Conciencia Digital

ISSN: **2600-5859**
Vol. 6 No. 4.2, pp. 28 – 45, noviembre 2023

www.concienciadigital.org

Guía rápida de un Sistema de Gestión de Seguridad de la Información para una ISP: Caso de estudio XNET

Quick Guide to an Information Security Management System for an ISP: XNET Case Study.

[1] Pablo Cesar Gordillo Chabla https://orcid.org/0009-0005-3636-1785
Maestría en Ciberseguridad, Universidad Católica de Cuenca, Cuenca, Ecuador.
pcgordilloch@ucacue.edu.ec

[2] Juan Pablo Cuenca Tapia https://orcid.org/0000-0001-5982-634X
Docente investigador, Universidad Católica de Cuenca, Cuenca, Ecuador
jcuenca@ucacue.edu.ec

[3] Eduardo Mauricio Campaña Ortega https://orcid.org/0000-0001-7720-5213
Docente investigador, Universidad Católica de Cuenca, Cuenca, Ecuador
eduardo.campana@ucacue.edu.ec

Artículo de Investigación Científica y Tecnológica
Enviado: 10/08/2023
Revisado: 17/09/2023
Aceptado: 02/10/2023
Publicado: 03/11/2023
DOI: **https://doi.org/10.33262/concienciadigital.v6i4.2.2751**

Cítese: Gordillo Chabla, P. C., Cuenca Tapia, J. P., & Campaña Ortega, E. M. (2023). Guía rápida de un Sistema de Gestión de Seguridad de la Información para una ISP: Caso de estudio XNET. *ConcienciaDigital*, 6(4.2), 28-45. https://doi.org/10.33262/concienciadigital.v6i4.2.2751

CONCIENCIA DIGITAL, *es* una revista multidisciplinar, t**rimestral,** que se publicará en soporte electrónico tiene como **misión** contribuir a la formación de profesionales competentes con visión humanística y crítica que sean capaces de exponer sus resultados investigativos y científicos en la misma medida que se promueva mediante su intervención cambios positivos en la sociedad. https://concienciadigital.org
La revista es editada por la Editorial Ciencia Digital (Editorial de prestigio registrada en la Cámara Ecuatoriana de Libro con No de Afiliación 663) www.celibro.org.ec

Conciencia Digital

ISSN: **2600-5859**
Vol. 6 No. 4.2, pp. 28 – 45, noviembre 2023

www.concienciadigital.org

Palabras claves:
Seguridad de la información, confidencialidad, integridad, disponibilidad, ISO 27001, Magerit.

Resumen

Introducción: Los usuarios de computadoras ya sean individuos o pertenecientes al sector público o privado, tienen expectativas informales respecto a sus equipos. Esperan que al encender la computadora se guarden los datos que dejaron el día anterior, que sus correos electrónicos lleguen a sus destinatarios sin pérdida de archivos adjuntos, y que, al acceder a la base de datos de nómina, los datos sean reales y coherentes. Sin embargo, estas expectativas no siempre se cumplen debido a posibles fallas de hardware, interceptación de correos electrónicos o manipulación de aplicaciones de nómina por parte de empleados desleales. **Objetivo:** El objetivo de este proyecto es crear una guía rápida para un sistema de gestión de la seguridad de la información, basado en MAGERIT y las normas ISO/IEC 27000, con el fin de analizar las vulnerabilidades. **Metodología:** Se llevó a cabo una investigación en fuentes confiables en línea para seleccionar los artículos de investigación, tesis y proyectos que fueron relevantes para este proyecto. Se realizó un análisis cualitativo y cuantitativo de cada uno de los activos de la información, así como una investigación descriptiva y bibliográfica de las amenazas encontradas. El objetivo fue identificar las mejores prácticas y controles necesarios para evitar que dichas amenazas se materialicen. **Resultados:** El resultado fue la implementación de un sistema de gestión de la seguridad de la información que permite eliminar o minimizar la probabilidad e impacto de los incidentes de seguridad. Se utilizaron las metodologías de riesgo MAGERIT y las normas ISO/IEC 27000. **Conclusión:** En conclusión, se presenta una guía rápida para un Sistema de Gestión de Seguridad de la Información para un ISP. Sin embargo, es importante tener en cuenta que cada ISP es único y las conclusiones específicas pueden variar según el contexto. **Área de estudio general:** Tecnologías de la Información. **Área de estudio específica:** Ciberseguridad.

Keywords:
Information security, confidentiality, integrity, availability, ISO 27001, Magerit.

Abstract

Introduction: Computer users, whether individuals or belonging to the public or private sector, have informal expectations of their computers. They expect that when they turn on the computer, the data they left the day before will be saved, that their emails will reach their recipients without loss of attachments, and that when they access the payroll database, the data will be real and

ISSN: **2600-5859**
Vol. 6 No. 4.2, pp. 28 – 45, noviembre 2023

consistent. However, these expectations are not always met due to possible hardware failures, email interception, or manipulation of payroll applications by dishonest employees. **Objective:** The objective of this project is to create a quick guide for an information security management system, based on MAGERIT and the ISO/IEC 27000 standards, in order to analyze vulnerabilities. **Methodology:** Research was carried out in reliable online sources to select the research articles, theses, and projects that were relevant to this project. A qualitative and quantitative analysis of each of the information assets was carried out, as well as a descriptive and bibliographic research of the threats found. The objective was to identify the best practices and controls necessary to prevent these threats from materializing. **Results:** The result was the implementation of an information security management system that allows to eliminate or minimize the probability and impact of security incidents. The MAGERIT risk methodologies and ISO/IEC 27000 standards were used. **Conclusion:** In conclusion, a quick guide is presented for an Information Security Management System for an ISP. However, it is important to note that each ISP is unique and the specific conclusions may vary depending on the context.

Introducción

En la actualidad la empresa XNET, posee una cartera aproximada de 1.000 clientes y que para su normal funcionamiento es necesario de un Presidente Ejecutivo, un Gerente General, dos Cajeras, una Contadora y tres Técnicos, donde su principal objetivo es el de brindar servicios de conexión a internet, inspirado en la idea de llegar a más hogares por medio de su red GPON y radio enlaces, con equipos de gama alta y con una red que han sido diseñado respetando protocolos de calidad, con el fin de brindar un servicio de internet estable y confiable.

Si bien es cierto que los ciberataques en la última década, venían teniendo un incremento significativo, en cuanto se refiere a Phishing, Malware y Ransomware específicamente, no obstante, con la llegada del Covid-19, en donde la Organización Mundial de la Salud, reconoció como pandemia el 11 de marzo de 2020 y según afirman Parra & Cabrera (2020), que en el Ecuador se reportaron los primeros casos, el 29 de febrero de 2020.

Tejena (2018), mencionan que las empresas tanto públicas como privadas enfrentan amenazas internas y externas que pueden conducir al robo de identidades e información, bases de datos y datos confidenciales de los clientes (p. 4), y con la implementación del teletrabajo, y, ante el incremento del 19,5% de consumo de internet en el mundo, han obligado a los ISPs a asumir nuevos desafíos para identificar necesidades y condiciones que garanticen la protección contra ciberataques y otras amenazas a los que están expuestos, según ESET (2021), en sus reportes realizados en Latinoamérica y las comparaciones del primero con el último trimestre, se pude evidenciar que existe un incremento del 704% en cuanto a detección de ataques de fuerza fruta y un incremento de 196% en intentos de comprometer accesos remotos.

Peralta & Aguilar (2021), afirma que en el Ecuador el 43% de la población, tienen acceso al internet, siendo la principal entrada para los ciberdelincuentes, al estar conectados a la información que se encuentra en el ciberespacio, además tomando en cuenta que Núñez & Carhuancho (2020), afirman que la ciberdelincuencia evolucionara según la cantidad de usuarios vaya en aumento y por otra parte Avila & Cuenca (2021), mencionan que empresas creen que están protegidas por dispositivos, aplicaciones y políticas de seguridad, pero en realidad la mayoría de los técnicos TIC no son expertos en ciberseguridad por lo que recomiendan que las empresas consideren contratar profesionales en ciberseguridad.

Por tal razón, la necesidad de crear la presente guía rápida de gestión de la seguridad de la información, en donde nos enfocáremos en valorar el entorno digital e infraestructura tecnológica, realizar una evaluación a cada uno de los riesgos, como también. definir las diferentes aplicaciones de control que sean necesarias para poder eliminar o minimizar la probabilidad y/o impacto causado por los diferentes incidentes de la seguridad de la información, que puedan ocurrir dentro de la empresa, haciendo uso de las siguientes metodologías de riesgo como es: MAGERIT, la norma ISO/IEC 27001 y la norma ISO/IEC 27002.

ISO/IEC 27000

Argüezo (2019), en su estructura de tesis describe a la familia de las normas ISO 27000, como un conjunto de normas globales e internacionales sobre la seguridad de la información, además contiene un conjunto de buenas prácticas para el establecimiento, implementación, mantenimiento y mejora de los sistemas de gestión de seguridad de la información, contiene la jerga en la que se basan el resto de normas. Es como una ayuda o referencia que describe los términos y directrices de todas las normas de la familia, del mismo modo, los principales pilares de la familia 27000 son las normas ISO/IEC 27001 y la norma ISO/IEC 27002, en donde su principal distinción entre las dos normas es de que la norma ISO/IEC 27001 según Bailón (2019), esta fue creada para certificar las medidas adecuadas para para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI, mientras que la norma ISO/IEC 27002, Caiza & Bolaños (2014), hacen referencia que un código de buenas prácticas que describe una serie del controles son perseguidos por la organización.

MAGERIT

Ortiz (2019), menciona que MAGERIT, es la metodología española que es promovida por el Ministerio de Administraciones Públicas de España y desarrollada por el Consejo Superior de Administración Electrónica (CSAE), que se utiliza para gestionar y analizar riesgos en sistemas de información. Esta metodología consta de tres libros: "Método", "Catálogo de elementos" y "Guía de técnicas", que sirven como referencia para la revisión de definiciones y la estimación de riesgos, y que Molina (2017), listan las siguientes fases: 1.-Caracterización de los activos: identificación, clasificación, dependencias y valoración. 2.- Caracterización de las amenazas y 3.- Evaluación de las salvaguardas.

Metodología

Se realizó una investigación de fuentes confiables, en diferentes repositorios dentro de la web, con el fin de optar entre los diferentes artículos de investigación, tesis y proyectos que más se asemejen y sean de utilidad para el presente proyecto, en donde se realizó análisis cualitativo y cuantitativo a cada uno de los activos de la información, como también una investigación descriptiva, aplicada y bibliográfica de cada una de las

amenazas encontradas, con el fin de encontrar las mejores prácticas y controles necesarios y así evitar que la misma se materialice, para esto se aplicó las siguientes fases:

Fase 1.- Aprobación de la dirección o gerencia para iniciar el proyecto. Como primer paso y el más importante, se consiguió la aprobación por parte de gerencia, ya que sin la semejante no se podía dar inicio con el presente proyecto, no obstante, se recalca que deberá existir, el respaldo y apoyo siempre y en todo momento por parte de gerencia.

Fase 2: Recopilación de la Información de la empresa. en esta fase se conoció a fondo la empresa, ya sea por medio de visitas, entrevistas y así tener un panorama claro sobre lo activos que se va a evaluar (Lema & Cuenca, 2020).

Fase 3: Revisar de la metodología MAGERIT y la norma ISO/IEC 27000. En esta fase se estudió como analizar y mitigar el riesgo.

Fase 4: Análisis FODA (Fortaleza, Oportunidades, Debilidades, Amenaza) de la empresa, con visión a seguridad de información.

Fase 5: Identificación de los activos críticos de la información. Dentro de la metodología MAGERIT, los activos son divididos en diferentes grupos dependiendo de la función que ejercen durante el tratamiento de la información, pudiendo estas ser: Información, Software, Físicos, Servicios, Personal. Según lo estipula el libro 2 de Magerit del 2012.

Fase 6: Valoración de los Activos. Una vez identificados cuales son los activos de la empresa, se procedió a realizar una valoración de los mismos, de acuerdo a 4 dimensiones (Argüezo, 2019).

Fase 7: Determinación de las Amenazas. En esta sección se identificaron todas las amenazas posibles, que puedan dañar de alguna manera nuestros activos informáticos de la empresa, donde se realizó una valoración de acuerdo a la frecuencia o degradación del activo (Argüezo, 2019).

Fase 8: Estimación del impacto. Para realizar este punto se hizo referencia entre los valores de los activos y las amenazas a las que se expone esto se logró realizando un

cálculo tanto para el activo como para la amenaza, pudiendo ser estos valores: 3 alto, 2 medio, 1 bajo y 0 sin impacto (Argüezo, 2019).

Fase 9: Cálculos del riesgo. Para realizar este cálculo, se realizó una multiplicación de la amenaza por el impacto. Según lo estipula el libro 3 de Magerit del 2012.

Fase 10: Identificación de Salvaguardas. Son medidas de protección que se presentan, con el fin de que la amenazas no causen tanto daño. Según lo estipula el libro 2 de Magerit del 2012.

Fase 11: -Diseñar la Guía Rápida del SGSI. Esta fase comprende en documentar los requisitos necesarios que se encuentran contemplados en la familia de las normas ISO/IEC 27000 y MAGERET, para luego posterior detallar las mediciones, supervisiones, análisis y evaluaciones del sistema, a través de los indicadores.

Resultados

Haciendo uso de la metodología Magerit y la norma ISO/IEC 27000, se identificaron las partes interesadas. Posteriormente realizó un análisis FODA a la empresa XNET, para conocer su situación actual (Loja & Cuenca, 2020) (Tabla 1).

Tabla 1

Análisis DAFO

Fortalezas	Debilidades
Cuenta con un servidor para almacenamiento de datos Cuenta con un servidor espejo del servidor principal.	No existe restricción a los usuarios para el acceso a los datos. Falta de capacitación al personal en temas de seguridad de la información.
Oportunidades	**Amenazas**
Capacitar al personal en temas de seguridad de la información. Creación de rolos y privilegios a los usuarios para el acceso a los datos.	No existe un SGSI

Nota. Resultados del análisis DAFO

Inventario de activos

Villadeza & Condor (2022), define a los activos del sistema de información como: partes o características que son vulnerables a ataques intencionales o ataques con percusiones y que afecta a la empresa. Además, son los elementos necesarios para la organización y procesamiento de información.

Se obtuvo un inventario de los activos informáticos que posee la empresa XNET, como se observa en la Tabla 2.

Tabla 2

Inventario de activos

Tipo	Código	Activo
Datos	D01	Archivos Digitales
	D02	Respaldo de Información Financiera
Servicios	S01	Página web
	S02	Facturación electrónica
Software	SW01	Sistema Financiero
	SW02	Sistema de Gestión de Clientes
	SW03	Sistemas Operativos
	SW04	Herramientas ofimáticas
Hardware	HW01	Servidor HP Proliant
	HW02	OLT Huawei
	HW03	Router Mikrotick
	HW04	Computadoras de oficina
	HW05	Impresoras
	HW06	Centralilla
	HW07	Switch CISCO
	HW08	Teléfonos IP
Soporte de información	MEDIA01	Discos duros
	MEDIA02	NAS
	MEDIA03	Flash Memory
Equipamiento Auxiliar	AUX01	UPS
	AUX02	CCTV
	AUX03	Cableado estructurado
	AUX04	Fibra Óptica
	AUX05	Ventiladores
Redes de Comunicación	COM01	RED LAN
	COM02	RED WIFI
	COM03	RED WAN
	COM04	Telefonía IP
	COM05	Red CCTV
Instalaciones	L01	Data center
	L02	Oficina de TIC

Conciencia Digital
ISSN: **2600-5859**
Vol. 6 No. 4.2, pp. 28 – 45, noviembre 2023
www.concienciadigital.org

Persona	P01	Técnicos Informáticos
	P02	Personal de atención al cliente

Nota. Lista de activos identificados en la empresa XNET

Valoración de los activos

Considerando los activos más importantes, se efectuó una valoración acuerdo a los criterios detallados en la Tabla 3, haciendo uso de la Norma ISO/IEC 27001, se evaluaron cada uno de los atributos que son elementales para la seguridad de la información siendo estas: Confidencialidad(C), Integridad(I), Disponibilidad(D) (Argüezo, 2019).

Tabla 3

Criterio de valoración

Confidencialidad	
Valor	Criterio
0	Cualquier persona dentro o fuera de la institución puede conocerla y utilizarla.
1	Todos en la organización pueden conocerlo y usarlo.
2	Puede ser conocido y utilizado por un grupo de personas que lo necesiten para realizar su trabajo.
3	Puede ser conocido y utilizado por un número muy reducido de personas, cuya divulgación puede perjudicar a la institución o a terceros.
Integridad	
Valor	Criterio
0	Su cambio no autorizado es de fácil reparación o no afecta el funcionamiento de la institución.
1	Los cambios no autorizados pueden repararse, pero pueden causar daños a la institución o a terceros.
2	Su modificación no autorizada es de difícil reparación y puede causar daños importantes a la institución o a terceros.
3	Su modificación no autorizada no puede repararse, imposibilitando su funcionamiento.
Disponibilidad	
Valor	Criterio
0	Su accesibilidad no afecta el funcionamiento normal de la institución.
1	Si una semana sin acceso podría causar un daño importante a la institución.
2	No tener acceso entre semana puede entorpecer las operaciones de la institución.
3	Una hora de indisponibilidad puede dificultar el desempeño de las actividades de la institución.

Nota. Valoración para la triada CID

El resultado de la valoración se observa en la siguiente tabla (Tabla 4).

Tabla 4

Valoración de los activos

Tipo	Código	C	I	D	Justificación
Datos	D01	1	2	1	No deben ser modificados y estar siempre disponibles.
	D02	2	2	1	Posiblemente impedirá la operación efectiva

Software	SW01	1	2	3	Para el acceso y edición deben estar autorizados y mantener un Log
	SW02	1	4	2	La información se podrá cambiar solo con autorización.
Hardware	HW01	1	2	3	Deben ser accedidos y manipulados por personal técnico.
	HW02	1	2	3	Deben ser accedidos y manipulados por personal técnico.
	HW03	1	2	3	Deben ser accedidos y manipulados por personal técnico.
	HW04	1	2	2	Deben ser accedidos y manipulados por personal técnico.
	HW08	1	2	1	Deben ser accedidos y manipulados por personal técnico.
Redes de comunicación	COM01	1	2	3	Garantizar que todos los paquetes lleguen a su lugar de destino correctamente y tiempos oportunos.
Instalaciones	L01	2	2	2	El acceso estará permitido exclusivamente a personal autorizado.
Personal	P01	1	2	2	Personal capacitado y con ética, que garantice la integridad, confidencialidad y disponibilidad de la información,
	P02	1	2	1	Personal capacitado y con ética, encargados de manejar la información con transparencia.

Nota. Valoración de los activos

Amenazas y vulnerabilidades

Haciendo uso de la norma ISO/IEC 27001, Se realizó un análisis de amenazas y vulnerabilidades de los activos más importantes, enfocados en los criterios de Riesgo(R), Impacto(I) y Probabilidad (P) (Tabla 5).

Tabla 5

Criterios de valoración para el impacto, probabilidad y riesgo

Probabilidad	
Valor	Criterio
0	Nunca
1	Una vez al año
2	Una vez cada mes
3	Una vez cada semana
Impacto	

Conciencia Digital
ISSN: **2600-5859**
Vol. 6 No. 4.2, pp. 28 – 45, noviembre 2023
www.concienciadigital.org

Valor	Criterio
0	Sin Impacto
1	Bajo
2	Medio
3	Alto

Riesgo	
Valor	Criterio
<=4	Poco relevante
>=6	Importante y debe ser tratado.

Nota. Valoración para el impacto, probabilidad y el riesgo

Cabe recalcar que el nivel de riesgo será calculado de acuerdo a la siguiente formula:

Probabilidad * Impacto = Nivel de Riesgo

Se definieron 3 niveles para determinar los criterios de gestión o aceptación del riesgo en función de los posibles indicadores que se muestran en la Figura 1.

Figura 1

Mapa de calor para el riesgo

		Probabilidad		
		Bajo	Medio	Alto
Impacto	Alto	3	6	9
	Medio	2	4	6
	Bajo	1	2	3

Nota. La figura expresa un mapa de calor para la valoración del riesgo

A continuación, se presenta la matriz del análisis de amenazas y vulnerabilidades para cada uno de los activos que se encontraron en el análisis de riesgos (Tabla 6).

Tabla 6

Análisis de amenazas y vulnerabilidades

Tipo	Código	Amenazas	Vulnerabilidades	R	I	P
Datos	D01	Eliminación de archivos	Accesos a los datos por usuarios no autorizados.	6	3	2
		Alteración de los archivos	Accesos a los datos por usuarios no autorizados.	6	3	2

Conciencia Digital
ISSN: **2600-5859**
Vol. 6 No. 4.2, pp. 28 – 45, noviembre 2023
www.concienciadigital.org

Tipo	Código	Amenazas	Vulnerabilidades	R	I	P
Servicios		Fuja de información	No existe políticas ante la fuja de información.	4	2	2
	S02	Acceso no autorizado	Bajo nivel de seguridad en las claves de acceso	3	3	1
Software	SW001	Acceso no autorizado	Bajo nivel de seguridad en las claves de acceso	6	3	2
		Eliminación o alteración de registros	Elevado nivel de privilegios a los usuarios.	4	2	2
	SW002	Fuera de servicio	Dependencia del ambiente web para agregar un cliente	4	2	2
Hardware	HW01	Fuego	Malas condiciones en las instalaciones eléctricas	3	3	1
		Daños por agua	Malas condiciones de cubierta de data center	3	3	1
		Averías de origen físico o lógico	Falta de mantenimiento preventivo y correctivo	3	3	1
		Corte de suministro eléctrico	Fallas en el suministro eléctrico por un lapso prolongado de tiempo	2	2	1
		Condiciones inadecuadas de temperatura	Inexistencia de equipo de aire acondicionado que regulen la temperatura de la data center	4	2	2
		Perdida de equipos	Poca seguridad en el acceso data center	4	2	2
	HW02	Daños por agua	Malas condiciones de las instalaciones de tubería de agua	3	3	1
		Averías de origen físico o lógico	Falla del equipo por vida útil del equipo cumplida	3	3	1
		Corte de suministro eléctrico	Fallas en el suministro eléctrico por un lapso prolongado de tiempo	2	2	1
		Condiciones inadecuadas de temperatura	Inexistencia de equipo de aire acondicionado que regulen la temperatura de la data center	2	2	2
		Perdida de servicio	Fuera de servicio de comunicación por fallas de configuración.	3	3	1
	HW03	Daños por agua	Malas condiciones de las instalaciones de tubería de agua	3	3	1
		Averías de origen físico o lógico	Falla del equipo por vida útil del equipo cumplida	3	3	1
		Corte de suministro eléctrico	Fallas en el suministro eléctrico por un lapso prolongado de tiempo	2	2	1
		Condiciones inadecuadas de temperatura	Inexistencia de equipo de aire acondicionado que regulen la temperatura de la data center	4	2	2
		Perdida de servicio	Fuera de servicio de comunicación por fallas de configuración.	4	2	2

Conciencia Digital
ISSN: **2600-5859**
Vol. 6 No. 4.2, pp. 28 – 45, noviembre 2023
www.concienciadigital.org

Tipo	Código	Amenazas	Vulnerabilidades	R	I	P
Equipamiento auxiliar	HW04	Corte de suministro eléctrico	Fallas en el suministro eléctrico	2	2	1
		fallas en periféricos de entrada y salida	Mal uso y/o ciclo de vida cumplida.	2	2	1
		infección de virus	Uso de antivirus gratuitos y desactualizados	4	2	2
		Fuego	Malas condiciones en las instalaciones eléctricas	2	2	1
		Daños por agua	Malas condiciones de cubierta de data center	2	2	1
		Averías de origen físico o lógico	Falta de mantenimiento preventivo y correctivo	2	2	1
	HW07	Corte de suministro eléctrico	Fallas en el suministro eléctrico por un lapso prolongado de tiempo	2	2	1
		Condiciones inadecuadas de temperatura	Inexistencia de equipo de aire acondicionado que regulen la temperatura de data center	2	2	1
		Perdida de equipos	Poca seguridad en el acceso data center	2	2	1
		Fallas de las baterías	Falta de mantenimiento en las baterías	2	2	1
	AUX01	No cubren las necesidades de respaldo	Falta de equipos para cubrir las necesidades de respaldo eléctrico	4	2	2
Redes de comunicación	COM01	Perdidas de paquetes	Problemas en los equipos mal configurados	6	3	2
		Fallas físicas	Errores en el funcionamiento ya sea por vida útil o falta de mantenimiento.	4	2	2
Instalaciones	L01	Incendio	Problemas de instalaciones eléctricas	3	3	1
Personal	P01	Perdida de personal	Renuncia por motivos personales o laborables.	6	3	2

Nota: Análisis de amenazas y vulnerabilidades

Evaluación del riesgo

Una vez realizado el análisis de amenazas y vulnerabilidades y definido su probabilidad e impacto, se procedió a evaluar el riesgo, y donde se debe decidir qué acciones se deberían tomar en referente a los riegos priorizados, donde se consideraron 3 niveles de criticidad: bajo, medio y alto (Tabla 7).

Tabla 7

Evaluación del riesgo

Cód.	Riesgo	Criticidad	Justificación	Aceptación
R01	Ingreso al Data Center por personal no autorizado	Medio	Poca seguridad para el acceso al sitio.	No es aceptable, pues se planifica incrementar más niveles de seguridad
R02	Acceso indiscriminado a los datos.	Medio	Inexistencia de controles, para control de acceso a los datos.	Es aceptable a corto plazo, se planifica la creación de roles y privilegios.
R03	Robo de la información	Medio	Falta de control para prevenir la fuga.	Es aceptable a corto plazo, se propone control, de uso de medios extraíbles.
R04	Daños o destrucción a la red de datos.	Medio	Acceso libre al cableado del edificio	Es aceptable a corto plazo, se propone reforzar la seguridad del cableado
R05	Fata de capacitación al personal	Medio	No existe capacitación en temas de seguridad al personal	Es aceptable, se propone crear capacitación de manera periódica.

Nota. Evaluación del riesgo

Controles y salvaguardas

Basándonos en la norma ISO/IEC27002:2013, se han creado varios controles/salvaguardas para cada uno de los riesgos que han sido identificados, mismos que no ayudaron a eliminar o reducir el riesgo o impacto (Tabla 8).

Tabla 8

Controles y salvaguardas

Cod.	Controles/Salvaguardas
R01	Levar control de personal que ingresan al Data Center. Instalar cámaras de seguridad en el Data Center. Mantener las puertas bloqueadas. Reforzar los niveles de ingreso.
R02	Asignar privilegios a todos los usuarios. Respaldar la información de manera semanal Aplicar restricciones a las carpetas compartidas. Registrar los usuarios que acceden a los datos.
R03	Firmar actas y acuerdos de confidencialidad Implementar servicio de directorio activo y aplicar políticas de seguridad. Aplicar bloqueo de puertos USB.

Conciencia Digital
ISSN: **2600-5859**
Vol. 6 No. 4.2, pp. 28 – 45, noviembre 2023
www.concienciadigital.org

	Realizar una gestión de cables, basados en el sistema de bandejas tanto para techos como para paredes.
R04	Proteger con medidas físicas y con llaves los accesos a switch y router de la empresa. Realizar inspecciones de manera trimestral y verificar que no esté expuesto a este riesgo nuevamente
R05	Realizar una capacitación sobre las buenas prácticas en temas de la seguridad de la información de manera semestral.

Nota. Controles/salvaguardas

Conclusiones

- Como conclusión se expide la presente guía rápida de un Sistema de Gestión de Seguridad de la Información para una ISP, más sin embargo hay que tener en cuenta que cada ISP es único y las conclusiones específicas pueden variar según el contexto.
- La presente guía nos permite abordar la protección de la infraestructura del ISP, incluidos los servidores, equipos de red y sistemas críticos. Esto implica implementar medidas técnicas para proteger los activos de información y prevenir amenazas como el acceso no autorizado, la intrusión y el robo de datos.
- Se ha llevado a cabo una evaluación de riesgos exhaustiva para identificar las amenazas y vulnerabilidades y asimismo valorar su riesgo, impago y probabilidad. Con base en la evaluación de riesgos, los ISP deben implementar los controles descritos en la Tabla 8, para monitorear y revisar continuamente los riesgos.
- Los ISP al manejar una gran cantidad de información confidencial de sus clientes, como datos de inicio de sesión, información de pago y detalles de tráfico, se debe implementar los controles para mejorar seguridad física y lógica, como también proteger los sistemas que almacenan o procesan datos sensibles.
- Los ISP están sujetos a diversas regulaciones y requisitos legales en relación con la protección de la información y la privacidad de los clientes. Al implementar un SGSI, es fundamental asegurarse de que se cumplan estos requisitos. Esto puede implicar el cumplimiento de regulaciones como la Ley de Protección de Datos.

Conflicto de intereses

Los autores declaran que no existe conflicto de intereses en relación con el artículo presentado.

Referencias bibliográficas

Argüezo, E. (2019). Propuesta de un sistema de gestión de seguridad de la informacion para la proteccion de los activos de informacion basados en la norma ISO 27001 en el area de informatica de la municipalidad provincial de Huánuco. [Tesis de grado, Universidad de Huánuco]. http://repositorio.udh.edu.pe/123456789/2084

Avila, R., & Cuenca, J. (2021). Análisis y evaluación de riesgos: aplicado a EMAPAL-EP, basado en la metodologia de MAGERIT version 3.0. Dominio de las Ciencias, 14. https://doi.org/10.23857/dc.v7i4.2425

Bailón, W. (2019). Gestión de riesgos del área informática de las empresas exportadoras de pesca blanca de Manta y Jaramijó. Polo del Conocimiento. https://doi.org/10.23857/pc.v4i8.1053

Caiza, M., & Bolaños, F. (2014). Las implementaciones de las normas de seguridad de la información: estudio de caso la Sociedad de Lucha Contra el Cáncer del Ecuador. Revista electrónica de Computación, Informática, Biomédica y Electrónica. https://www.redalyc.org/articulo.oa?id=512251568001

ESET. (2021). Security Report Latinoamérica 2021. https://www.welivesecurity.com/wp-content/uploads/2021/06/ESET-security-report-LATAM2021.pdf

Lema, C., & Cuenca, J. (2020). Plan de gestión de seguridad de la información, caso de estudio: gobierno provincial del cañar. Journal of Science and Research, 14. https://doi.org/10.5281/zenodo.4142114

Loja, E., & Cuenca, J. (2020). Propuesta de guía rápida de un sistema de gestión de la seguridad de la informacion, para el registro de la propiedad del Canton Cuenca. Dominio de las Ciencias, 27. https://doi.org/10.23857/dc.v6i4.1566

Molina, M. (2017). Análisis de riesgos de centro de datos basado en la herramienta Pilar de Magerit. Espirales revista multidisciplinaria de investigación. https://doi.org/10.31876/re.v1i11.125

Núñez, F., & Carhuancho, B. (2020). Ciberdelincuencia en tiempos de COVID-19: ¿La vulneración a derechos constitucionales? Lumen. https://doi.org/10.33539/lumen.2020.v16n1.2287

Ortiz, J. (2019). Análisis de riesgo y vulnerabilidades de la red de datos, en un ISP, utilizando el estandar ISO/IEC 2007:2008. Caso de estudio: Empresa Sistelcel. Polo del Conocimiento. https://doi.org/10.23857/pc.v4i7

Parra, M., & Cabrera, E. (2020). Evolución de la COVID-19 en Ecuador. Investigacion y Desarrollo. https://doi.org/10.31243/id.v13.2020.1002

Peralta, M., & Aguilar, D. (2021). La ciberseguridad y su concepcion en las PYMES de Cuenca, Ecuador. 1(57). https://ojs.econ.uba.ar/index.php/Contyaudit/article/view/2061/2797

Tejena, M. (2018). Análisis de riesgos en seguridad de la información. Polo del Conocimiento. https://doi.org/10.23857/pc.v3i4.809

Villadeza, K., & Condor, R. (2022). Diseño de un sistema de gestión de seguridad de la informacion basado en la norma técnica peruana-ISO/IEC 27001:2014 para la municipalidad distrital de HUÁCAR 2022. [Tesis de grado, Universidad Nacional Hermiliovaldizán]. https://repositorio.unheval.edu.pe/bitstream/handle/20.500.13080/8238/TIS00137V66.pdf?sequence=1&isAllowed=y

Conciencia Digital

ISSN: **2600-5859**
Vol. 6 No. 4.2, pp. 28 – 45, noviembre 2023

www.concienciadigital.org