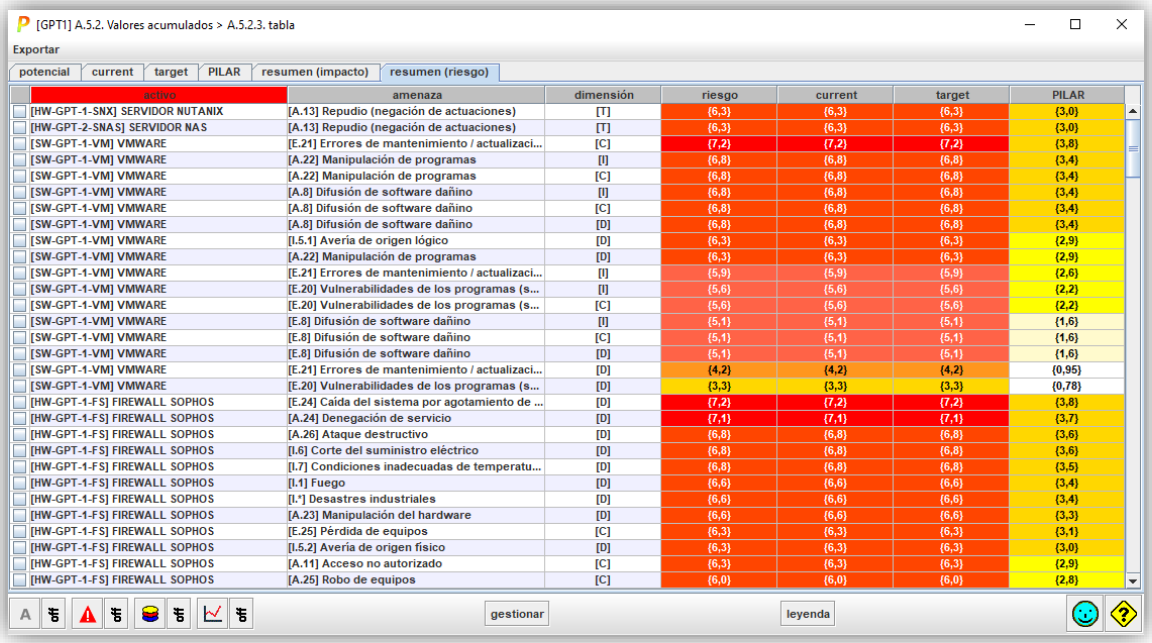
Figura 26. Riesgo residual



Fuente: PILAR – MAGERIT (2022)

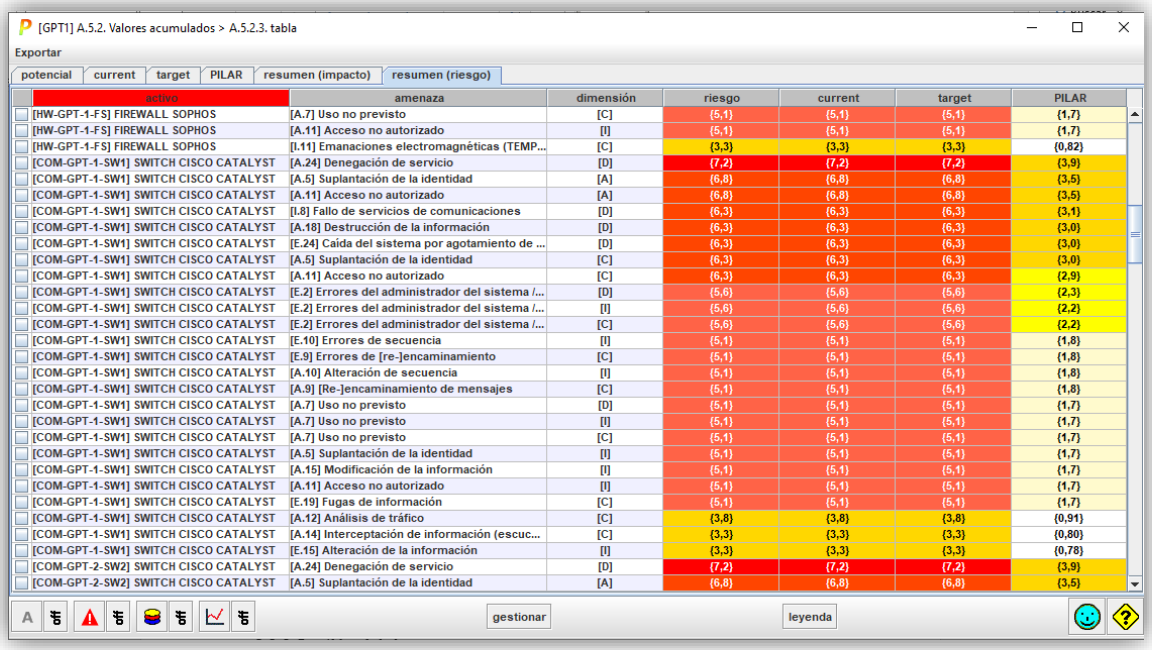
En los siguientes gráficos se muestra el resumen de los valores acumulados por activo:

Figura 27. Tabla de valores acumulados por activo



Fuente: PILAR – MAGERIT (2022)

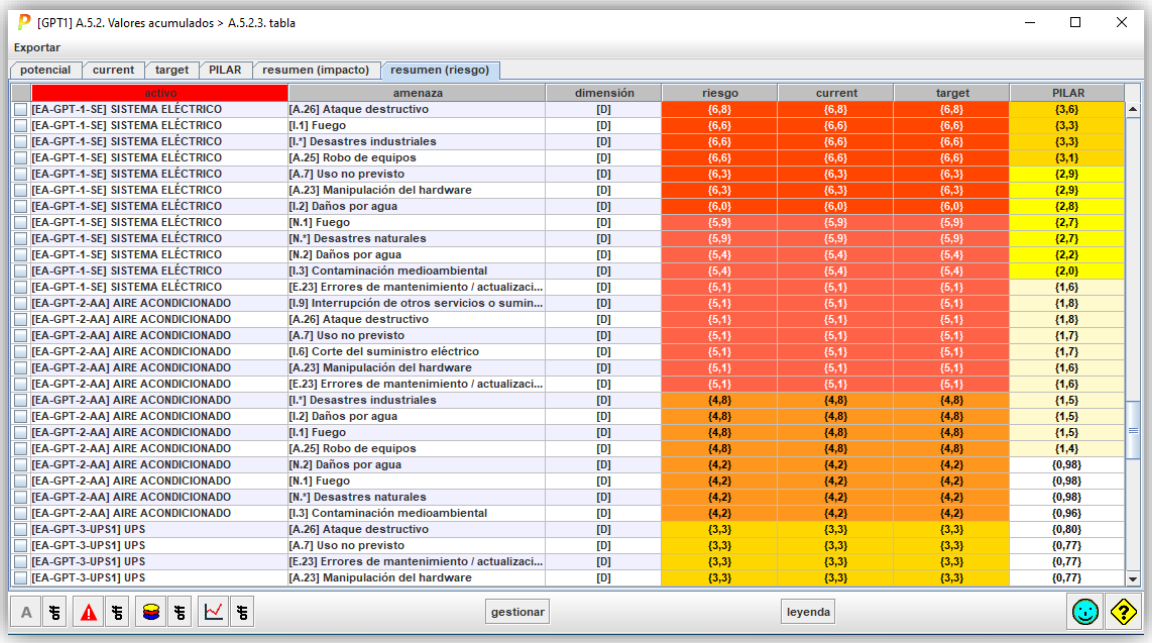
Figura 28. Tabla de valores acumulados por activo



activo	amenaza	dimensión	riesgo	current	target	PILAR
[HW-GPT-1-FS] FIREWALL SOPHOS	[A.7] Uso no previsto	[C]	{5,1}	{5,1}	{5,1}	{1,7}
[HW-GPT-1-FS] FIREWALL SOPHOS	[A.11] Acceso no autorizado	[I]	{5,1}	{5,1}	{5,1}	{1,7}
[HW-GPT-1-FS] FIREWALL SOPHOS	[I.11] Emanaciones electromagnéticas (TEMP...	[C]	{3,3}	{3,3}	{3,3}	{0,82}
[COM-GPT-1-SW1] SWITCH CISCO CATALYST	[A.24] Denegación de servicio	[D]	{7,2}	{7,2}	{7,2}	{3,9}
[COM-GPT-1-SW1] SWITCH CISCO CATALYST	[A.5] Suplantación de la identidad	[A]	{6,8}	{6,8}	{6,8}	{3,5}
[COM-GPT-1-SW1] SWITCH CISCO CATALYST	[A.11] Acceso no autorizado	[A]	{6,8}	{6,8}	{6,8}	{3,5}
[COM-GPT-1-SW1] SWITCH CISCO CATALYST	[I.8] Fallo de servicios de comunicaciones	[D]	{6,3}	{6,3}	{6,3}	{3,1}
[COM-GPT-1-SW1] SWITCH CISCO CATALYST	[A.18] Destrucción de la información	[D]	{6,3}	{6,3}	{6,3}	{3,0}
[COM-GPT-1-SW1] SWITCH CISCO CATALYST	[E.24] Caída del sistema por agotamiento de ...	[D]	{6,3}	{6,3}	{6,3}	{3,0}
[COM-GPT-1-SW1] SWITCH CISCO CATALYST	[A.5] Suplantación de la identidad	[C]	{6,3}	{6,3}	{6,3}	{3,0}
[COM-GPT-1-SW1] SWITCH CISCO CATALYST	[A.11] Acceso no autorizado	[C]	{6,3}	{6,3}	{6,3}	{2,9}
[COM-GPT-1-SW1] SWITCH CISCO CATALYST	[E.2] Errores del administrador del sistema /...	[D]	{5,6}	{5,6}	{5,6}	{2,3}
[COM-GPT-1-SW1] SWITCH CISCO CATALYST	[E.2] Errores del administrador del sistema /...	[I]	{5,6}	{5,6}	{5,6}	{2,2}
[COM-GPT-1-SW1] SWITCH CISCO CATALYST	[E.2] Errores del administrador del sistema /...	[C]	{5,6}	{5,6}	{5,6}	{2,2}
[COM-GPT-1-SW1] SWITCH CISCO CATALYST	[E.10] Errores de secuencia	[I]	{5,1}	{5,1}	{5,1}	{1,8}
[COM-GPT-1-SW1] SWITCH CISCO CATALYST	[E.9] Errores de [re-]encaminamiento	[C]	{5,1}	{5,1}	{5,1}	{1,8}
[COM-GPT-1-SW1] SWITCH CISCO CATALYST	[A.10] Alteración de secuencia	[I]	{5,1}	{5,1}	{5,1}	{1,8}
[COM-GPT-1-SW1] SWITCH CISCO CATALYST	[A.9] [Re-]encaminamiento de mensajes	[C]	{5,1}	{5,1}	{5,1}	{1,8}
[COM-GPT-1-SW1] SWITCH CISCO CATALYST	[A.7] Uso no previsto	[D]	{5,1}	{5,1}	{5,1}	{1,7}
[COM-GPT-1-SW1] SWITCH CISCO CATALYST	[A.7] Uso no previsto	[I]	{5,1}	{5,1}	{5,1}	{1,7}
[COM-GPT-1-SW1] SWITCH CISCO CATALYST	[A.7] Uso no previsto	[C]	{5,1}	{5,1}	{5,1}	{1,7}
[COM-GPT-1-SW1] SWITCH CISCO CATALYST	[A.5] Suplantación de la identidad	[I]	{5,1}	{5,1}	{5,1}	{1,7}
[COM-GPT-1-SW1] SWITCH CISCO CATALYST	[A.15] Modificación de la información	[I]	{5,1}	{5,1}	{5,1}	{1,7}
[COM-GPT-1-SW1] SWITCH CISCO CATALYST	[A.11] Acceso no autorizado	[I]	{5,1}	{5,1}	{5,1}	{1,7}
[COM-GPT-1-SW1] SWITCH CISCO CATALYST	[E.19] Fugas de información	[C]	{5,1}	{5,1}	{5,1}	{1,7}
[COM-GPT-1-SW1] SWITCH CISCO CATALYST	[A.12] Análisis de tráfico	[C]	{3,8}	{3,8}	{3,8}	{0,91}
[COM-GPT-1-SW1] SWITCH CISCO CATALYST	[A.14] Interceptación de información (escuc...	[C]	{3,3}	{3,3}	{3,3}	{0,80}
[COM-GPT-1-SW1] SWITCH CISCO CATALYST	[E.15] Alteración de la información	[I]	{3,3}	{3,3}	{3,3}	{0,78}
[COM-GPT-2-SW2] SWITCH CISCO CATALYST	[A.24] Denegación de servicio	[D]	{7,2}	{7,2}	{7,2}	{3,9}
[COM-GPT-2-SW2] SWITCH CISCO CATALYST	[A.5] Suplantación de la identidad	[A]	{6,8}	{6,8}	{6,8}	{3,5}

Fuente: PILAR – MAGERIT (2022)

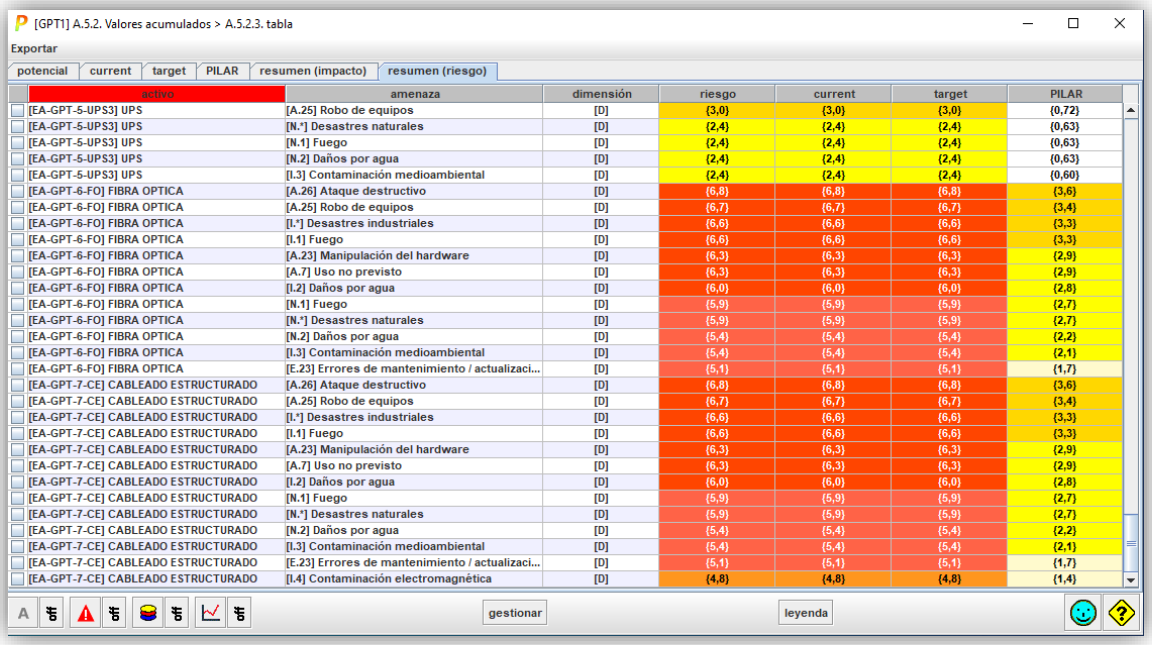
Figura 29. Tabla de valores acumulados por activo



activo	amenaza	dimensión	riesgo	current	target	PILAR
[EA-GPT-1-SE] SISTEMA ELÉCTRICO	[A.26] Ataque destructivo	[D]	{6,8}	{6,8}	{6,8}	{3,6}
[EA-GPT-1-SE] SISTEMA ELÉCTRICO	[I.1] Fuego	[D]	{6,6}	{6,6}	{6,6}	{3,3}
[EA-GPT-1-SE] SISTEMA ELÉCTRICO	[I.*] Desastres industriales	[D]	{6,6}	{6,6}	{6,6}	{3,3}
[EA-GPT-1-SE] SISTEMA ELÉCTRICO	[A.25] Robo de equipos	[D]	{6,6}	{6,6}	{6,6}	{3,1}
[EA-GPT-1-SE] SISTEMA ELÉCTRICO	[A.7] Uso no previsto	[D]	{6,3}	{6,3}	{6,3}	{2,9}
[EA-GPT-1-SE] SISTEMA ELÉCTRICO	[A.23] Manipulación del hardware	[D]	{6,3}	{6,3}	{6,3}	{2,9}
[EA-GPT-1-SE] SISTEMA ELÉCTRICO	[I.2] Daños por agua	[D]	{6,0}	{6,0}	{6,0}	{2,8}
[EA-GPT-1-SE] SISTEMA ELÉCTRICO	[N.1] Fuego	[D]	{5,9}	{5,9}	{5,9}	{2,7}
[EA-GPT-1-SE] SISTEMA ELÉCTRICO	[N.*] Desastres naturales	[D]	{5,9}	{5,9}	{5,9}	{2,7}
[EA-GPT-1-SE] SISTEMA ELÉCTRICO	[N.2] Daños por agua	[D]	{5,4}	{5,4}	{5,4}	{2,2}
[EA-GPT-1-SE] SISTEMA ELÉCTRICO	[I.3] Contaminación medioambiental	[D]	{5,4}	{5,4}	{5,4}	{2,0}
[EA-GPT-1-SE] SISTEMA ELÉCTRICO	[E.23] Errores de mantenimiento / actualizaci...	[D]	{5,1}	{5,1}	{5,1}	{1,6}
[EA-GPT-2-AA] AIRE ACONDICIONADO	[I.9] Interrupción de otros servicios o sumin...	[D]	{5,1}	{5,1}	{5,1}	{1,8}
[EA-GPT-2-AA] AIRE ACONDICIONADO	[A.26] Ataque destructivo	[D]	{5,1}	{5,1}	{5,1}	{1,8}
[EA-GPT-2-AA] AIRE ACONDICIONADO	[A.7] Uso no previsto	[D]	{5,1}	{5,1}	{5,1}	{1,7}
[EA-GPT-2-AA] AIRE ACONDICIONADO	[I.6] Corte del suministro eléctrico	[D]	{5,1}	{5,1}	{5,1}	{1,7}
[EA-GPT-2-AA] AIRE ACONDICIONADO	[A.23] Manipulación del hardware	[D]	{5,1}	{5,1}	{5,1}	{1,6}
[EA-GPT-2-AA] AIRE ACONDICIONADO	[E.23] Errores de mantenimiento / actualizaci...	[D]	{5,1}	{5,1}	{5,1}	{1,6}
[EA-GPT-2-AA] AIRE ACONDICIONADO	[I.*] Desastres industriales	[D]	{4,8}	{4,8}	{4,8}	{1,5}
[EA-GPT-2-AA] AIRE ACONDICIONADO	[I.2] Daños por agua	[D]	{4,8}	{4,8}	{4,8}	{1,5}
[EA-GPT-2-AA] AIRE ACONDICIONADO	[I.1] Fuego	[D]	{4,8}	{4,8}	{4,8}	{1,5}
[EA-GPT-2-AA] AIRE ACONDICIONADO	[A.25] Robo de equipos	[D]	{4,8}	{4,8}	{4,8}	{1,4}
[EA-GPT-2-AA] AIRE ACONDICIONADO	[N.2] Daños por agua	[D]	{4,2}	{4,2}	{4,2}	{0,98}
[EA-GPT-2-AA] AIRE ACONDICIONADO	[N.1] Fuego	[D]	{4,2}	{4,2}	{4,2}	{0,98}
[EA-GPT-2-AA] AIRE ACONDICIONADO	[N.*] Desastres naturales	[D]	{4,2}	{4,2}	{4,2}	{0,98}
[EA-GPT-2-AA] AIRE ACONDICIONADO	[I.3] Contaminación medioambiental	[D]	{4,2}	{4,2}	{4,2}	{0,96}
[EA-GPT-3-UPS1] UPS	[A.26] Ataque destructivo	[D]	{3,3}	{3,3}	{3,3}	{0,80}
[EA-GPT-3-UPS1] UPS	[A.7] Uso no previsto	[D]	{3,3}	{3,3}	{3,3}	{0,77}
[EA-GPT-3-UPS1] UPS	[E.23] Errores de mantenimiento / actualizaci...	[D]	{3,3}	{3,3}	{3,3}	{0,77}
[EA-GPT-3-UPS1] UPS	[A.23] Manipulación del hardware	[D]	{3,3}	{3,3}	{3,3}	{0,77}

Fuente: PILAR – MAGERIT (2022)

Figura 30. Tabla de valores acumulados por activo



activo	amenaza	dimensión	riesgo	current	target	PILAR
[EA-GPT-5-UPS3] UPS	[A.25] Robo de equipos	[D]	{3,0}	{3,0}	{3,0}	{0,72}
[EA-GPT-5-UPS3] UPS	[N.*] Desastres naturales	[D]	{2,4}	{2,4}	{2,4}	{0,63}
[EA-GPT-5-UPS3] UPS	[N.1] Fuego	[D]	{2,4}	{2,4}	{2,4}	{0,63}
[EA-GPT-5-UPS3] UPS	[N.2] Daños por agua	[D]	{2,4}	{2,4}	{2,4}	{0,63}
[EA-GPT-5-UPS3] UPS	[I.3] Contaminación medioambiental	[D]	{2,4}	{2,4}	{2,4}	{0,60}
[EA-GPT-6-FO] FIBRA OPTICA	[A.26] Ataque destructivo	[D]	{6,8}	{6,8}	{6,8}	{3,6}
[EA-GPT-6-FO] FIBRA OPTICA	[A.25] Robo de equipos	[D]	{6,7}	{6,7}	{6,7}	{3,4}
[EA-GPT-6-FO] FIBRA OPTICA	[I.*] Desastres industriales	[D]	{6,6}	{6,6}	{6,6}	{3,3}
[EA-GPT-6-FO] FIBRA OPTICA	[I.1] Fuego	[D]	{6,6}	{6,6}	{6,6}	{3,3}
[EA-GPT-6-FO] FIBRA OPTICA	[A.23] Manipulación del hardware	[D]	{6,3}	{6,3}	{6,3}	{2,9}
[EA-GPT-6-FO] FIBRA OPTICA	[A.7] Uso no previsto	[D]	{6,3}	{6,3}	{6,3}	{2,9}
[EA-GPT-6-FO] FIBRA OPTICA	[I.2] Daños por agua	[D]	{6,0}	{6,0}	{6,0}	{2,8}
[EA-GPT-6-FO] FIBRA OPTICA	[N.1] Fuego	[D]	{5,9}	{5,9}	{5,9}	{2,7}
[EA-GPT-6-FO] FIBRA OPTICA	[N.*] Desastres naturales	[D]	{5,9}	{5,9}	{5,9}	{2,7}
[EA-GPT-6-FO] FIBRA OPTICA	[N.2] Daños por agua	[D]	{5,4}	{5,4}	{5,4}	{2,2}
[EA-GPT-6-FO] FIBRA OPTICA	[I.3] Contaminación medioambiental	[D]	{5,4}	{5,4}	{5,4}	{2,1}
[EA-GPT-6-FO] FIBRA OPTICA	[E.23] Errores de mantenimiento / actualizaci...	[D]	{5,1}	{5,1}	{5,1}	{1,7}
[EA-GPT-7-CE] CABLEADO ESTRUCTURADO	[A.26] Ataque destructivo	[D]	{6,8}	{6,8}	{6,8}	{3,6}
[EA-GPT-7-CE] CABLEADO ESTRUCTURADO	[A.25] Robo de equipos	[D]	{6,7}	{6,7}	{6,7}	{3,4}
[EA-GPT-7-CE] CABLEADO ESTRUCTURADO	[I.*] Desastres industriales	[D]	{6,6}	{6,6}	{6,6}	{3,3}
[EA-GPT-7-CE] CABLEADO ESTRUCTURADO	[I.1] Fuego	[D]	{6,6}	{6,6}	{6,6}	{3,3}
[EA-GPT-7-CE] CABLEADO ESTRUCTURADO	[A.23] Manipulación del hardware	[D]	{6,3}	{6,3}	{6,3}	{2,9}
[EA-GPT-7-CE] CABLEADO ESTRUCTURADO	[A.7] Uso no previsto	[D]	{6,3}	{6,3}	{6,3}	{2,9}
[EA-GPT-7-CE] CABLEADO ESTRUCTURADO	[I.2] Daños por agua	[D]	{6,0}	{6,0}	{6,0}	{2,8}
[EA-GPT-7-CE] CABLEADO ESTRUCTURADO	[N.1] Fuego	[D]	{5,9}	{5,9}	{5,9}	{2,7}
[EA-GPT-7-CE] CABLEADO ESTRUCTURADO	[N.*] Desastres naturales	[D]	{5,9}	{5,9}	{5,9}	{2,7}
[EA-GPT-7-CE] CABLEADO ESTRUCTURADO	[N.2] Daños por agua	[D]	{5,4}	{5,4}	{5,4}	{2,2}
[EA-GPT-7-CE] CABLEADO ESTRUCTURADO	[I.3] Contaminación medioambiental	[D]	{5,4}	{5,4}	{5,4}	{2,1}
[EA-GPT-7-CE] CABLEADO ESTRUCTURADO	[E.23] Errores de mantenimiento / actualizaci...	[D]	{5,1}	{5,1}	{5,1}	{1,7}
[EA-GPT-7-CE] CABLEADO ESTRUCTURADO	[I.4] Contaminación electromagnética	[D]	{4,8}	{4,8}	{4,8}	{1,4}

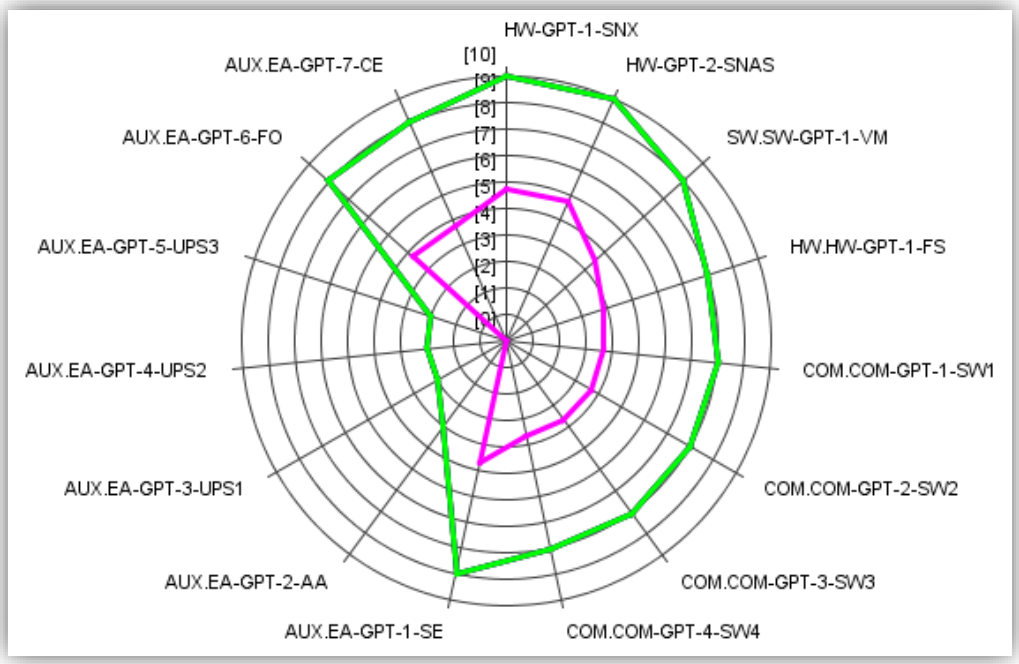
Fuente: PILAR – MAGERIT (2022)

Interpretación de resultados

Una vez realizado el análisis de riesgo con PILAR, los activos que reflejan mayor índice de riesgo son el SERVIDOR NUTANIX y el SERVIDOR NAS, de la misma forma los activos de telecomunicaciones reflejan un riesgo bastante considerable por lo que es necesario gestionar dichos riesgos.

A continuación, se muestran los gráficos con la interpretación de los resultados:

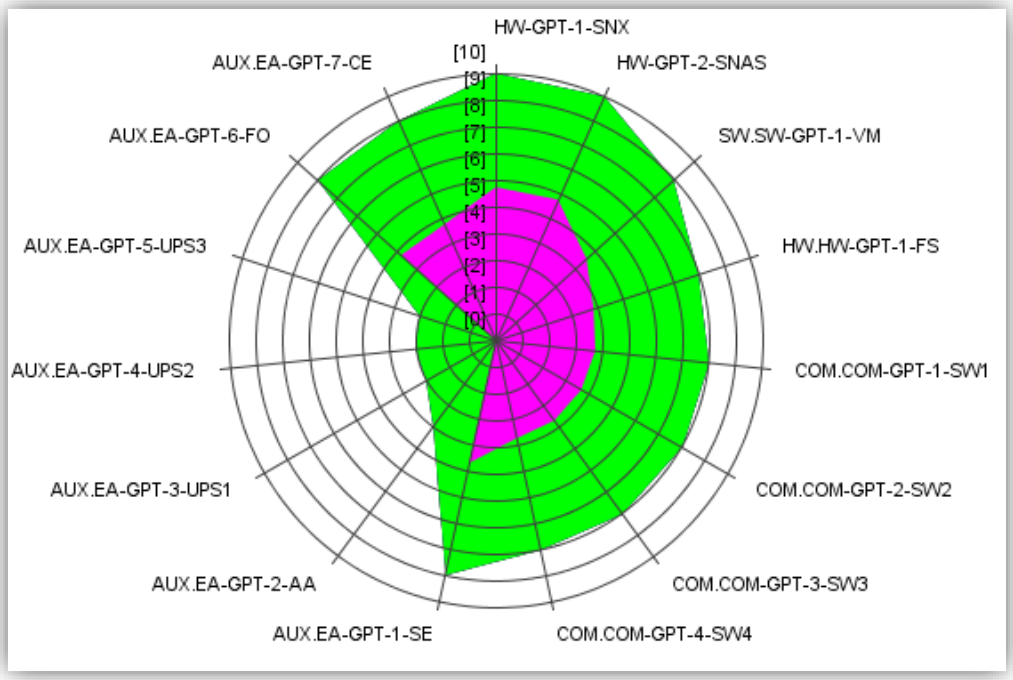
Figura 31. Gráfico de resultados



Fuente: PILAR – MAGERIT (2022)

En base al gráfico se determina en una escala del 1 al 10 donde 1 es el más bajo y 10 el más alto, los activos del Gobierno Provincial de Tungurahua con alto grado de riesgo, que almacenan gran parte de información relevante para la Institución, así como los activos de interconexión de red, son los más expuestos y los que generan un alto grado de interés para establecer medidas de protección.

Figura 32. Gráfico de resultados



Fuente: PILAR – MAGERIT (2022)

El gráfico ratifica lo dicho y surge la necesidad de contar con medidas que minimicen los riesgos, gestionar dichos riesgos en base a una política de seguridad de la información y partir de allí establecer las medidas más convenientes en beneficio del Gobierno Provincial de Tungurahua.

Gestión del riesgo

El Libro I de la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Magerit versión 3, establece los siguientes lineamientos para la gestión de riesgos:

- Si el riesgo es **crítico** requiere atención urgente.
- Si el riesgo es **grave** requiere atención.
- Si el riesgo es **apreciable** es objeto de estudio para su tratamiento.
- Y si el riesgo es **asumible** no hay la necesidad de tomar acciones, aunque cabe hacer una aclaración, la aceptación de un riesgo siempre va a ser arriesgada, hay que tomarla con prudencia y justificación.

Las razones por las cuales se acepta un riesgo son las siguientes:

- Si el impacto residual es completamente asumible.
- Si el riesgo residual es asumible.
- Si el coste de las salvaguardas oportunas es desproporcionado en comparación al impacto y riesgos residuales.

Para tratar los riesgos la metodología Magerit recomienda varias opciones para tratar los riesgos, las cuales se citan a continuación:

- **Eliminación del Riesgo. -** Consiste en eliminar el activo más comprometido y asociado con el riesgo. Esta medida es sumamente drástica y costosa.

- **Transferir el Riesgo. -** Consiste en valorar la subcontratación de un servicio de almacenamiento de información o la contratación de un seguro, También es una opción costosa por los costos elevados que implica optar por esta opción, de la misma forma la ser una Institución Pública se dispone de recursos económicos limitados y asociados con un Plan Anual de Compras previamente analizado y aprobado.

- **Asumir el Riesgo. -** Consiste en analizar el riesgo y asumir el control de dicho riesgo y vigilarlo constantemente con el fin de que, no se propague o aumente.

- **Mitigar el Riesgo. -** Finalmente esta opción es la más identificada y opcionada después de una análisis y evaluación de riesgos, puesto que la Institución implantaría una serie de medidas y salvaguardas para cada uno de los activos con el fin de blindarse y fortalecer las medidas en contra de los riesgos y amenazas que ponen en riesgo los activos de la institución.

CAPÍTULO III. ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN

3.1. Guía de Seguridad de la Información

Razón para emitir una guía de Seguridad de la Información

La información en todas sus formas es un activo imprescindible para una organización, ya sea esta pública o privada, la misma que sería protegida y resguardada de forma adecuada.
La presente guía tiene como finalidad elevar el cuidado y protección de la información con lineamientos, recomendaciones, tras una adecuada gestión de riesgos y acorde a la realidad del Gobierno Provincial de Tungurahua.

Características

Esta guía toma como base los riesgos que implica la seguridad de la información desde una perspectiva de cumplimiento de directrices.
Mediante una evaluación de riesgos se logra obtener un panorama claro de la situación actual de la empresa y busca alcanzar la madurez en materia de seguridad de la información.

Introducción

La Guía de Seguridad de la Información del Gobierno Provincial de Tungurahua establece lineamientos y políticas administrativas, técnicas y legales, las cuales adoptarán los funcionarios de la Institución y personal externo que utilice los servicios tecnológicos de la Entidad Provincial.
El objetivo es definir una Guía de Seguridad de la Información, con el propósito de regular la Gestión de Seguridad de la Información, y de esta forma garantizar los principios de confidencialidad, integridad, disponibilidad, confiabilidad y no repudio de la información.

Consideraciones importantes

- La Máxima Autoridad del Gobierno Provincial de Tungurahua es la responsable de apoyar el proceso de implementación de la Guía de Gestión de Seguridad de la Información y asignar los recursos necesarios para su cumplimiento.
- La Dirección de Sistemas y Tecnologías de la Información del Gobierno Provincial de Tungurahua es la responsable de gestión, asesoría y apoyo ante cualquier actividad relacionada con la Seguridad de la Información.
- La Dirección de Sistemas y Tecnologías de la Información del Gobierno Provincial de Tungurahua es la responsable de supervisar la implementación de la presente Guía de Seguridad de la Información y velar por su cumplimiento.
- La Dirección de Sistemas y Tecnologías de la Información del Gobierno Provincial de Tungurahua es la responsable de verificar de forma periódica el cumplimiento de la presente Guía.
- La revisión, actualización y mejoras, que se deriven a corto, mediano o largo plazo de la presente Guía, es responsabilidad de la Dirección de Sistemas y Tecnologías de la Información del Gobierno Provincial de Tungurahua.

Elementos

Política de Seguridad

La Política de Seguridad especifica los lineamientos de cumplimiento por parte de todos los funcionarios del Gobierno Provincial de Tungurahua, enfocada en la Seguridad de la Información y de esta forma asegurar los niveles de confidencialidad, integridad y disponibilidad de la Información.

Organización Interna

Define las directrices para gestionar la seguridad de la información dentro del Gobierno Provincial de Tungurahua.

Comité de Seguridad de la Información

La Máxima Autoridad del Gobierno Provincial de Tungurahua designa un Comité de Seguridad de la Información, el cual se conforma por un delegado de cada una de las Direcciones que conforman el Gobierno Provincial de Tungurahua, el comité lo lidera el Director de Sistemas y Tecnologías de la Información.

El Comité de Seguridad de la Información sesionará de forma trimestral con el fin de revisar, aprobar proyectos y otras actividades inherentes a la Seguridad de la Información del Gobierno Provincial de Tungurahua.

Acuerdos de confidencialidad

El Gobierno Provincial de Tungurahua establecerá un mecanismo de aceptación del compromiso de confidencialidad e integridad de la información institucional para ser aplicado a todos los funcionarios que por cualquier razón requieran acceso a la plataforma tecnológica o a los sistemas de información de la Entidad Provincial.

Segregación de funciones

El Gobierno Provincial de Tungurahua definirá de forma clara y precisa, la segregación de funciones mediante el establecimiento de roles y permisos para los funcionarios de la Entidad Provincial, que tienen a cargo la administración técnica y funcional de los sistemas de información, aplicativos y usuarios con privilegios en las diferentes computadoras.

Esta división establece diferentes etapas de aprobación, autorización, ejecución y mantenimiento de registros a cargo de los funcionarios asignados en cada función. De esta manera se garantiza la transparencia, se evitarán los errores involuntarios y posiciones de poder que faciliten actuaciones indebidas.
Todo proyecto, que se desarrolle en la Entidad Provincial dentro de sus consideraciones se considera la inclusión de un capítulo relativo a la Seguridad de la Información, que se maneje dentro del mismo.

Seguridad de conexiones remotas

En situaciones controladas por el Gobierno Provincial de Tungurahua permitirá o no el acceso de terceros y usuarios externos a sus redes internas, para ello contará estrictamente con la aprobación y autorización del Director Departamental del área requirente, el responsable de la Dirección de Sistemas y estará avalado por el Oficial o Delegado de Seguridad de la Información.
En caso de contar con la aprobación y acceso se lo realizará mediante uso de una VPN (Virtual Private Network) Institucional.

Autorización y uso de Redes Inalámbricas

Todos los usuarios que accedan a la red inalámbrica del Gobierno Provincial de Tungurahua aceptan de forma directa las políticas, términos y condiciones y condiciones futuras, que se derivan de la presente guía.

Es de carácter obligatorio la autorización del Director Departamental del área requirente, el responsable de la Dirección de Sistemas y estará avalado por el Oficial o Delegado de Seguridad de la Información.

La Dirección de Sistemas y Tecnologías de la Información verificará requisitos técnicos mínimos para el correcto uso de la red Institucional.

Se prohíbe explícitamente el uso de la red Institucional para propósitos de índole personal o particular que tengan alguna repercusión negativa y que

llegaría a afectar la Seguridad implementada en la Red de la Entidad Provincial.

Gestión de los activos de información

Este control tiene como propósito mantener la protección adecuada de los activos del Gobierno Provincial de Tungurahua.
Contar con un adecuado inventario de activos para lograr mantener la protección de los activos del Gobierno Provincial de Tungurahua. El inventario incluirá la información relevante al tipo de activo que especifique su ubicación, características, condiciones, información de licencias y su valor económico estimado. Los activos se asignarán a un funcionario responsable de su custodia y protección conforme la normativa legal vigente.

Propiedad de los activos

Los activos adquiridos, así como la información que en ellos se genere, almacene o procese son de propiedad del Gobierno Provincial de Tungurahua. La organización en cualquier momento dispondría de esos activos y se los entregaría a otro funcionario para su custodia y protección.

Uso aceptable de los activos

El funcionario responsable por la custodia y protección de los activos se llamará designado. Se tendrá una base de datos donde se asignará a cada activo a su designado. Identificar a los designados para los activos y asignar responsabilidades de implementación y mantenimiento de los controles adecuados.

Clasificación de la información

Este control asegura que la información recibe el nivel adecuado de protección. Este proceso de clasificación es muy importante para cumplir con los

lineamientos de seguridad de la información dispuestos por la Entidad Provincial.

Esta guía también combina dos principios básicos de control de acceso. Para la información más sensitiva, utiliza el principio de “necesidad de saber”, y para la menos sensitiva, el principio de “necesidad de retención”.

Debido al hecho que la información es uno de los recursos más valiosos para el cumplimiento de la misión funcional del Gobierno Provincial de Tungurahua, es necesario conocer con que activos de información se cuenta, quién es su correspondiente propietario y qué niveles de clasificación se requieren, de manera, que se logre identificar claramente, cómo sería esta información administrada, transportada o procesada, con el fin de protegerla de acuerdo a su importancia, criticidad y nivel de confidencialidad requerido durante su utilización dentro de la Entidad Provincial, contra una posible divulgación no autorizada, uso indebido, modificación no autorizada y posible destrucción o borrado ya sea este intencional o accidental.

La información estará protegida a lo largo de su ciclo de vida, desde su creación hasta su destrucción. Sin estas políticas el Gobierno Provincial de Tungurahua está expuesto a la pérdida de credibilidad ante la opinión pública, interrupciones en la operación, costos excesivos, e inclusive demandas por parte de otras Entidades estatales o personas naturales.

Esta información estará protegida proporcionalmente a su nivel de sensibilidad, sin importar el lugar, su forma, que tecnología fue usada para manejarla, y el propósito para el que ella existe y ser revisado este nivel de clasificación al menos una vez al año.

Directrices de clasificación

Toda información existente, generada y modificada que exista en los equipos de cómputo, sistemas de información y bases de datos del Gobierno Provincial de Tungurahua, se clasificará de acuerdo con los lineamientos establecidos en

el presente trabajo de investigación, conforme a una política de confidencialidad, integridad y disponibilidad.

Se considera información confidencial cualquier dato sensible, que se usa para discriminar, hacer daño o permitir a otros atentar o causar cualquier tipo de acción ilegal. La información que, no se revela a terceros y no es pública es información confidencial.

Clasificación por confidencialidad

Por confidencialidad, la información se clasifica en uno de los siguientes niveles:

CF1: Información que está al alcance de todos y no genera ninguna pérdida de vidas ni atenta contra la integridad del ciudadano.
Por ejemplo, información de promoción y divulgación de derechos humanos.

CF2: Información que no es altamente confidencial pero que, no sería de uso y conocimiento público, es decir, aquella cuyo conocimiento crea expectativas y producir pérdidas económicas bajas o atentar contra la integridad personal.
Por ejemplo, información de la hoja de vida de los empleados. En este tipo de documentos consta información personal y sensible si se quiere y solo estará al alcance de personal autorizado.

CF3: Información altamente confidencial y sensible; su conocimiento genera situaciones de riesgo para ciudadanos, desprestigio para la entidad.
Por ejemplo, informes de situaciones de riesgos y alertas tempranas, información financiera del peticionario.

Clasificación por integridad

Por integridad, la información se clasifica en uno de los siguientes niveles:
IN1: Información de naturaleza no financiera que no tenga repercusión en decisiones de relevancia administrativa, si fuera errada; la pérdida que origina

es pequeña y su reconstrucción o recuperación consiste en la repetición de un proceso sencillo.

IN2: Información relacionada con la gestión provincial y aquella en la cual se basan las decisiones de operación y uso diario de la organización y que necesita un nivel muy razonable de protección contra errores y fraude.

IN3: Información para la toma de decisiones estratégicas de alto nivel administrativo que conlleve a la ocurrencia de un fraude con pérdidas altamente significativas. La información estará libre de error y protegida contra fraude.

Clasificación por disponibilidad

Por disponibilidad, la información se clasifica bajo dos conceptos: retención y recuperación.

- Por Retención:

RTN1: No hay ningún requisito de retención; depende de las necesidades de cada usuario. Por ejemplo, archivos personales de trabajo.

RTN2: Información financiera sobre la cual se ha normalizado, por conveniencia, un período de retención particular.

RTN3: Información sobre la cual existen requisitos legales o contractuales especiales que exigen formas específicas de almacenamiento o duración de retención.

- Por Recuperación

RCP1: El tiempo de recuperación no es inmediato, tiene un margen de espera, por lo menos, una semana sin traer consecuencia alguna.

RCP2: El tiempo máximo de recuperación e inicio del procesamiento es menor a una semana.

RCP3: El tiempo máximo de recuperación e inicio del procesamiento es menor a un día.

Control de acceso

Todos los funcionarios del Gobierno Provincial de Tungurahua de acuerdo a su perfil de trabajo, tendrán una cuenta asociada a los servicios con los que cuenta la Entidad Provincial.

El personal que disponga de una cuenta institucional se sujetará obligatoriamente a las políticas de seguridad aplicables y vigentes dentro de la Entidad Provincial.

Todos los usuarios son absolutamente responsables de todas y cada una de las actividades desarrolladas y ejecutadas con su usuario y contraseña.
Los técnicos de la Dirección de Sistemas y Tecnología de la Información son los responsables de controlar y supervisar la asignación de cuentas de acceso, dicho procedimiento comprenderá el ciclo de vida de acceso al usuario, el cual consiste en registro inicial, uso y mantenimiento y cancelación final de acceso.

Control de acceso a las redes

El objetivo de este control es evitar el acceso no autorizado a la red Institucional.

El servicio de Internet suministrado por el Gobierno Provincial de Tungurahua es una herramienta de apoyo relacionada con el desarrollo de actividades relacionadas con su ámbito específico de trabajo y un medio por el cual ejecuten directamente sus funciones y responsabilidades.
El acceso a páginas web se restringe como medida de seguridad, conforme a los perfiles de usuario definidos por cada Director Departamental.

Se prohíbe la ejecución o cualquier intento de ejecución con fines ilícitos como accesos no autorizados, robo o daño de información, sobrecarga o deterioro de los servicios informáticos y red de la Institución.

Se prohíbe el acceso a sitios de pornografía, juegos o apuestas de cualquier tipo.
La Dirección de Sistemas es la unidad Dirección autorizada para limitar el acceso a determinadas páginas de Internet, los servicios ofrecidos por la red, la descarga de archivos y cualquier otro ajeno a los fines institucionales y a las funciones que desempeñan los funcionarios de las diferentes direcciones departamentales.

Protección de puertos de configuración

El acceso físico a los puertos de configuración y diagnóstico estará configurado previamente y restringido en los dispositivos asignados al personal.
La conexión lógica a los puertos de configuración y diagnóstico estará controlada con mecanismos de autenticación que permitan únicamente su acceso a los responsables de dichas actividades.

Control de acceso a las aplicaciones y a la información

El objetivo de este control es evitar el acceso no autorizado a la información del Gobierno Provincial de Tungurahua.
Restringir y limitar el acceso a la información por parte de los usuarios y del personal técnico de soporte conforme a la política definida de control de acceso.

Los permisos otorgados dentro de cada sistema son controlados por roles y perfiles de usuario que determinan los niveles de acceso de acuerdo con las funciones que desempeñan cada usuario, conforme a las políticas y roles de cada perfil.

Aislamiento de sistemas sensibles

Los sistemas de carácter sensible no operan en un entorno informático (servidor, bases de datos) compartido y estarán ubicados en un segmento de red especial para sistemas sensibles, protegido por un firewall y un sistema de detección de intrusos.

Controles criptográficos

Este control tiene como objetivo proteger la confidencialidad e integridad de la información.
La información que contenga contraseñas de usuario o claves para el control de acceso a los sistemas de información, no se almacenarán en texto plano.

Es responsabilidad de los administradores de los diferentes sistemas, definir algoritmos de encriptación para ser utilizados en los sistemas de información críticos con base a un análisis de riesgos y considerar los criterios de confidencialidad, integridad, autenticidad y no repudio.

Gestión de claves criptográficas

Las llaves o claves criptográficas se protegerán contra pérdida, modificación y destrucción no autorizadas por tanto resulta necesario definir criterios para almacenamiento de las claves, forma de acceso, cambio o actualización.

Revocar las claves si se han puesto en peligro o se retira un funcionario la Entidad Provincial.

Mantener un registro activo de auditorías de las actividades de gestión de llaves.

Protección contra código malicioso

Los sistemas de información, equipos móviles como equipos fijos de escritorio son vulnerables a código malicioso por ello, los usuarios asignados al personal de la Entidad no instalarán ni utilizarán software sin la debida autorización de la Dirección de Sistemas.

La Dirección de Sistemas contará permanentemente con software efectivo, así como con las herramientas de protección a nivel de red y de PC contra código malicioso.

Es responsabilidad de cada usuario o personal externo previo al uso de cualquier medio extraíble analizar con antivirus provisto por la Entidad.

Gestión de la seguridad de las redes

La protección de la información en las redes y la protección de infraestructura de soporte está a cargo del administrador de la red el cual aplicará todos los controles necesarios que garanticen seguridad de la red y los datos en tránsito. Toda conexión a la red contará con un mecanismo de autenticación que valide y autorice el ingreso de los usuarios.

La seguridad perimetral tendrá mecanismos de control que incluyan: Firewall, IPS, Filtro de contenido, Antivirus, Antispyware, Antispam.

Las conexiones de red se área extendida (WAN) estarán protegidas, controlar el tráfico de entrada y salida de red al utilizar software de filtrado de contenido. Implementación de controles de filtrado de contenido para evitar que los recursos de la Entidad Provincial sean utilizados para: visitar páginas no autorizadas que disminuyan la productividad de los funcionarios, comprometer la seguridad de los activos de información.

Mantener un constate monitoreo sobre la red interna, con la ayuda de herramientas que permitan detectar, prevenir y recuperarse contra código malicioso encontrado en su plataforma tecnológica.

Segregación de usuarios en redes

Las funciones y responsabilidades del personal de la Dirección de Sistemas y Tecnologías de la Información estarán bien definidas, para control y seguridad de la red, así como no permitir que ningún funcionario o personal externo tengan control sobre un sistema de información. Estas funciones son:
Administrador de red, Administrador de bases de datos, administrador de servidores y administrador de sistemas de información; responsables de la administración, monitoreo, controles, seguridad y buen funcionamiento de cada área específica de administración de la Entidad Provincial.

Seguridad de archivos del Sistema

Esta guía tiene como objetivo proteger la confidencialidad e integridad de la información a través de los siguientes controles:
Control de software operativo: verificar y someter a pruebas un posible impacto adverso con respecto a la seguridad en caso de cambios de sistemas operativos.

Cambios en paquetes de software: En el caso del uso o contratación de software externo a través de un proveedor, se establecerá las condiciones de cumplimiento mediante un contrato en el cual se establecerán lineamientos como riesgos, responsables técnicos, controles de seguridad y actualizaciones presentes o futuras.

Seguridad en los procesos de desarrollo

Esta guía define criterios y ambientes bajo los cuales trabaje el personal que realice mantenimiento de software, los roles que intervienen son los siguientes:

Desarrollador autorizado: descarga los programas fuente, y efectúa los cambios solicitados.

Dirección de Sistemas y Tecnologías de la Información: Revisa y autoriza mediante el responsable del área de desarrollo de software, los cambios sobre los programas fuente según los requerimientos aprobados.
Oficial de seguridad: Verifica el cumplimiento del procedimiento de control de cambios de software realizado, así como pruebas de estrés y controles de seguridad.

Respaldo de la información

Todos los activos de información se respaldarán obligatoriamente con una copia para proteger su información. El personal responsable de los activos de información establecerá los procedimientos adecuados para implementar un proceso de estrategia para el respaldo de la información más adecuado para cada activo, hacer copias de seguridad, probar sus tiempos de restauración e integridad.

Registro y Monitoreo

El registro de eventos es una de las herramientas más importantes de la administración de la seguridad. El registro de eventos estará permanentemente activo en todas las plataformas y sistemas de información del Gobierno Provincial de Tungurahua. Tener un equilibrio entre los eventos a registrar y el impacto en el desempeño de las plataformas en producción.

Registro de falla

Se registrarán todas las fallas de las plataformas de cómputo y comunicaciones con el fin de hacer un seguimiento a los problemas presentados, reducir su incidencia, prevenir su recurrencia y evitar alteraciones a la continuidad de las operaciones de la Entidad.

El administrador del sistema revisará los reportes de fallas identificadas en los registros de cada una de las plataformas de tecnología, en caso de encontrar un evento adverso y fuera de lo normal, se reportará inmediatamente al oficial de seguridad.

Fuga de información

Para limitar el riesgo de fuga de información se considerarán los siguientes aspectos:

- La información de salida contará con la marcación, clasificación de información y destinatarios definidos y solo estos tendrán acceso a la información.
- Explorar los medios y comunicaciones de salida para determinar la información oculta.
- Verificar el comportamiento de las comunicaciones y del sistema de modulación y enmascaramiento para reducir la probabilidad de que un tercero deduzca información a partir de tal comportamiento.
- Utilizar sistemas y software suficientemente probados.
- Monitorear periódicamente las actividades del personal clave de sistemas siempre que esté conforme a la normatividad vigente del Gobierno Provincial de Tungurahua.
- Monitorear periódicamente el uso de los recursos en los sistemas de información.

Planificación y aceptación del sistema

Gestión de la capacidad

Los técnicos de la Dirección de Sistemas son los responsables de revisar periódicamente la capacidad y el desempeño de los componentes tecnológicos. Todos los componentes críticos se revisarán periódicamente, reemplazo de partes, piezas o componentes y garantizar el correcto uso y buen funcionamiento de los equipos tecnológicos.

Esta información se registrará, por cada uno de los técnicos de la Dirección de Sistemas, en una bitácora.

Aceptación del sistema

Los cambios, actualizaciones, nuevas versiones o nuevo desarrollo de sistemas de Información cumplirán con un proceso formal y metodológico de aceptación por parte de la Dirección de Sistemas y de la Dirección de Planificación, por lo cual se considera como mínimo lo siguiente:

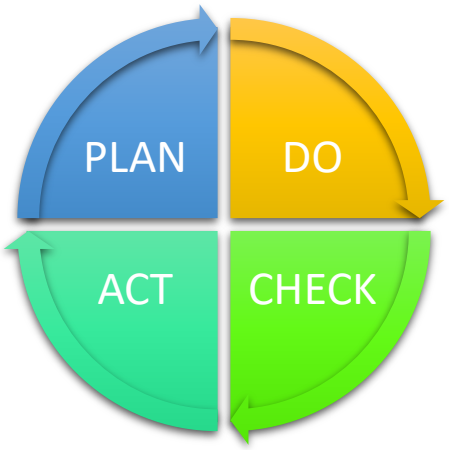
- Verificación de los niveles de desempeño de los servidores.
- Documentación de los cambios o actualizaciones realizadas.
- Análisis de riesgos y vulnerabilidades.
- Procedimientos para reinicio de los servicios.
- Entrenamiento en la operación del cambio.
- Consideración de los cambios en el plan de contingencias.

3.2. Evaluación y medición de desempeño del sistema de gestión de seguridad de la información.

Lo que no se monitorea no se mide, lo que no se mide no se controla, lo que no se controla no se mejora, lo que no se mejora no se gestiona, frase atribuida a (Thomson, 1824 - 1907).

Varias leyes, normas y reglamentos referentes a la seguridad de la información hacen referencia a la medición de desempeño; de esta forma resulta importante citar el ciclo Deming, llamado así por su creador Edward Deming el cual hace referencia a un ciclo de mejora continua (Quintero Parra, 2015).

Figura 33. Ciclo Deming



Fuente: tomado a partir de Recalde Caicedo (2019)

Se conoce que el Ciclo Deming consiste en un proceso de mejora continua: Plan: Planificar, Do: Hacer, Check: Controlar, Act: Actuar.

Todo este proceso se suma a la medición de un SGSI el cual entre sus objetivos tiene:

- Evaluar y llevar acabo un control de efectividad del SGSI.
- Evaluar la eficiencia presente y futura del SGSI.
- Monitorear el progreso y la mejora continua del SGSI.
- Documentar los resultados de todas las operaciones realizadas con respecto a los riesgos de la seguridad de la información.

El Gobierno Provincial de Tungurahua determinará:

- Establecer información cuantificable y documentada para la evaluación de desempeño de la seguridad de la información, así como niveles de eficiencia de gestión de la seguridad de la información.
- Establecer un método, que se adapte al Gobierno Provincial de Tungurahua que garantice resultados comparables para ser considerados como válidos.

- Los técnicos del departamento de Sistemas del Gobierno Provincial de Tungurahua se encargarán de llevar a cabo el seguimiento y medición, y socializarlo con el Comité de Seguridad de la Información.
- Los técnicos son los responsables de realizar un seguimiento y la medición y presentar los resultados obtenidos una vez al mes al Comité de Seguridad de la Información.
- La evaluación, medición y análisis de los resultados se los realizará de forma mensual, así como establecer los siguientes criterios:
- Cuantificación del rendimiento de seguridad a nivel del sistema de información para un sistema de información operativo.
- Cuantificar la integración de la seguridad de la información dentro del proceso de desarrollo de sistemas, software o sistemas de información.
- Cuantificar el rendimiento de la seguridad de la información en todo el Gobierno Provincial de Tungurahua.

Auditoría Interna

El Gobierno Provincial de Tungurahua llevará intervalos planificados para la realización de auditoría interna la cual tenga como objetivo brindar información sobre el SGSI.

Resulta muy necesario generar un procedimiento de auditoría interna con el fin de evitar incumplimientos a la Ley y cualquier requisito de seguridad relacionado con la Seguridad de la Información, y al ser una entidad pública sujeta a posibles auditorías externas de diferentes entidades de control.

Para llevar a cabo esta auditoría se contará con un documento matriz el cual establezca todas las actividades a llevar a cabo dentro del Gobierno Provincial de Tungurahua en función a una auditoría externa, utilizar como guía las Normas Técnicas Ecuatorianas NTE INEN ISO/IEC 27000 para la Gestión de Seguridad de la Información.

El Gobierno Provincial de Tungurahua establecerá los siguientes parámetros de cumplimiento obligatorio en el caso de una Auditoría Interna o Externa:

- Establecer un programa de auditoría que incluya: informes, planificación presente y futura, responsabilidades y la frecuencia con la cual se desarrollará dicha auditoría interna.
- Definir criterios y alcance de la auditoría.
- Asegurar el personal que desarrollará dicha auditoría de manera imparcial y objetiva.
- Informar a la alta gerencia (máxima autoridad) y Comité de Seguridad de la Información los resultados de la auditoría.
- Documentar la evidencia y resultados de la auditoría y conservar dicha documentación.

Revisión

Toda la documentación e información obtenida en las anteriores etapas se someterá a revisión de la alta gerencia (máxima autoridad) y sometida a aprobación del Comité de Seguridad de la Información.

La revisión de la documentación e información levantada tendrá las siguientes consideraciones:

- Análisis de resultados.
- Medidas o acciones a considerar.
- Información del comportamiento de seguridad de la información en el Gobierno Provincial de Tungurahua.
- Acciones necesarias correctivas presentes y futuras alineadas a una auditoría externa.
- Seguimiento de resultados.
- Cumplimiento de lineamientos y objetivos enfocados a la Seguridad de la Información del Gobierno Provincial de Tungurahua.
- Socialización, comentarios y mejora continua enfocado en la gestión de seguridad de la información.

Mejora continua

La mejora continua va de la mano con la conformidad, eficiencia y eficacia de las medidas empleadas en beneficio de la seguridad de la información del Gobierno Provincial de Tungurahua.

Cabe citar acciones para la eliminación de la no conformidad si por alguna razón hubiera algún tipo de inconformidad y que no quede ningún cabo suelto:

- Revisión y atención de la no conformidad.
- Causas que determinaron la no conformidad.
- Soluciones consensuadas de la no conformidad presente o futura o potencialmente recurrente, en base a acciones correctivas.
- De ser necesario realizar los cambios necesarios dentro del proceso de Gestión de Seguridad de la Información del Gobierno Provincial de Tungurahua.
- Y finalmente documentar cualquier tipo de acción correctiva presente o futura del proceso de Gestión de Seguridad de la Información del Gobierno Provincial de Tungurahua.

Medidas Candidatas

Dedicar suficiente tiempo a establecer medidas de desempeño de la seguridad de la información es fundamental para obtener el máximo valor de medir el desempeño de la seguridad de la información (Chew, y otros, 2008).

Medida 1: Presupuesto de Seguridad

CAMPO	DATOS
Identificador de medida	Presupuesto para seguridad 1
Meta	▪ Establecer un entorno de seguridad y responsabilidad para el personal e instalaciones del Gobierno Provincial de Tungurahua. ▪ Proporcionar los recursos necesarios enfocados en la seguridad de la información del Gobierno Provincial de Tungurahua.
Medida	Incorporar en el Plan Operativo Anual, así como en el Plan Anual de Contratación la asignación de recursos necesarios acorde al presupuesto establecido en el presente año fiscal, para cubrir las necesidades presentes y futuras enfocadas a la seguridad de la información.
Tipo de medida	Impacto alto, medio y bajo.
Objetivo	Cubrir necesidades presentes y futuras conforme a las necesidades propias de la Institución enfocadas en la seguridad de la información.
Implementación - Evidencia	1. ¿Cuál es el presupuesto total asignado a la seguridad de la información en el Gobierno Provincial de Tungurahua? 2. ¿Cuál es el presupuesto total de tecnologías de la información en el Gobierno Provincial de Tungurahua?
Frecuencia	La frecuencia de recopilación de datos se realizará anualmente. La frecuencia de recopilación de informes se realizará anualmente.
Responsable	▪ Propietario de la Información: Director de Sistemas y el Director Financiero del Gobierno Provincial de Tungurahua. ▪ Recopilador de información: Comité de Seguridad de la Información del Gobierno Provincial de Tungurahua. ▪ Cliente de información: Personal de la Dirección de Sistemas del Gobierno Provincial de Tungurahua.
Fuente	Guía de Seguridad de la Información, Esquema Gubernamental de Seguridad de la Información.
Informe	Gráficos que ilustren el presupuesto total asignado para la seguridad de la información e informe detallado emitido por el Comité de Seguridad de la Información.

Medida 2: Gestión de vulnerabilidades

CAMPO	DATOS
Identificador de medida	Medida de vulnerabilidad 1
Meta	▪ Establecer un entorno de seguridad y responsabilidad para el personal e instalaciones del Gobierno Provincial de Tungurahua. ▪ Asegurar la identificación y mitigación de las vulnerabilidades a las cuales está expuesto el Gobierno Provincial de Tungurahua.
Medida	Porcentaje de vulnerabilidades de mayor riesgo mitigadas dentro de un período determinado de tiempo definido por el Gobierno Provincial de Tungurahua.
Tipo de medida	Eficiencia / Eficacia
Objetivo	Llevar un control de mitigación de las vulnerabilidades de mayor riesgo para el Gobierno Provincial de Tungurahua. Llevar un control de mitigación de las vulnerabilidades de mediano y bajo riesgo para el Gobierno Provincial de Tungurahua.
Implementación - Evidencia	1. ¿Número de vulnerabilidades de mayor riesgo identificadas durante cada mes a lo largo de todo un año? 2. ¿Número de vulnerabilidades de mayor riesgo mitigadas dentro de este período de tiempo? 3. ¿Número de vulnerabilidades de mediano y bajo riesgo identificadas de forma bimensual a lo largo de todo un año? 4. ¿Número de vulnerabilidades de mediano y bajo riesgo dentro de este período de tiempo?
Frecuencia	La frecuencia de la recopilación de vulnerabilidades de mayor riesgo se realizará de forma mensual. La frecuencia de la recopilación de vulnerabilidades de mediano y bajo riesgo se realizará de forma bimensual.
Responsable	Propietario de la información: Director de Sistemas. Recopilador de información: Responsable de la Administración del Data Center del Gobierno Provincial de Tungurahua.
Fuente	Software de exploración de vulnerabilidades, registro de auditorías, sistema de gestión de vulnerabilidades, registro de gestión de cambios.
Informe	Reporte detallado de vulnerabilidades encontradas y propuestas de mitigación.

Medida 3: Control de accesos

CAMPO	DATOS
Identificador de medida	Medida de control de acceso remoto 1
Meta	Establecer un entorno de seguridad y responsabilidad para el personal e instalaciones del Gobierno Provincial de Tungurahua. Restringir el acceso a la información, a los sistemas a personas o equipos desconocidos, no autorizados.
Medida	Porcentaje de puntos de acceso remoto utilizados para obtener acceso no autorizado.
Tipo de medida	Eficacia / Eficiencia
Objetivo	Llevar un control de puntos de acceso remoto no autorizados o desconocidos.
Implementación - Evidencia	¿Utiliza el Gobierno Provincial de Tungurahua herramientas automatizadas para mantener un diagrama de red actualizado que identifique todos los puntos de acceso remoto? SÍ NO ¿Cuántos puntos de acceso remoto existen en el Gobierno Provincial de Tungurahua? ¿El Gobierno Provincial de Tungurahua emplea Sistemas de Detección de Intrusos (IDS) para monitorear el tráfico que atraviesa los puntos de acceso remoto? SÍ NO ¿El Gobierno Provincial de Tungurahua recopila y realiza un registro de los puntos de acceso remoto? ¿El Gobierno Provincial de Tungurahua mantiene una base de datos de incidentes de seguridad que identifica categorías de incidentes estandarizados por cada incidente?
Frecuencia	Frecuencia de recopilación mensual. Frecuencia de informes bimensual.
Responsable	Propietario de la información: Administrador de la red institucional. Recopilador de información: Administrador del Data Center institucional.
Fuente	Base de datos de incidentes, diagramas de red, registros y alertas IDS.
Informe	Reporte con gráficos que ilustran los puntos de acceso remoto utilizados para accesos no autorizados, frente al total de puntos de acceso remoto existentes en el Gobierno Provincial de Tungurahua.

Medida 4: Concientización y Capacitación

CAMPO	DATOS
Identificador de medida	Medida de capacitación en seguridad 1
Meta	▪ Establecer un entorno de seguridad y responsabilidad para el personal e instalaciones del Gobierno Provincial de Tungurahua. ▪ Asegurarse de que el personal del Gobierno Provincial de Tungurahua esté adecuadamente capacitado para llevar a cabo sus funciones y responsabilidades relacionadas con la seguridad de la información.
Medida	Porcentaje del personal del Gobierno Provincial de Tungurahua que recibió capacitación en seguridad de la información.
Tipo de medida	Implementación
Objetivo	Llevar un programa de capacitación integral en temas de seguridad de la información a todo el personal del Gobierno Provincial de Tungurahua.
Implementación - Evidencia	1. ¿Definición de responsabilidades de seguridad con criterios de calificación? 2. ¿Se mantienen registros de qué empleados tienen responsabilidades significativas de seguridad? 3. ¿Cantidad de empleados con responsabilidad significativa en seguridad de la información? 4. ¿Se cuenta con planes de capacitación, sobre todo con personal con responsabilidades significativas de seguridad? 5. ¿Se mantienen registros de capacitaciones en temas de seguridad de la información?
Frecuencia	Frecuencia de recopilación: mensual. Frecuencia de infirmes: mensual.
Responsable	Propietario de la información: Personal de Sistemas del Gobierno Provincial de Tungurahua. Recopilador de información: Personal de empleados del Gobierno Provincial de Tungurahua.
Fuente	Registros de asistentes y participantes en capacitación.
Informe	Reporte con gráficos y porcentajes de registros del personal que ha recibido la capacitación, frente al personal que no ha recibido la capacitación.

Medida 5: Auditoría y Rendición de Cuentas

CAMPO	DATOS
Identificador de medida	Registro de Auditoría 1
Meta	▪ Establecer un entorno de seguridad y responsabilidad para el personal e instalaciones del Gobierno Provincial de Tungurahua. ▪ Crear, proteger y conservar los registros de auditoría del sistema de información que permita realizar un seguimiento, análisis, investigación y notificación de actividades no autorizadas con respecto a la seguridad de la información.
Medida	Frecuencia de revisión y análisis de registros de auditorías de control enfocadas en seguridad de la información.
Tipo de medida	Eficacia / Eficiencia
Objetivo	Establecer un alto grado de control de revisión, análisis y medidas adoptadas enfocadas a presentes o futuras auditorías internas o externas a los sistemas de información.
Implementación - Evidencia	1. ¿Tiene el Gobierno Provincial de Tungurahua criterios claramente definidos sobre evidenciar actividades inapropiadas dentro de los registros de auditoría? 2. ¿Cuál es el período de tiempo que el Gobierno Provincial de Tungurahua define entre una auditoría y otra, después de establecer las correcciones y correctivos resultantes?
Frecuencia	Frecuencia de recopilación: Semanal Frecuencia de infirmes: Bimensual.
Responsable	▪ Propietario de la información: Director de Sistemas. ▪ Recopilador de información: Administrador de la red y Data Center del Gobierno Provincial de Tungurahua.
Fuente	Informes de registros de auditoría.
Informe	Reporte con gráficos y porcentajes de la cantidad de sistemas auditados, novedades y observaciones realizadas.

Medida 6: Planificación de Contingencia

CAMPO	DATOS
Identificador de medida	Medida de Pla de Contingencia
Meta	Establecer un entorno de seguridad y responsabilidad para el personal e instalaciones del Gobierno Provincial de Tungurahua. Implementar de manera efectiva planes de contingencia y respuestas a emergencias, respaldo y recuperación ante posibles desastres de los sistemas de información del Gobierno Provincial de Tungurahua, para garantizar la disponibilidad de la información y la continuidad de las operaciones ante posibles situaciones de emergencia.
Medida	Porcentaje de Sistemas de información, que se han realizado con pruebas semestrales o anuales de planes de contingencia.
Tipo de medida	Eficacia / Eficiencia
Objetivo	Establecer un plan de contingencia enfocado no solo en la parte operativa de los sistemas de información, también enfocado en la seguridad de la información del Gobierno Provincial de Tungurahua.
Implementación - Evidencia	¿Con cuántos Sistemas de Información cuenta el Gobierno Provincial de Tungurahua y se dispone de algún tipo de inventario? ¿El Gobierno Provincial de Tungurahua cuenta con planes de contingencia? ¿Cuántos planes de contingencia fueron elaborados y aprobados el último año?
Frecuencia	Frecuencia de recopilación: anual. Frecuencia de informes: anual.
Responsable	Propietario de la información: Director de Sistemas Recopilador de información: Personal de la Dirección de Sistemas del Gobierno Provincial de Tungurahua, Comité de Seguridad.
Fuente	Resultados de las pruebas del Plan de Contingencia.
Informe	Reporte con gráficos y porcentajes de las pruebas realizadas de los planes de contingencia frente a los porcentajes de las pruebas no realizadas de planes de contingencia en los sistemas de información del Gobierno Provincial de Tungurahua.

Medida 7: Identificación y Autenticación

CAMPO	DATOS
Identificador de medida	Identificación – Autenticación 1
Meta	▪ Establecer un entorno de seguridad y responsabilidad para el personal e instalaciones del Gobierno Provincial de Tungurahua. ▪ Todos los usuarios están identificados y autenticados de acuerdo con la Política de Seguridad de la Información del Gobierno Provincial de Tungurahua.
Medida	Porcentaje de usuarios con acceso a cuentas propias y compartidas.
Tipo de medida	Eficacia / Eficiencia
Objetivo	Establecer medidas de control e identificación a los usuarios basados en una política de seguridad de la información.
Implementación - Evidencia	1. ¿Cuál es el número de usuarios con accesos a los diferentes sistemas del Gobierno Provincial de Tungurahua? 2. ¿Cuántos usuarios tienen acceso a cuentas compartidas del Gobierno Provincial de Tungurahua?
Frecuencia	Frecuencia de recopilación: mensual. Frecuencia de informes: mensual.
Responsable	Propietario de la información: Director de Sistemas. Recopilador de información: Administrador de Sistemas.
Fuente	Base de datos de usuarios, listas de control de accesos, listas de Identificación de usuarios.
Informe	Reportes con gráficos y porcentajes de usuarios con acceso y cuentas autorizadas de acceso frente a usuarios sin acceso ni cuentas autorizadas.

Medida 8: Respuestas a Incidentes

CAMPO	DATOS
Identificador de medida	Medida de respuesta a incidentes 1
Meta	▪ Establecer un entorno de seguridad y responsabilidad para el personal e instalaciones del Gobierno Provincial de Tungurahua. ▪ Documentar y reportar incidentes de los funcionarios del Gobierno Provincial de Tungurahua.
Medida	Porcentaje de incidentes los cuales han sido reportados dentro de un marco de tiempo asignado como reporte aplicable por la Dirección de Sistemas del Gobierno Provincial de Tungurahua.
Tipo de medida	Eficacia / Eficiencia
Objetivo	Establecer un registro de rastreo y reporte de incidentes los cuales se atenderán en el menor tiempo posible por la Dirección de Sistemas del Gobierno Provincial de Tungurahua.
Implementación - Evidencia	1. ¿Cuántos incidentes se reportaron en el primer trimestre del año? Categoría 1: Acceso no autorizado Categoría 2: Denegación de servicio Categoría 3: Código Malicioso Categoría 4: Intentos de acceso indebido 2. De los incidentes informados, ¿Cuántos se informaron dentro del plazo establecido como categoría de incidente?
Frecuencia	Frecuencia de recopilación: mensual Frecuencia de informes: semestral
Responsable	Propietario de la información: responsable del área de infraestructura de la Dirección de Sistemas. Recopilación de información: Administrador de TI, Administrador de red y Data Center del Gobierno Provincial de Tungurahua.
Fuente	Registro de incidentes, base de datos de registro de incidentes.
Informe	Reporte con gráficos de reportes atendidos realizados por el personal del Gobierno Provincial de Tungurahua frente a reportes no atendidos.

Medida 9: Mantenimiento

CAMPO	DATOS
Identificador de medida	Medida de mantenimiento 1
Meta	▪ Establecer un entorno de seguridad y responsabilidad para el personal e instalaciones del Gobierno Provincial de Tungurahua. ▪ Establecer un cronograma de mantenimientos periódico de los sistemas de información del Gobierno Provincial de Tungurahua y proporcionar controles efectivos sobre los sistemas, herramientas, técnicas y mecanismos utilizados para realizar el mantenimiento de los sistemas de información.
Medida	Porcentaje de componentes de los sistemas que han sido sometidos a mantenimiento conforme a la actividades planificadas y no planificadas establecidas por el Gobierno Provincial de Tungurahua.
Tipo de medida	Eficacia / Eficiencia
Objetivo	Establecer un adecuado número de mantenimientos correctivos y preventivos que permitan al personal del Gobierno Provincial de Tungurahua realizar un trabajo acorde a sus funciones y responsabilidades.
Implementación - Evidencia	1. ¿Cuenta el Gobierno Provincial de Tungurahua con un sistema programado de mantenimientos periódicos? 2. ¿Existe un registro de mantenimientos de acuerdo a un cronograma establecido por la Dirección de Sistemas del Gobierno Provincial de Tungurahua?
Frecuencia	Frecuencia de recopilación: trimestral. Frecuencia de informes: semestral.
Responsable	Propietario de la información: Personal responsable de la infraestructura del Gobierno Provincial de Tungurahua. Recopilador de información: Administrador de TI, Comité de Seguridad de la Información del Gobierno Provincial de Tungurahua.
Fuente	Registros de mantenimiento, programas de mantenimientos.
Informe	Reporte con gráficos de porcentajes de equipos y sistemas que han recibido mantenimiento preventivo y correctivo, frente a equipos y sistemas que no han recibido mantenimiento.

Medida 10: Evaluación de Riesgos

CAMPO	DATOS
Identificador de medida	Medida de evaluación de riesgos 1
Meta	▪ Establecer un entorno de seguridad y responsabilidad para el personal e instalaciones del Gobierno Provincial de Tungurahua. ▪ Evaluación periódica de riesgos de seguridad de la información de los activos del Gobierno Provincial de Tungurahua.
Medida	Porcentaje de vulnerabilidades encontradas y correctivos aplicados en un determinado lapso de tiempo.
Tipo de medida	Eficacia / Eficiencia
Objetivo	Evaluar periódicamente los riesgos relacionados con la seguridad de la información en base a un cronograma previamente establecido por los funcionarios de la Dirección de Sistemas del Gobierno Provincial de Tungurahua.
Implementación - Evidencia	1. ¿El Gobierno Provincial de Tungurahua realiza escaneo o exploración de vulnerabilidades de los sistemas con los que cuenta? SI NO 2. ¿Cuál es la periodicidad de los escaneos o exploraciones de vulnerabilidades? Semanal Mensual Trimestral Semestral Anual 3. ¿El Gobierno Provincial de Tungurahua documenta las vulnerabilidades encontradas? SI NO 4. ¿Cuáles son las vulnerabilidades más comunes y de mayor o menor riesgos encontradas?
Frecuencia	Frecuencia de recopilación: mensual Frecuencia de informes: mensual
Responsable	Propietario de la información: Administrador del Data Center e Infraestructura del Gobierno Provincial de Tungurahua. Recopilador de la información: Administrador de Sistemas y Comité de Seguridad de la Información.
Fuente	Informe de escaneo de vulnerabilidades
Informe	Gráfico con porcentajes de vulnerabilidades mitigadas frente a vulnerabilidades no mitigadas.

Medida 11: Integridad de la Información

CAMPO	DATOS
Identificador de medida	Medida de Integridad de la Información 1
Meta	▪ Establecer un entorno de seguridad y responsabilidad para el personal e instalaciones del Gobierno Provincial de Tungurahua. ▪ Establecer parámetros de protección contra códigos maliciosos en los sistemas de información del Gobierno Provincial de Tungurahua, control de alertas y avisos de seguridad y medidas de respuesta.
Medida	Porcentaje de vulnerabilidades mitigadas, parches de seguridad y medidas empleadas de mitigación y control.
Tipo de medida	Implementación Eficacia y Eficiencia
Objetivo	Establecer medidas de respuesta frente a alertas de código malicioso y cualquier otra medida que atente contra la seguridad de la Información del Gobierno Provincial de Tungurahua.
Implementación - Evidencia	1. ¿El Gobierno Provincial de Tungurahua cuenta con medidas de alerta y aviso frente a amenazas de código malicioso? 2. ¿Cuántas vulnerabilidades se identificaron mediante un análisis de vulnerabilidades? 3. ¿Cuántas soluciones se implementaron para mitigar posibles vulnerabilidades? 4. ¿Cuántas soluciones se aplicaron, pero no surtieron efecto con la implementación de parches o medidas de seguridad?
Frecuencia	Frecuencia de recopilación: semanal. Frecuencia de informes: mensual.
Responsable	Propietario de la información: Personal responsable de incidentes relacionados con la seguridad de la información. Recopilador de información: Administrador de Sistemas, Data Center y Monitoreo de Red de la Institución.
Fuente	Informe de exploración de vulnerabilidades, repositorio de alertas y avisos, evaluación de riesgos.
Informe	Gráfico con porcentajes del número total de vulnerabilidades encontradas, mitigadas y solventadas, frente a vulnerabilidades encontradas no mitigadas ni solventadas.

3.3. Aplicación de dominios, controles y documentación

A continuación, se muestra una matriz la cual contiene 14 dominios de controles de seguridad, 35 categorías (objetivos de control) principales de seguridad y 114 controles, la que se usará como referencia al seleccionar controles, levantar información y documentar el proceso que permita definir la Guía de Seguridad de la Información para el Gobierno Provincial de Tungurahua, conforme lo establece el Esquema Gubernamental de Seguridad de la Información basado en ISO/IEC 27001 y de esta forma demostrar su valía y ponerla en práctica por parte de la Institución.

Cuadro de aplicabilidad - EGSI V2.0

Ítem	Sección	Descripción	Estado actual del Control (Implementado, Parcialmente Implementado, Por Implementar)	Aplica Si/No	Justificación de la selección (Si) o de la exclusión (No) (Resultados, evaluación, análisis)	Observaciones
	1	**Políticas de Seguridad de la Información**				
	1.1	**Dirección de gestión de seguridad de la información**				
1	1.1.1	Políticas de Seguridad de la Información				
2	1.1.2	Revisión de las políticas para la seguridad de la información				
	2	**Organización de la Seguridad de la Información**				
	2.1	**Organización interna**				
3	2.1.1	Compromiso de la máxima autoridad de la institución con la seguridad de la información				
4	2.1.2	Separación de funciones				
5	2.1.3	Contacto con las autoridades				
6	2.1.4	Contacto con los grupos de interés especial				
7	2.1.5	Seguridad de la Información en la gestión de proyectos				
8	2.1.6	Consideraciones de la seguridad si se trata con ciudadanos o clientes				
	2.2	**Dispositivos móviles y teletrabajo**				
9	2.2.1	Política de dispositivos móviles				
10	2.2.2	Teletrabajo				
	3	**Seguridad de los recursos humanos**				
	3.1	**Antes del empleo**				
11	3.1.1	Investigación de antecedentes				
12	3.1.2	Términos y condiciones laborales				
	3.2	Durante el empleo				
13	3.2.1	Responsabilidades de la Máxima Autoridad o su delegado				
14	3.2.2	Concienciación, educación y formación en seguridad de la información				

15	3.2.3	Proceso disciplinario				
	3.3	Finalización o cambio de empleo				
16	3.3.1	Responsabilidades ante la finalización o cambio de empleo				
	4	**Gestión de activos**				
	4.1	Responsabilidad de los activos				
17	4.1.1	Inventario de activos				
18	4.1.2	Propiedad de los activos				
19	4.1.3	Uso aceptable de los activos				
20	4.1.4	Devolución de activos				
	4.2	Clasificación de la información				
21	4.2.1	Directrices de Clasificación de la información				
22	4.2.2	Etiquetado de la información				
23	4.2.3	Manejo de los activos				
	4.3	Manejo de los Soportes de almacenamiento - medios				
24	4.3.1	Gestión de medios extraíbles				
25	4.3.2	Eliminación de los medios				
26	4.3.3	Transferencia de medios físicos				
	5	**Control de acceso**				
	5.1	Requisitos institucionales para el control de acceso				
27	5.1.1	Política de control de acceso				
28	5.1.2	Acceso a redes y servicios de red				
	5.2	Gestión de acceso de los usuarios				
29	5.2.1	Registro y retiro de usuarios				
30	5.2.2	Provisión de accesos a usuarios				
31	5.2.3	Gestión de los derechos de acceso con privilegios especiales				
32	5.2.4	Gestión de la información confidencial de autenticación de los usuarios				
33	5.2.5	Revisión de los derechos de acceso de usuario				
34	5.2.6	Retiro o adaptación de los derechos de acceso				
	5.3	Responsabilidades del usuario				
35	5.3.1	Uso de la información confidencial para la autenticación				
	5.4	Control de acceso a sistemas y aplicaciones				
36	5.4.1	Restricción del acceso a la información				
37	5.4.2	Procedimientos seguros de inicio de sesión				
38	5.4.3	Sistema de gestión de contraseñas				
39	5.4.4	Uso de herramientas de administración de sistemas				
40	5.4.5	Control de acceso al código fuente del programa				
	6	**Criptografía**				
	6.1	Controles criptográficos				
41	6.1.1	Política de uso de los controles criptográficos				
42	6.1.2	Gestión de Claves				
	7	**Seguridad física y del entorno**				
	7.1	Áreas seguras				
43	7.1.1	Perímetro de seguridad física				

44	7.1.2	Controles físicos de entrada				
45	7.1.3	Seguridad de oficinas, despachos e instalaciones				
46	7.1.4	Protección contra las amenazas externas y ambientales				
47	7.1.5	Trabajo en áreas seguras				
48	7.1.6	Áreas de carga y entrega				
	7.2	Seguridad de los Equipos				
49	7.2.1	Ubicación y protección de equipos				
50	7.2.2	Instalaciones de suministro				
51	7.2.3	Seguridad del cableado				
52	7.2.4	Mantenimiento de los equipos				
53	7.2.5	Salida de los activos fuera de las instalaciones de la institución				
54	7.2.6	Seguridad de los equipos y activos fuera de las instalaciones				
55	7.2.7	Seguridad en la reutilización o eliminación segura de dispositivos de almacenamiento				
56	7.2.8	Equipo informático de usuario desatendido				
57	7.2.9	Política de puesto de trabajo despejado y pantalla limpia				
	8	**Seguridad de las operaciones**				
	8.1	Procedimientos y responsabilidades operacionales				
58	8.1.1	Documentación de procedimientos de operación				
59	8.1.2	Gestión de cambios				
60	8.1.3	Gestión de capacidades				
61	8.1.4	Separación de ambientes de desarrollo, pruebas y producción				
	8.2	Protección contra un malware				
62	8.2.1	Controles contra malware				
	8.3	Copias de seguridad				
63	8.3.1	Copias de seguridad de la información				
	8.4	Registro y monitoreo				
64	8.4.1	Registro de eventos				
65	8.4.2	Protección de los registros de información				
66	8.4.3	Registros de administración y operación				
67	8.4.4	Sincronización de relojes				
	8.5	Control del software en producción				
68	8.5.1	Instalación del software en sistemas en producción				
	8.6	Gestión de la vulnerabilidad técnica				
69	8.6.1	Gestión de las vulnerabilidades técnicas				
70	8.6.2	Restricciones en la instalación de software				
	8.7	Consideraciones sobre la auditoría de sistemas de información				
71	8.7.1	Controles de auditoría de sistemas de información				
	9	**Seguridad en las comunicaciones**				
	9.1	Gestión de la seguridad de redes				
72	9.1.1	Controles de red				
73	9.1.2	Seguridad de los servicios de red				
74	9.1.3	Separación en las redes				

	9.2	Transferencia de información				
75	9.2.1	Políticas y procedimientos de transferencia de información				
76	9.2.2	Acuerdos de transferencia de información				
77	9.2.3	Mensajería electrónica				
78	9.2.4	Acuerdos de confidencialidad o no revelación				
	10	**Adquisición, desarrollo y mantenimiento de los sistemas**				
	10.1	Requisitos de seguridad de los sistemas de información				
79	10.1.1	Análisis de requisitos y especificaciones de seguridad de la información				
80	10.1.2	Asegurar los servicios de aplicaciones en redes públicas				
81	10.1.3	Controles de transacciones en línea				
	10.2	Seguridad en el desarrollo y en los procesos de soporte				
82	10.2.1	Política de desarrollo seguro				
83	10.2.2	Procedimientos de control de cambios en sistemas				
84	10.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo				
85	10.2.4	Restricciones a los cambios en los paquetes de software				
86	10.2.5	Principios de ingeniería de sistemas seguros				
87	10.2.6	Ambiente de desarrollo seguro				
88	10.2.7	Desarrollo externalizado				
89	10.2.8	Pruebas de seguridad del sistema				
90	10.2.9	Pruebas de aceptación de sistemas				
	10.3	Datos de prueba				
91	10.3.1	Protección de los datos de prueba				
	11	**Relaciones con proveedores**				
	11.1	Seguridad de la información en relación con los proveedores				
92	11.1.1	Política de seguridad de la información en las relaciones con los proveedores				
93	11.1.2	Requisitos de seguridad en contratos con terceros				
94	11.1.3	Cadena de suministro de tecnologías de la información y de las comunicaciones				
	11.2	Gestión de la provisión de servicios del proveedor				
95	11.2.1	Monitoreo y revisión de los servicios de proveedores				
96	11.2.2	Gestión de cambios en los servicios de proveedores				
	12	**Gestión de incidentes de seguridad de la información**				
	12.1	Gestión de los incidentes de seguridad de la información y mejoras				
97	12.1.1	Responsabilidades y procedimientos				
98	12.1.2	Reporte de los eventos de seguridad de la información				
99	12.1.3	Reporte de debilidades de seguridad de la información				
100	12.1.4	Apreciación y decisión sobre los eventos de seguridad de la información				
101	12.1.5	Respuesta a incidentes de seguridad de la información				
102	12.1.6	Aprendizaje de los incidentes de seguridad de la información				
103	12.1.7	Recopilación de evidencias				
	13	**Aspectos de seguridad de la información para la gestión de la continuidad del negocio**				

	13.1	Continuidad de seguridad de la información				
104	13.1.1	Planificación de la continuidad de seguridad de la información				
105	13.1.2	Implementación de la continuidad de seguridad de la información				
106	13.1.3	Verificar, revisar y evaluar la continuidad de seguridad de la información				
	13.2	Redundancias				
107	13.2.1	Disponibilidad de las instalaciones de procesamiento de la información				
	14	**Cumplimiento**				
	14.1	Cumplimiento de los requisitos legales y contractuales				
108	14.1.1	Identificación de la legislación aplicable y de los requisitos contractuales				
109	14.1.2	Derechos de propiedad intelectual				
110	14.1.3	Protección de los registros				
111	14.1.4	Protección y privacidad de la información de carácter personal				
112	14.1.5	Reglamentos de controles criptográficos				
	14.2	Revisiones de seguridad de la información				
113	14.2.1	Revisión independiente de seguridad de la información				
114	14.2.2	Cumplimiento de las políticas y normas de seguridad				
115	14.2.3	Comprobación del cumplimiento técnico				

LEYENDA	
COLOR	**DESCRIPCIÓN**
	Dominio
	Objetivo de control
	Control de seguridad

CONCLUSIONES

- El análisis de la situación actual de seguridad de la información realizado en el Gobierno Provincial de Tungurahua evidenció la falta de una metodología para el tratamiento de riesgos asociados a la seguridad de la información, así como la falta de lineamentos que permitan brindar mediante una Guía de Seguridad de la Información, seguridad a los activos de alta dependencia para la Institución.

- La identificación de los activos del Gobierno Provincial de Tungurahua que representan mayor riesgo y un alto grado de criticidad con respecto a la seguridad de la información son el servidor Nutanix y el servidor NAS (Network Attached Storage) Synology del Data Center principal, en los cuales se encuentra más del 90% de información institucional, incluidos respaldos y sistemas de uso interno, de la misma forma los activos de interconexión de red constan también como activos de alto riesgo con respecto a acceso a la información dentro de la Institución Provincial. Activos en los que se fija la atención debida para garantizar la seguridad y protección de la información.

- La definición del alcance del Esquema Gubernamental de Seguridad de la Información en base a la realidad actual del Gobierno Provincial de Tungurahua, el mismo que es aplicable a los activos de mayor dependencia y por ende de mayor criticidad para la Institución, con proyección al desarrollo de una política integral que abarque aristas personalizadas que ponderen grados de criticidad y riesgo de un activo. Con la implementación de una guía y políticas de seguridad de la información, el Gobierno Provincial de Tungurahua cumplirá con los lineamientos definidos de acuerdo al Acuerdo Ministerial Nro. 025-2019 emitido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información.

RECOMENDACIONES

- El compromiso de la Máxima Autoridad y Directores Departamentales resulta fundamental a la hora de la implementación y cumplimiento de la Guía de Seguridad de la Información, se recomienda establecer y definir en el Gobierno Provincial de Tungurahua la implementación de un Comité de Seguridad de la Información, el cual estará a cargo de llevar un control y seguimiento adecuado de la guía y cumplimiento de Políticas de Seguridad de la Información en la Institución.

- Se recomienda la designación de un Técnico de la Dirección de Sistemas, el cual es el responsable específicamente de la Seguridad de la Información que asuma un rol determinante en el uso y actualización continua de políticas y guías de Seguridad de la Información.

- Se recomienda realizar una revisión continua de las políticas y guías de Seguridad de la Información, con el fin de mantener información actualizada conforme exista cambio de normativa, crecimiento a nivel de planta y equipos, así como crecimiento a nivel de software y proyectos de desarrollo internos. Con una revisión continua y actualizada no solamente se garantiza resultados a nivel institucional, sino que permitirá que la Guía sirva como referencia para establecer futuras guías en los diferentes Gobiernos Autónomos Descentralizados, en base a una realidad y necesidad específica de cada GAD.

BIBLIOGRAFÍA

Abreu, J. L. (2014). *El método de la investigación Research Method. Daena: International Journal of Good Conscience, 9(3), 195-204.* (artículo científico): International Journal of Good Conscience.

Abril, A., Pulido, J., & Bohada, J. (2013). Análisis de Riesgos en Seguridad de la Información. *Revista Ciencia, Innovación y Tecnología (RCIYT)* | *Vol. 1*.

Aldaz Calispa, N. I. (2021). *Propuesta de un plan de contingencia para salvaguardar los activos de información en el Departamento de tecnología de información y comunicación de la Empresa Pública Municipal de residuos sólidos Rumiñahui-Aseo EPM empleando la metodología Magerit.* (tesis): Universidad Politécnica Salesiana.

Aldaz Calispa, N. I., & Pazmiño Sanchez, F. P. (2021). *Propuesta de un plan de contingencia para salvaguardar los activos de información en el Departamento de tecnología de información y comunicación de la Empresa Pública Municipal de residuos sólidos Rumiñahui-Aseo EPM empleando la metodología Magerit.* Quito - Ecuador: Universidad Politécnica Salesiana.

Amutio Gómez, M. A., Candau, J., & Mañas, J. A. (2012). *MAGERIT version 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de*

Información Libro I Método. Madrid - España: Ministerio de Hacienda y Administraciones Públicas.

Amutio Gómez, M. A., Candau, J., & Mañas, J. A. (2012). *MAGERIT-version 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método.* Madrid: Ministerio de Hacienda y Administraciones Públicas.

Amutio Gómez, M. A., Candau, J., & Mañas, J. A. (2012). *MAGERIT-version 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II - Catálogo de Elementos.* Madrid - España: Ministerio de Hacienda y Administraciones Públicas.

Amutio Gómez, M. A., Candau, J., & Mañas, J. A. (2012). *MAGERIT-version 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III - Guía de Técnicas.* Madrid - España: Ministerio de Hacienda y Administraciones Públicas.

Ávila, G. (2018). *Elaboración de una política de seguridad de la información para una institución pública basado en el esquema gubernamental de seguridad de la información.* Quito - Ecuador: Universidad Internacional SEK.

Baldecchi, R. (2014). *Implementación efectiva de un SGSI ISO 27001.* Santiago - Chile: ISACA.

BBC News Mundo. (16 de septiembre de 2019). *www.bbc.com*. Obtenido de https://www.bbc.com/mundo/noticias-america-latina-49721456

Castro & Bayona, Z. O. (2011). *Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios.* Universidad Distrital Francisco José de Caldas.

Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A., & Robinson, W. (2008). *Performance Measurement Guide for Information Security.* United States of America: National Institute of Standards and Technology.

Comunicación, I. N. (2018). *Implantación de un SGSI en la empresa .*

Dirección Nacional de Interoperabilidad Seguridad de la Información e Infraestructura. (2020). *Guía para la Gestión de Riesgos de Seguridad de la Información.* Subsecretaría de Estado-Gobierno Electrónico.

Enríquez, L. (31 de agosto de 2022). *Hacia una cultura de "Valor al Riesgo" en la ciberseguridad del Ecuador.* Obtenido de htt p s : //w ww. uas b.e du. ec/ciberderechos/2022/08/31/hacia-una-cultura-de-valor-al-riesgo-en-la-ciberseguridad-del-ecuador/

Esquema Gubernamental de Seguridad de la Información EGSI.pdf. (2020). *Esquema Gubernamental de Seguridad de la Información -EGSI-.* Quito: Registro Oficial Corte Constitucional del Ecuador.

Frayssinet, D. M. (2014). *Taller de Implementación de la norma ISO 27001.* Lima - Perú.

Gaibor, M. O. (2008). Propuesta de Políticas de Seguridad de la Información para la Escuela Politécnica Nacional. *Tesis de Investigación*.

Gallardo, Á. M. (2018). *Elaboración de una política de seguridad de la información para una institución pública basado en el esquema gubernamental de seguridad de la información.* Quito - Ecuador: Universidad Internacional SEK.

Gobierno Provincial de Tungurahua. (2022). *https://www.tungurahua.gob.ec/*. Obtenido de https://www.tungurahua.gob.ec/

Gomez, A. M. (2012). *MAGERIT-version 3.0 Metodología de analisis y gestión de riesgos de los sistemas de información Libro I-Metodo. MA Amutio Gomez, MAGERIT-version, 3.* (tesis maestría): Ministerio de Hacienda y Administraciones Públicas.

Gomez, A. M. (2012). *MAGERIT-version 3.0 Metodología de analisis y gestión de riesgos de los sistemas de información Libro I-Metodo. MA Amutio Gomez, MAGERIT-version, 3.* (tesis maestría): Ministerio de Hacienda y Administraciones Públicas.

Gomez, A. M. (2012). *MAGERIT-version 3.0 Metodología de analisis y gestión de riesgos de los sistemas de información Libro I-Metodo. MA Amutio Gomez, MAGERIT-version, 3.* (tesis maestría): Ministerio de Hacienda y Administraciones Públicas.

Gómez, E. F. (2019). *Plan de contingencia para los equipos y sistemas informáticos utilizando la metodología MAGERIT.* (artículo científico): Revista Científica y Tecnológica UPSE, 6(1), 34-41.

Gómez, E., Duchimaza, J., Holguín, J., & Lindao, M. (2019). *Plan de contingencia para los equipos y sistemas informáticos utilizando la metodología MAGERIT.* artículo científico: Revista Científica y Tecnológica UPSE, 6(1), 34-41.

INFORMACIÓN, M. D. (2020). *Esquema Gubernamental de Seguridad de la Información (EGSI).* Registro Oficial - Corte Constitucional del Ecuador.

Instituto Nacional de Ciberseguridad. (2017). *INCIBE.* Obtenido de Glosario de términos de Ciberseguridad: https://www.incibe.es/

Kowask Bezerra, E., Alcántara Lima, F., Cesar Motta, A., & Boca Piccolini, J. (2014). *Gestión del riesgo de las TI NTC 27005.* Bogota D.C. - Colombia : Universidad Nacional de Colombia - CEDIA.

Mahecha, G. M., & Coello, F. G. (2016). Desarrollo de un sistema de información para gestionar la implantación, mantenimiento y mejora contínua de un sistema de gestión de seguridad de la infirmación basado en la norma ISO 27001:2013. *Tesis de investigación*.

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2020). *Esquema Gubernamental de Seguridad de la Información (EGSI).* Quito - Ecuador: Registro Oficial - Corte Constitucional del Ecuador.

Molina, M. J., & Sánchez, S. Y. (2019). *Análisis de la participación de las medianas empresas de la ciudad de León en operaciones bursátiles de la bolsa de valores de Nicaragua, en el período comprendido diciembre 2018 a junio 2019.* (tesis): Universidad Nacional Autónoma de Nicaragua.

Montalbán, E., Gómez, R., & Borré, D. (2020). *Diseño de un sistema de gestión de seguridad de la información para el proceso administrativo de la infraestructura tecnológica de instituciones académicas basado en Magerit.* (artículo científico): Aglala, 11(1), 227-245.

Ortiz, C. L. (24 de enero de 2022). *www.revistas.udec.cl.* Obtenido de https://revistas.udec.cl/index.php/gyap/article/view/5949

Patiño, G. S. (2018). *Propuesta metodológica de gestión de riesgos de Tecnología de información y comunicación (TIC) para entidades públicas*

conforme normativa NTE INEN ISO/IEC 27005. Quito - Ecuador: Universidad de las Fuerzas Armadas.

PMG-SSI. (2022). *Seguridad de la Información*. Obtenido de Blog especializado en Seguridad de la Información y Ciberseguridad: https://www.pmg-ssi.com/2017/01/iso-27005-como-identificar-los-riesgos/

Quintero Parra, L. (2015). Diseño de un sistema de gestión de seguridad de la información (sgsi) para el departamento de informática de la Superintendencia de Notariado y Registro.

Ramírez, C. E., & Rinconc, P. M. (2022). La importancia de la seguridad de la información en el sector público en Colombia. *Revista Ibérica de Sistemas y Tecnologías de Información*.

Recalde Caicedo, J. P. (2019). *Plan de implementación de un SGSI y aplicación de controles críticos en el centro de operaciones de seguridad en la empresa GMS.* Quito.

Solarte, S. F., Enriquez, R. E., & Benavides, R. M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica ESPOL - RTE* .

Thomson, W. (1824 - 1907). *Físico y Matemático Británico.* Netherhall

ANEXOS

ANEXO 1. Solicitud de Autorización

Honorable Gobierno Provincial de Tungurahua

Bolívar 491 y Castillo esquina
(03) 375 0220
Casilla: 18-01-320
gobierno.provincial@tungurahua.gob.ec

Ambato, 24 de enero de 2022

Ingeniero
Galo Xavier Robayo Laz
DIRECTOR GENERAL PROVINCIAL DE LA DIRECCIÓN DE SISTEMAS
GOBIERNO PROVINCIAL DE TUNGURAHUA
Presente

De mi consideración:

Por medio del presente solicito cordialmente autorización para desarrollar un proyecto de investigación y desarrollo previo a la obtención del título de Magister en Ciberseguridad en la Pontificia Universidad Católica del Ecuador Sede Ambato, el cual consiste en una Guía de Gestión de Seguridad de la Información para el Gobierno Provincial de Tungurahua.

Cabe recalcar que para el desarrollo del proyecto es necesario contar con la información adecuada y la colaboración del personal de la Dirección a su cargo, lo cual permitirá la culminación del mismo y servirá como un aporte importante para la Institución.

Sin otro particular y seguro de contar con su valiosa ayuda y autorización para el desarrollo del proyecto, anticipo mis agradecimientos.

Atentamente,

VICTOR FELIX BARREZUETA

Ing. Víctor Félix Barrezueta
CI. 1803838851

Tungurahua
para el Ecuador y el mundo

www.tungurahua.gob.ec

ANEXO 2. Entrevista

NOMBRES Y APELLIDOS: Ing. Galo Xavier Robayo Laz.

CARGO: DIRECTOR DE SISTEMAS DEL GOBIERNO PROVINCIAL DE TUNGURAHUA

PREGUNTAS	SI	NO	DESCONOCE	OBSERVACIÓN
¿Actualmente la Dirección de Sistemas del Gobierno Provincial de Tungurahua, cuenta con una Guía que Gestione la Seguridad de la Información?		X		
¿En los últimos dos años se ha realizado algún tipo de análisis o gestión de riesgos de seguridad de la información?		X		
¿Existen roles definidos para el control y acceso al Data Center del Gobierno Provincial de Tungurahua?		X		
¿Existe un plan de emergencia que permita recuperar las funciones de los sistemas en el caso de un ataque crítico al servidor principal del Data Center?		X		
¿Están definidos los roles y responsables de la seguridad de la información dentro de la Dirección de Sistemas?	X			Existen roles con respecto a funciones, sin embargo ningún rol está orientado específicamente a la seguridad de la información.
¿Se cuenta con procedimientos para manipulación de activos del Data Center?		X		
¿Cuál es el activo o activos que considera de vital importancia del Data Center?	X			Dentro del Data Center se encuentran activos como el SERVIDOR NUTANIX en el cual se levanta 27 servidores virtuales, los que administran todos los servicios que brinda la Institución, de igual forma el SERVIDOR NAS que guarda gran parte de información de

				documentación digital de toda la Institución, en el caso de falla en el servidor se ha implementado una solución de hiperconvergencia, por lo cual considero que el SERVIDOR NUTANIX es de suma importancia para la Institución.
¿Se toma las medidas adecuadas en el caso de cambio de personal a cargo de la administración y seguridad del Data Center?	X			Se planifica con la debida anticipación el cambio de personal ya sea por permiso, vacaciones o cambio de autoridades.
¿Existe algún sistema de alerta en el caso de sobrecalentamiento o incendio en el Data Center?	X			Existe un sistema de alerta a los dispositivos móviles de todo el personal de la Dirección de Sistemas, que notifica inmediatamente en el caso de sobrecalentamiento o incendio en el Data Center.
¿Se realizan pruebas de evaluación y mantenimiento al Data Center?		X		
¿Se ha realizado alguna auditoría interna o externa en los últimos dos años con fines de medir el grado de cumplimiento legal y normativa internacional referente a la Gestión de Seguridad de la Información?		X		

AGRADEZCO SU COLABORACIÓN Y TIEMPO BRINDADO

ANEXO 3. ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN

Mediante Acuerdo Ministerial Nro. 025-2019 con fecha 10 de enero de 2020 se publica en el Registro Oficial el Esquema Gubernamental de Seguridad de la Información (EGSI V2.0).

Artículo 1.- Expedir el Esquema Gubernamental de Seguridad de la Información -EGSI-, el cual es de implementación obligatoria en las Instituciones de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva, que se encuentra como Anexo al presente Acuerdo Ministerial.

Artículo 2.- Las Instituciones de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva, realizarán la Evaluación de Riesgos sobre sus activos de información críticos y diseñarán el plan para el tratamiento de los riesgos de su Institución, utilizán como referencia la “GUÍA PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN” que es parte del Anexo del presente Acuerdo Ministerial, previo a la actualización o implementación de los controles de seguridad.

Artículo 3.- Recomendar a las Instituciones de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva, utilicen como guía las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información.

Artículo 4.- Las Instituciones de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva, actualizarán o implementarán el Esquema Gubernamental de Seguridad de la Información EGSI en un plazo de doce (12) meses contados a partir de la publicación del presente Acuerdo Ministerial en el Registro Oficial.

La Evaluación de Riesgos y el plan para el tratamiento de los riesgos de cada Institución se realizarán en un plazo de cinco (5) meses y la actualización o implementación de los controles del Esquema Gubernamental de Seguridad de la Información (EGSI) se realizará en un plazo de siete (7) meses.

La actualización o implementación, se realizará en cada institución de acuerdo al ámbito de acción, estructura orgánica, recursos y nivel de madurez en gestión de Seguridad de la Información.

Artículo 5.- La máxima autoridad designará al interior de su Institución, un Comité de Seguridad de la Información (CSI), que estará integrado por los responsables de las siguientes áreas o quienes hagan sus veces: Talento Humano, Administrativa, Planificación y Gestión Estratégica, Comunicación Social, Tecnologías de la Información, Unidades Agregadores de Valor y el Área Jurídica participará como asesor.

El Comité de Seguridad de la Información tiene como objetivo, garantizar y facilitar la implementación de las iniciativas de seguridad de la información en la institución.

Los Comités en la primera convocatoria definirán su agenda y su reglamento interno.

Artículo 6.- El Comité de Seguridad de la Información, tendrá las siguientes responsabilidades:

a) Gestionar la aprobación de la política y normas institucionales en materia de seguridad de la información, por parte de la máxima autoridad de la Institución.
b) Realizar el seguimiento de los cambios significativos de los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
c) Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad de la información, con nivel de impacto alto.
d) Coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios, en base al EGSI.
e) Promover la difusión de la seguridad de la información dentro de la institución.
f) Coordinar el proceso de gestión de la continuidad de la operación de los servicios y sistemas de información de la institución frente a incidentes de seguridad imprevistos.
g) El comité convocará bimensualmente o si las circunstancias así lo ameritan, se llevará registros y actas de las reuniones.
h) Informar a la máxima autoridad los avances de la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI).

i) Reportar a la máxima autoridad las alertas que impidan la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI).
j) Recomendar a la máxima autoridad mecanismos que viabilicen la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI).

Artículo 7.- El Comité de Seguridad de la Información (CSI) designará al interior de su Institución a un funcionario como Oficial de Seguridad de la Información (OSI).

El Oficial de Seguridad tendrá conocimiento en Seguridad de la Información y Gestión de Proyectos, es el responsable de la Unidad de Seguridad de la Información, se recomienda que no pertenezca al área de Tecnologías de la Información.

Artículo 8.- El Oficial de Seguridad de la Información tendrá las siguientes responsabilidades:

a) Identificar todas las personas o instituciones públicas o privadas, que de alguna forma influyen o impactan en la implementación del EGSI.
b) Generar propuestas para la elaboración de la documentación esencial del Esquema Gubernamental de Seguridad de la Información (EGSI).
c) Asesorar a los funcionarios en la ejecución del Estudio de Gestión de Riesgos de Seguridad de la Información en las diferentes áreas.
d) Elaborar el Plan de concienciación en Seguridad de la Información basado en el Esquema Gubernamental de Seguridad de la Información (EGSI).
e) Elaborar un plan de seguimiento y control de la implementación de las medidas de mejora o acciones correctivas.
f) Coordinar la elaboración del Plan de Continuidad de Seguridad de la Información.
g) Orientar y generar un procedimiento adecuado para el manejo de los incidentes de seguridad de la información presentados al interior de la institución.
h) Coordinar la gestión de incidentes de seguridad con nivel de impacto alto a través de otras instituciones gubernamentales.

i) Mantener la documentación de la implementación del EGSI debidamente organizada.
j) Verificar el cumplimiento de las normas, procedimientos y controles de seguridad institucionales establecidos.
k) Informar al Comité de Seguridad de la Información, el avance de la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI), así como las alertas que impidan su implementación.
l) Previa la terminación de sus funciones el Oficial de Seguridad realizará la transferencia de la documentación e información de la que fue responsable al nuevo Oficial de Seguridad, en caso de ausencia, el Comité de Seguridad de la Información. (Esquema Gubernamental de Seguridad de la Información EGSI.pdf, 2020)

ANEXO 4. CATÁLOGO DE AMENAZAS / VULNERABILIDADES

EJEMPLOS DE VULNERABILIDADES EN DIVERSAS ÁREAS DE SEGURIDAD / EJEMPLOS DE AMENAZAS QUE EXPLOTARÍAN ESTAS VULNERABILIDADES		
Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de esquemas de reemplazo periódico.	Destrucción de equipos o de medios.
	Susceptibilidad a la humedad, el polvo y la suciedad.	Polvo, corrosión, congelamiento
	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	Ausencia de un eficiente control de cambios en la configuración	Error en el uso
	Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía
	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
	Almacenamiento sin protección	Hurto de medios o documentos
	Falta de cuidado en la disposición final	Hurto de medios o documentos
	Copia no controlada	Hurto de medios o documentos
Software	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos
	Defectos bien conocidos en el software	Abuso de los derechos
	Ausencia de "terminación de la sesión" al abandonar la estación de trabajo	Abuso de los derechos
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de los derechos
	Ausencia de pistas de auditoria	Abuso de los derechos
	Asignación errada de los derechos de acceso	Abuso de los derechos
	Software ampliamente distribuido	Corrupción de datos
	En términos de tiempo utilización de datos errados en los programas de aplicación	Corrupción de datos
	Interfaz de usuario compleja	Error en el uso
	Ausencia de documentación	Error en el uso
	Configuración incorrecta de parámetros	Error en el uso
	Fechas incorrectas	Error en el uso
	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos
	Tablas de contraseñas sin protección	Falsificación de derechos
	Gestión deficiente de las contraseñas	Falsificación de derechos
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
	Software nuevo o inmaduro	Mal funcionamiento del software
	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software
	Ausencia de control de cambios eficaz	Mal funcionamiento del software
	Descarga y uso no controlado de software	Manipulación con software
	Ausencia de copias de respaldo	Manipulación con software
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de medios o documentos
	Falla en la producción de informes de gestión	Uso no autorizado del equipo
Red	Ausencia de pruebas de envío o recepción de mensajes	Negación de acciones
	Líneas de comunicación sin protección	Escucha encubierta
	Tráfico sensible sin protección	Escucha encubierta
	Conexión deficiente de los cables.	Falla del equipo de telecomunicaciones
	Punto único de falla	Falla del equipo de telecomunicaciones
	Ausencia de identificación y autentificación de emisor y receptor	Falsificación de derechos
	Arquitectura insegura de la red	Espionaje remoto
	Transferencia de contraseñas en claro	Espionaje remoto
	Gestión inadecuada de la red (Tolerancia a fallas en el	Saturación del sistema de

	enrutamiento)	información
	Conexiones de red pública sin protección	Uso no autorizado del equipo
Personal	Ausencia del personal	Incumplimiento en la disponibilidad del personal
	Procedimientos inadecuados de contratación	Destrucción de equipos o medios
	Entrenamiento insuficiente en seguridad	Error en el uso
	Uso incorrecto de software y hardware	Error en el uso
	Falta de conciencia acerca de la seguridad	Error en el uso
	Ausencia de mecanismos de monitoreo	Procesamiento ilegal de los datos
	Trabajo no supervisado del personal externo o de limpieza	Hurto de medios o documentos
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo
Lugar	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Destrucción de equipo o medios
	Ubicación en un área susceptible de inundación	Inundación
	Red energética inestable	Pérdida del suministro de energía
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de equipo
Organización	Ausencia de procedimiento formal para el registro y retiro de usuarios	Abuso de los derechos
	Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso	Abuso de los derechos
	Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con los clientes y/o terceras partes	Abuso de los derechos
	Ausencia de procedimiento de monitoreo de los recursos de procesamiento de información	Abuso de los derechos
	Ausencia de auditorías (supervisiones) regulares	Abuso de los derechos
	Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de los derechos
	Ausencia de reportes de fallas en los registros de administradores y operadores	Abuso de los derechos
	Respuesta inadecuada de mantenimiento del servicio	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de acuerdos de niveles del servicio, o insuficiencia.	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimiento de control de cambios	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimiento formal para el control de la documentación del SGSI	Corrupción de datos
	Ausencia de procedimiento formal para la supervisión del registro del SGSI	Corrupción de datos
	Ausencia de procedimiento formal para la autorización de la información disponible al público	Datos provenientes de fuentes no confiables
	Ausencia de asignación adecuada de responsabilidades en la seguridad de la información	Negación de acciones
	Ausencia de planes de continuidad	Falla del equipo
	Ausencia de políticas sobre el uso del correo electrónico	Error en el uso
	Ausencia de procedimientos para la introducción del software en los sistemas operativos	Error en el uso
	Ausencia de registros en las bitácoras (logs) de administrador y operario.	Error en el uso
	Ausencia de procedimientos para el manejo de información clasificada	Error en el uso
	Ausencia de responsabilidades en la seguridad de la información en la descripción de los cargos	Error en el uso

	Ausencia o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados	Procesamiento ilegal de datos
	Ausencia de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información	Hurto de equipo
	Ausencia de política formal sobre la utilización de computadores portátiles	Hurto de equipo
	Ausencia de control de los activos, que se encuentran fuera de las instalaciones	Hurto de equipo
	Ausencia o insuficiencia de política sobre limpieza de escritorio y de pantalla	Hurto de medios o documentos
	Ausencia de autorización de los recursos de procesamiento de la información	Hurto de medios o documentos
	Ausencia de mecanismos de monitoreo establecidos para las brechas en la seguridad	Hurto de medios o documentos
	Ausencia de revisiones regulares por parte de la gerencia	Uso no autorizado del equipo
	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad	Uso no autorizado del equipo
	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	Uso de software falso o copiado

Fuente: NTE INEN-ISO/IEC 27005:2012

ANEXO 5. CATÁLOGO DE AMENAZAS HUMANAS

FUENTES DE AMENAZAS HUMANAS		
Fuente de Amenaza	Motivación	Acciones Amenazantes
Pirata informático, intruso ilegal	Reto Ego Rebelión Estatus Dinero	Piratería
		Ingeniería social
		Intrusión, accesos forzados al sistema
		Acceso no autorizado al sistema
Criminal de la computación	Destrucción de información Divulgación ilegal de información Ganancia monetaria Alteración no autorizada de los datos	Crimen por computador (por ejemplo, espionaje cibernético)
		Acto fraudulento (por ejemplo, repetición, personificación, interceptación)
		Soborno de la información
		Suplantación de identidad
		Intrusión en el sistema
Terrorismo	Chantaje Destrucción Explotación Venganza Ganancia política Cubrimiento de los medios de comunicación	Bomba/terrorismo
		Guerra de la información (warfare)
		Ataques contra el sistema (por ejemplo, negación distribuida del servicio)
		Penetración en el sistema
		Manipulación del sistema
Espionaje industrial (Inteligencia, empresas, gobiernos extranjeros, otros intereses gubernamentales)	Ventaja competitiva Espionaje económico	Ventaja de defensa
		Ventaja Política
		Explotación económica
		Hurto de información
		Intrusión en la privacidad personal
		Ingeniería social
		Penetración en el sistema
		Acceso no autorizado al sistema (acceso a información clasificada, de propiedad y/o relacionada con la tecnología)
Intrusos (empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Curiosidad Ego Inteligencia Ganancia monetaria Venganza Errores y omisiones no intencionales (por ejemplo, error en el ingreso de los datos, error de programación)	Asalto a un empleado
		Chantaje
		Observar información reservada
		Uso inadecuado del computador
		Fraude y hurto
		Soborno de información
		Ingreso de datos falsos o corruptos
		Interceptación
		Código malicioso (por ejemplo, virus, bomba lógica, troyano)
		Venta de información personal
		Errores en el sistema (bugs)
		Intrusión al sistema
		Sabotaje del sistema
		Acceso no autorizado al sistema

Fuente: NTE INEN-ISO/IEC 27005:2012

ANEXO 6. CATÁLOGO DE AMENAZAS COMUNES

EJEMPLOS DE AMENAZAS COMUNES		
Tipo	Amenaza	Origen
Daño Físico	Fuego	A, D, E
	Daño por agua	A, D, E
	Contaminación	A, D, E
	Accidente importante	A, D, E
	Destrucción del equipo o los medios	A, D, E
	Polvo, corrosión, congelamiento	A, D, E
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
	Fenómenos volcánicos	E
	Fenómenos meteorológicos	E
	Inundación	E
Pérdida de los servicios esenciales	Falla en el sistema de suministro de agua o de aire acondicionado	A, D
	Pérdida de suministro de energía	A, D, E
	Falla en el equipo de telecomunicaciones	A, D
Perturbación debida a la radiación	Radiación electromagnética	A, D, E
	Radiación térmica	A, D, E
	Impulsos electromagnéticos	A, D, E
Compromiso de la información	Interceptación de señales de interferencia comprometedoras	D
	Espionaje remoto	D
	Escucha encubierta	D
	Hurto de medios o documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	A, D
	Datos provenientes de fuentes no confiables	A, D
	Manipulación con hardware	D
	Manipulación con software	A, D
	Detección de la posición	D
Fallas técnicas	Falla del equipo	A
	Mal funcionamiento del equipo	A
	Saturación del sistema de información	A, D
	Mal funcionamiento del software	A
	Incumplimiento en el mantenimiento del sistema de información	A, D
Acciones no autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta del software	D
	Uso de software falso o copiado	A, D
	Corrupción de los datos	D
	Procesamiento ilegal de los datos	D
Compromiso de las funciones	Error en el uso	A
	Abuso de derechos	A, D
	Falsificación de derechos	D
	Negación de acciones	D
	Incumplimiento en la disponibilidad del personal	A, D, E

Fuente: NTE INEN-ISO/IEC 27005:2012

Leyenda	
A - accidentales	para las acciones humanas que dañan accidentalmente los activos de información
D - deliberadas	para todas las acciones deliberadas que tienen como objetivo los activos de la información
E - ambientales	para todos los incidentes que no se basa en las acciones humanas