




Políticas de seguridad de la información y metodología Magerit en la empresa Induamerica Chiclayo S.A.C

Information security policies and Magerit methodology in the company Induamerica Chiclayo S.A.C

Eli Linares¹ , Luis Balverdi¹  y Immer Cuellar¹ .

RESUMEN

El objetivo de este trabajo fue diseñar un modelo de políticas de seguridad de la información basada en la ISO 27001:2013 y la metodología Magerit (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) para el área Tecnología de Información de Induamerica Chiclayo S.A.C. La investigación fue tipo básica de diseño descriptivo y propositivo, la población y muestra fue constituida por los activos de información de la empresa, se empleó como técnica la entrevista y como un instrumento la guía de entrevista utilizando metodología Magerit. Los resultados muestran que los activos de información son los datos/información, servicios, software, equipamiento, comunicaciones, equipamiento auxiliar, instalaciones y personal. Las amenazas expuestas son naturales, de origen industrial, errores y fallos no intencionados y ataques intencionados. Con el análisis de gestión de riesgos y un modelo adecuado de políticas de seguridad basados en la Norma ISO 27001:2013 el cual permitirá un desarrollo de implementación de acuerdo con las amenazas que podrían materializarse y afectar un activo.

Palabras clave: Informática, activos de información, sistemas informáticos.

ABSTRACT

The objective of this work was to design a model of information security policies based on ISO 27001:2013 and the Magerit methodology (Methodology of Analysis and Risk Management of Information Systems) for the Information Technology area of Induamerica Chiclayo S.A.C. The research was basic type of descriptive and propositive design, the population and sample was constituted by the company's information assets, the interview technique was used and as an instrument the interview guide using Magerit methodology. The results show that the information assets are data/information, services, software, equipment, communications, auxiliary equipment, facilities and personnel. The exposed threats are natural, industrial, unintentional errors and failures, and intentional attacks. With the risk management analysis and an adequate model of security policies based on the ISO 27001:2013 Standard, which will allow an implementation development according to the threats that could materialize and affect an asset

Keywords: Information technology, information assets, information systems.

DOI: <https://doi.org/10.37787/pakamuros-unj.v10i2.224>

Recibido: 17/11/2021. Aceptado: 29/03/2022

* Autor para correspondencia

¹. Universidad Peruana Unión, Perú. Email: eli.fernandez@upeu.edu.pe; harley.balverdi@upeu.edu.pe; immer@upeu.edu.pe

INTRODUCCIÓN

Debido a la inquietud por la confidencialidad, integridad y disponibilidad de la información, las empresas tienen la necesidad de implementar políticas en el sistema de gestión de seguridad en la información, la cual permita obtener beneficios en un corto, mediano y largo de tiempo a fin de reducir los riesgos de los sistemas de Información (Rodríguez, et al., 2020). Entre las principales modalidades de ataque al sistema de seguridad que sufren las empresas alrededor del mundo destaca filtraciones internas en 1.6%, códigos dañinos 1.4%, dispositivo robado en 1.0%, ataques de bots en 0.4%, etc., cuyos efectos principales son pérdida de información en 5.9%, paralización de las actividades en 4.0%, deterioro de los equipos en 0.5% (Fernández, 2020).

En España, de acuerdo con Jiménez (2020) más del 57% de las empresas han sufrido ataques informáticos durante el periodo 2020, lo cual ha generado que más del 96% de la alta dirección se interese por emplear mecanismos y herramientas sistemáticas con la finalidad de asegurar la seguridad de la información. Así pues, Yañez (2017) expone la realidad que se presenta en la Subsecretaría de Economía y Empresas de menor tamaño en Chile, quien consideró importante la implementación de un Sistema de Gestión de Seguridad de la Información, aplicar la Norma ISO 27001:2013 y diseñar un software que permita adoptar políticas y seguir procesos enfocados a garantizar la seguridad de la información y mejorar la toma de decisiones, gestión de los riesgos, monitoreo constante, entre otros, lo cual ha generado cambios positivos y significativos para la entidad. En Perú, respecto a la seguridad de información, la realidad no es distinta a la que se presenta dentro de las empresas alrededor del mundo, es así que Aguirre (2018) reconoce que la empresa de Servicios Informáticos S.A.C. ha presentado falencias relacionadas con la gestión de seguridad debido a que no se aplican correctamente procedimientos para resguardar la información y documentos, tampoco hacen el uso efectivo de los recursos tecnológicos, provocando que la información pueda ser fácilmente vulnerada. Por lo que, frente a tales contingencias, la gerencia consideró de manera relevante, diseñar un software aplicando la norma ISO 27001:2013, con la finalidad de que se puedan evaluar fácilmente los riesgos que se presenten en la empresa, los mismos que impactan de forma negativa en la realización de sus actividades.

Para el año 2013 se publicó una nueva versión acompañada de reformas estructurales para evaluar y tratar los riesgos para ser denominada ISO 27001:2013 (Valencia & Orozco, 2017). En lo que refiere a la información De la Peña (2015) y De Pablos et al. (2019), refieren que está comprendida por diversos datos procesados, transformados y expuestos ordenadamente con la finalidad de disminuir las probabilidades de riesgos a futuro. Por otro lado, de esta manera se contribuye adecuadamente en la toma

de decisiones asertivas (Beynon,2018; Reyes, Maderni y Silva, 2015). En tanto la seguridad de la información es el conjunto de medidas preventivas y reactivas adoptadas por las organizaciones con el propósito de resguardar y proteger la información buscando asegurar que sean íntegras, disponibles y confiables (Miguel, 2016; Joyanes, 2015; Mahfuth et al., 2017; Baca, 2015; Altamirano y Bayona, 2017). La metodología Magerit (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), es una guía para implementar sistemas de gestión de seguridad de la información, por medio de la cual se puede analizar los riesgos a los que se encuentran expuestos los activos informáticos de una organización (Miranda et al., 2016; Postigo, 2020). La seguridad informática a través de la metodología Magerit permite evaluar el desempeño de los sistemas informáticos de tal manera que proporcione resistencia frente a los actos ilícitos en donde se vean comprometidos los datos e información almacenada y transmitida por las redes o sistemas informáticos (Amutio, 2015; Pachao, 2019).

En la empresa Induamerica Chiclayo S.A.C., se percibe que existen deficiencias significativas que afectan el adecuado funcionamiento de esta, dentro de los cuales destaca la ausencia de un modelo de políticas de seguridad de la información, deficiente gestión de riesgos en el área de tecnología de información y sistemas de la empresa. Asimismo, no existe una valoración de riesgos en los activos, escasa participación en la identificación de riesgos, controles de seguridad, carece de concienciación y apropiación en seguridad de la información por parte de los trabajadores, no se cuenta con un sistema o registro de información adecuada para la gestión del riesgo y como consecuencia no se identifica los riesgos a los que están expuestos los activos, priorizarlos y tratarlos.

De acuerdo con la exploración de los datos e información se planteó como objetivo diseñar un modelo de políticas de seguridad de la información basada en la ISO 27001:2013 y la metodología Magerit para reducir los riesgos a los que se encuentran expuestos los activos de información del área de tecnologías de la información (TI) de la empresa Induamerica Chiclayo S.A.C.

MATERIALES Y MÉTODOS

Tipo y diseño de investigación

La investigación fue básica (Cantillo y Buitrago, 2018; Concytec, 2018), debido a que se efectuó un análisis de los componentes de las variables en su entorno natural; así también, se realizó un diseño descriptivo-propositivo, debido a que se caracterizó los activos, amenazas y riesgos, dando paso a la formulación de alternativas de solución mediante la propuesta de acción.

Técnicas e instrumentos de recolección de datos

Se solicitó autorización al área de tecnologías de la información de Induamerica Chiclayo S.A.C, Región Lambayeque. La técnica para la recolección de los datos fue la entrevista, Rivero (2018) señala que permite recolectar los datos necesarios concernientes a las variables en estudio mediante la participación de los involucrados en los diversos procesos, es decir de fuentes primarias. De esta manera se consignó como instrumento la guía de entrevista, la misma que fue aplicada a los encargados del área de informática para describir en qué medida las acciones se vienen desarrollando y obtener información específica.

Para el análisis de datos se empleó el método cuantitativo, se obtuvieron datos descriptivos con la finalidad de expresarlos en tablas de doble entrada, utilizando Microsoft Office. Asimismo, para el procesamiento de los datos se empleó el programa de Microsoft Excel elaborando tablas correspondientes a los activos, los riesgos y amenazas, estos facilitaron la presentación ordenada de la información. De igual manera se empleó el método analítico, por cuanto se observó y analizó la naturaleza de la problemática presentada de tal manera que se pueda adquirir mayor conocimiento sobre las variables en estudio.

RESULTADOS

En la Tabla 1, se ha identificado los activos de información pertenecientes al Grupo Induamerica, los mismos que se describieron en relación con los tipos de activos en la guía Magerit. También se muestra la descripción por elementos para la valorización de los activos de información en sus 5 dimensiones (software, equipamiento, comunicaciones, instalaciones y personal).

Tabla 1. Identificación activos de información

Datos/información	Contenido
Copia de seguridad del sistema de información del Grupo Induamerica.	Batch de copia de seguridad del sistema de información Osiris.
Código fuente del sistema Osiris.	Código fuente del sistema interno desarrollado.
Servicios	
Servicio de correo corporativo.	Gestión de comunicación en la empresa, clientes y público puedan comunicarse con el área competente para sus reclamos o consultas.
Portal Web – Grupo Induamerica.	Servicio administrable que está disponible hacia el público en general.
Servicio de soporte técnico.	Servicio presentado para atención directa con los usuarios del Grupo Induamerica.
Software	
Software propio del Grupo Induamerica.	Software desarrollado por el Grupo Induamerica necesidades específicas.
Base Datos.	Administrar y gestionar la información que se utilizan en el Grupo Induamerica.
Antivirus.	Software para prevenir virus y eliminar malware.
Sistemas operativos.	Software que administra el uso de las computadoras.
Ofimática.	Programas informáticos que se aplican al trabajo de oficina.
Equipamiento	
Servidores de aplicaciones del Grupo Induamerica.	Computadoras que proveen los recursos de almacenar datos y ejecutar el software y diferentes aplicaciones del Grupo Induamerica.

Dispositivos de respaldo.	Discos duros que almacenan información y son útiles para la recuperación de desastres.
Ordenadores y laptops	Permite la realización de tareas del personal administrativo conectados a través de la red interna.
Impresoras.	Impresión de documentos, guía de remisión, código de barra, etc.
Switch.	Administrar el acceso y resolver problemas de rendimiento en la red.
Mikrotik	Control de la red.
Comunicaciones	
Internet.	Permite el acceso a diferentes páginas web o necesidades externas.
Equipamiento auxiliar	
Cableado estructurado.	Provee la transferencia de datos en las distintas áreas del Grupo Induamerica.
UPS	Sistema de Alimentación Ininterrumpida para los Servidores.
Instalaciones	
Oficinas de tecnologías de información Grupo Induamerica.	Estructura física que alberga al área de tecnologías de información Grupo Induamerica.
Personal	
Personal de TI	Equipo de tecnologías información encargado de implementar funcionalidades del sistema de información.

Las amenazas a las que están expuestos los activos de la organización fue clasificado mediante Magerit, la cual está dividida en cuatro grupos (Tabla 2).

Tabla 1. Amenazas de los activos según dimensiones

	[N] Naturales	Caracterización en sus dimensiones				
		C	I	D	A	T
[N.1] Fuego.						
[HW] Servidores de aplicaciones del Grupo Induamerica.				1		
[HW] Dispositivos de respaldo.				1		
[HW] Ordenadores y laptops.				3		
[HW] Impresoras.				3		
[HW] Switch.				2		
[HW] Mikrotik				2		
[L] Oficinas de tecnologías de información Grupo Induamerica.				1		
[N.2] Daños por agua.						
[HW] Servidores de aplicaciones del Grupo Induamerica.				1		
[HW] Dispositivos de respaldo.				1		
[HW] Ordenadores y laptops.				3		
[HW] Impresoras.				3		
[HW] Switch.				2		
[HW] Mikrotik				2		
[AUX] Cableado estructurado.				2		
[AUX] UPS.				2		
[L] Oficinas de tecnologías de información Grupo Induamerica.				1		
[N.7] Fenómeno sísmico.						
[HW] Servidores de aplicaciones del Grupo Induamerica.				1		
[HW] Dispositivos de respaldo.				1		
[HW] Ordenadores y laptops.				4		
[L] Oficinas de tecnologías de información Grupo Induamerica.				1		
[I] De origen industrial						
[I.1] Fuego.						
[HW] Servidores de aplicaciones del Grupo Induamerica.				1		1
[HW] Dispositivos de respaldo.				2		1
[HW] Ordenadores y laptops.						3

[HW] Impresoras.						3
[HW] Switch.						3
[HW] Mikrotik						3
[AUX] Cableado estructurado.						3
[AUX] UPS.						4
[L] Oficinas de tecnologías de información Grupo Induamerica.						1
[I.2] Daños por agua.						
[HW] Servidores de aplicaciones del Grupo Induamerica.			1			1
[HW] Dispositivos de respaldo.			2			1
[HW] Ordenadores y laptops.						3
[HW] Impresoras.						3
[HW] Switch.						3
[HW] Mikrotik.						3
[AUX] UPS.						3
[I.5] Avería de origen físico o logito.						
[SW]Software propio del Grupo Induamerica.						1
[SW]Sistemas operativos.						2
[HW] Servidores de aplicaciones del Grupo Induamerica.						1
[HW]Ordenadores y laptops.						1
[I.7] Condiciones inadecuadas de temperatura o humedad.						
[HW] Servidores de aplicaciones del Grupo Induamerica.						1
[I.8] Fallo de servicios de comunicación.						
[COM] Internet						2
[E] Errores y fallos no intencionados						
[E.2] Errores del administrador.						
[D]Copia de seguridad del sistema de información del Grupo Induamerica.						1
[D]Código fuente del sistema Osiris.						1
[S]Servicio de soporte técnico.						1
[SW]Software propio del Grupo Induamerica.						1
[SW]Base de datos.						1
[E.8] Difusión de software dañino.						
[SW]Antivirus.						1
[SW]Sistemas operativos.						1
[SW]Ofimática.						2
[E.18] Destrucción de información.						
[SW]Base datos.						1
[E.19] Fugas de información.						
[SW]Base datos.						1
[P]Personal de TI		2	3		2	3 3
[E.20] Vulnerabilidades de los programas (software).						
[SW]Software propio del Grupo Induamerica.						1
[E.21] Errores de mantenimiento / actualización (SW).						
[SW]Antivirus.						1
[SW]Sistemas operativos.						1
[E.23] Errores de mantenimiento / actualización (HW).						
[HW]Ordenadores y laptops.						1
[E.28] Indisponibilidad del personal.						
[P]Personal de TI						1
[A] Ataques intencionados						
[A.5] Suplantación de la identidad del usuario.						
[S] Portal web - Grupo Induamerica.						4
[SW] Software propio del Grupo Induamerica.						1
[A.6] Abuso de privilegios de acceso.						
[D] Copia de seguridad del sistema de información del Grupo Induamerica.		1			1	2 2
[D] Código fuente del sistema Osiris.		1			1	2 2
[A.7] Uso no previsto.						
[S] Servicio de correo corporativo.						2

[A.11] Acceso no autorizado.					
[SW] Software propio del Grupo Induamerica.	1		1	1	1
[A.15] Modificación Deliberada De La Información.					
[SW]Base datos.	1	1	1	1	1
[A.19] Divulgación De Información.					
[D] Código fuente del sistema Osiris.	1	1	1	1	1
[A.30] Ingeniería Social					
[P] Personal de TI	1	1		1	1

Nota: Valoración de relevancia: 1=Muy alta; 2=Alta; 3=Media; 4=Baja; 5=Depreciable

Tabla 3, se muestra los resultados de la valorización de las amenazas, según el tipo de activos y su respectiva valoración.

Tabla 3. Valoración de las amenazas según tipo de activos

Amenazas	F	Valoración				
		C	I	D	A	T
[D] Datos/Información						
[E.2] Errores del administrador.	PF	1	1	2		
[A.6] Abuso de privilegios de acceso.	N	1	1			
[A.19] Divulgación de información.	N	1				
[S] Servicios						
[A.7] Uso no previsto.	N	2	1	1		
[A.5] Suplantación de la identidad del usuario.	N	1	1	1	1	1
[E.2] Errores del administrador.	PF	1	1	3		
[SW] Software						
[A.11] Acceso no autorizado.	N	1	1	1		
[A.15] Modificación deliberada de la información.	PF	1	1			
[A.5] Suplantación de la identidad del usuario.	F	1	1			
[E.18] Destrucción de información.	N			1		
[E.19] Fugas de información.	PF	3				
[E.2] Errores del administrador.	N			1		
[E.21] Errores de mantenimiento/actualización SW.	N		2	1		
[E.8] Difusión de software dañino.	N	1	1	1		
[I.5] Avería de origen físico o lógico.	N			1		
[HW] Equipamiento informático						
[I.1] Fuego.	PF			1		
[I.2] Daños por agua.	N			1		
[I.5] Avería de origen físico o lógico.	N			1		
[I.7] Condiciones inadecuadas de temperatura o humedad.	N			1		
[N.7] Fenómeno Sísmico	PF			1		
[N.1] Fuego.	PF			1		
[N.2] Daños por agua.	PF			1		
[COM] Redes comunicación						
[I.8] Fallo de servicios de comunicaciones	PF			1		
[AUX] Equipamiento auxiliar						
[I.1] Fuego.	PF			1		
[I.2] Daños por agua.	PF			1		
[N.2] Daños por agua.	PF			1		

[L] Instalaciones			
[I.1] Fuego.	PF	1	
[N.7] Fenómeno Sísmico	PF	1	
[N.2] Daños por agua.	PF	1	
[P] Personal			
[E.19] Fugas de información.	N	1	1 1
[E.28] Indisponibilidad del personal.	N		3
[A.30] Ingeniería social	N	1	1 1

Nota: Valoración de relevancia: 1=Muy alta; 2=Alta; 3=Media; 4=Baja; 5=Depreciable; Frecuencia de amenaza: 100 Muy frecuente (MF) = A diario; 10 Frecuente (F) = Mensualmente; 1 Normal (N) = Una vez al año; 0.1 Poco frecuente (PF) = Cada varios años; F= frecuencia

Tabla 4, muestra el índice de riesgo de acuerdo con los activos, indicando el nivel del valor del riesgo.

Tabla 4. Índices de riesgo de acuerdo con los activos

Tipo de activo	Nombre de activo	Valor del activo	Nivel del valor de riesgo*
[D] Datos / Información	Copia de seguridad del sistema de información del Grupo Induamerica.	MA	Grave
	Código fuente del sistema Osiris.	A	
	Servicio de correo corporativo.	A	
[S] Servicios	Portal web - Grupo Induamerica.	M	Aceptable
	Servicio de soporte técnico.	M	
	Software propio del Grupo Induamerica.	A	
[SW] Software	Base datos	MA	Grave
	Antivirus.	A	
	Sistemas operativos.	A	
	Ofimática.	M	
[HW] Equipamiento informático	Servidores de aplicaciones del Grupo Induamerica.	A	Tolerable
	Dispositivos de respaldo.	A	
	Ordenadores y laptops.	M	
	Impresoras.	M	
[COM] Redes comunicación	Switch.	MA	Aceptable
	Mikrotik	MA	
[AUX] Equipamiento auxiliar	Internet.	M	Aceptable
[COM] Equipamiento auxiliar	Cableado estructurado.	M	Aceptable
[COM] Equipamiento auxiliar	UPS	M	Aceptable
[L] Instalaciones	Oficinas de tecnologías de información Grupo Induamerica.	M	Grave
[P] Personal	Personal de TI.	M	Aceptable

Nota: E(10)=Extremo; MA(9)=Muy Alto; A(6-8)=Alto; M(3-5)=Medio; B(1-2)=Bajo; D(0)=Depreciable; E=daño extremadamente grave; MA=daño muy grave; A=daño grave; M=daño importante; B=daño menor y D=irrelevante a efectos prácticos.

* Aceptable (A)=1-3; Tolerable (B)=4-9; Grave(C)=10-50; Inaceptable (D)= 51-100

Del diseño del modelo resulto las siguientes actividades que son importantes para la obtención de óptimos resultados (Tabla 5).

Tabla 5. Modelo de seguridad Induamerica Chiclayo S.A.C -Norma ISO/IEC 27001:2013

Metodología Magerit		Controles de seguridad ISO 27001:2013 anexo A.	
Tipo de activo	[D] Datos / información		A.5. Políticas de seguridad
			A.5.1 Directrices de la dirección en Si.
	Nombre	Amenazas Riesgos	A.5.1.1 Conjunto de políticas para SI

Política

Copia de seguridad del sistema de información del Grupo Induamerica.	[E.2] Errores del administrador.	Truncamiento de la generación copia de seguridad.	<p>Elaborar un manual de procedimiento para la generación de copias de seguridad y respaldar los archivos de logs o registro de los sistemas en proceso, cada cierto tiempo durante el día.</p> <p>Conocer y manejar el software utilizado para la generación y/o restauración de copias de respaldo, registrando el contenido y su prioridad. Rotación de las copias de respaldo, debidamente marcadas.</p> <p>Ningún usuario recibirá un identificador de acceso a la red de comunicaciones, recursos Informáticos o aplicaciones hasta que no acepte formalmente la Política de Seguridad vigente.</p> <p>Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones, conforme a los criterios establecidos por el responsable de la información.</p> <p>La asignación de contraseñas debe ser realizada de forma individual, por lo que el uso de contraseñas compartidas está prohibido.</p> <p>Está prohibido que las contraseñas se encuentren de forma legible en cualquier medio impreso y dejarlos en un lugar donde personas no autorizadas puedan descubrirlos. Los usuarios no deben almacenar las contraseñas en ningún programa o sistema que proporcione esta facilidad</p>
Código fuente del sistema Osiris.	[E.2] Errores del administrador.	<p>Realizar publicaciones de codificaciones erróneas que generen el mal funcionamiento del software y afecten en el proceso operativo en el Grupo Induamerica.</p> <p>Alteración indiscriminada de datos para fines personales.</p> <p>Clonación y comercialización de la copia del código fuente.</p>	<p>Elaborar un manual de procedimientos para las publicaciones, estén asociados calidad y precisión del trabajo llevado a cabo por el equipo de desarrollo que incluyan auditorías, revisión de código para detectar errores, verificación del cumplimiento de los requerimientos de seguridad del software establecidos, etc. y no exista alternaciones y clonaciones.</p>
Tipo de activo	[SW] Software	Riesgos	<p>A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información</p> <p>A.14.2 Seguridad en los procesos de desarrollo y soporte</p> <p>Política</p>
Nombre	Amenazas	Fallos en la actualización de software servidor	<p>Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas de la organización y someter a prueba para asegurar que no haya impacto.</p>
Software propio del Grupo Induamerica.	[I.5] Avería de origen físico o lógico.	Incompatible, que afectan el funcionamiento de sus procesos del Grupo Induamerica.	
	[E.20] Vulnerabilidades de los programas (software).	Calculo erróneo de las operaciones con valor monetario.	Elaborar, establecer y aplicar las reglas para el desarrollo de software y de sistemas, desarrollos dentro de la organización y por terceros.

	[A.5] Suplantación de la identidad del usuario.	Que se revele información restringida en el Grupo Induamerica para fines propios.	Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.
	[A.11] Acceso no autorizado.	Manipulación de la información con fines maliciosos.	Los cambios de sistemas de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios. Para la prestación del servicio de desarrollo de Software aplicativo se observará lo siguiente: Todo proyecto de desarrollo o construcción de software requiere de un estudio de factibilidad que permita establecer la rentabilidad del proyecto, así como los beneficios que se obtendrán del mismo.
	[E.2] Errores del administrador.	Paralice las operaciones relacionadas al uso software y afecten en el proceso operativo en el Grupo Induamerica. Detención de los servicios de la base datos.	La organización debe establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.
	[E.2] Errores del administrador.	Corrupción de la base datos por tareas automatizadas.	
Base datos	[E.18] Destrucción de información.	La indisponibilidad de la información. Revelar información no autorizada del Grupo Induamerica.	Implementar procedimientos de desarrollo donde se deben llevar a cabo pruebas de funcionalidad y seguridad de la información.
	[E.19] Fugas de información.	Revelar información no autorizada del Grupo Induamerica.	
	[A.15] Modificación deliberada de la información.	Afecte económicamente al Grupo Induamerica.	
	[E.8] Difusión de software dañino.	Propagación de virus en toda la red del Grupo Induamerica,	El personal contratado tendrá la obligación de utilizar los programas antivirus y sus actualizaciones para prevenir la entrada en los Sistemas de cualquier elemento destinado a destruir o corromper los datos informáticos.
Antivirus.	[E.21] Errores de mantenimiento / actualización de programas (software).	causando retrasos y secuestros de la información.	Cualquier fichero introducido en la red corporativa o en el puesto de trabajo del usuario a través de soportes automatizados, Internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual y control de virus.
Sistemas operativos.	[I.5] Avería de origen físico o lógico.	Fallos en los programas, que afectan el funcionamiento del sistema y la seguridad de la información del Grupo Induamerica.	Definir e implementar los registros de eventos y actividades correspondientes a sistemas operativos y otras plataformas de procesamiento

Tipo de activo	Nombre	Amenazas	Riesgos	
Ofimática.	[E.8] Difusión de software dañino.	Difusión de software dañino.	Propagación de virus que pueda afecte el correcto funcionamiento de los sistemas del Grupo Induamerica.	Es responsabilidad de los usuarios almacenar su información únicamente en la partición del disco duro diferente a la destinada para archivos de programas y sistemas operativos, generalmente c:\.
Tipo de activo	[L] Instalaciones			El personal contratado tendrá la obligación de utilizar los programas antivirus y sus actualizaciones para prevenir la entrada en los Sistemas de cualquier elemento destinado a destruir o corromper los datos informáticos. A.11 Seguridad física y ambiental A.11.2 Áreas seguras A.11.1.4 Protección contra las amenazas externas y ambientales Política
Oficinas de tecnologías de información	[N.1] Fuego. [N.2] Daños por agua. [N.7] Fenómeno Sísmico.		Destrucción de las instalaciones de las oficinas y afecten operativamente lo procesos de negocio y económicamente al Grupo Induamerica.	Las oficinas de tecnologías de trabajo deben contar con una adecuado plan de contingencia para aplicar seguridad física. Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes, con un plan de continuidad del negocio y de Recuperación de Desastres que es puesto a prueba a intervalos regulares.
Grupo	Induamerica. [I.1] Fuego.			

DISCUSIÓN

El modelo de políticas de seguridad basados en la Norma ISO 27001:2013 es importante para la empresa Induamerica Chiclayo S.A.C. por cuanto establece un control a los activos de información expuestos del área de TI de la empresa, contribuyendo así para guiar la conducta individual y profesional de los colaboradores respecto a la información que genera o procesa la empresa. Tales resultados coinciden con lo expuesto por Malagón y Figueroa (2016), pues sustentaron que fue necesario supervisar la implementación de las políticas de seguridad haciendo uso de la metodología Magerit con la finalidad de que el desempeño de la institución educativa pueda mejorar notablemente. En relación con los resultados de la investigación permitieron deducir que entre los activos de información de la empresa Induamerica Chiclayo S.A.C se clasifican en ocho tipos de activos, por cuanto se analizó los activos más graves [D] Datos/Información, [HW] Equipamiento informático, [L] Instalaciones. Tales resultados son congruentes a los expuestos por Pardo (2015), llegó a concluir que la empresa tiene a su disposición una cantidad de activos suficientes para hacer frente a sus necesidades, para lo cual es importante que se adopten buenas prácticas orientadas a velar por los principios de confidencialidad, integridad y disponibilidad, además prever los riesgos y amenazas que se presentan, las mismas que podrían poner en riesgo su buen funcionamiento.

Por otro lado, los resultados alcanzados en el estudio han permitido conocer una gestión de riesgos en la empresa Induamerica Chiclayo S.A.C. Los activos se encuentran expuestos a una serie de amenazas, asociadas a amenazas naturales, errores y fallos intencionados, de origen industrial y ataques intencionados principalmente a causa de la ausencia de controles acorde con las necesidades de la empresa. Estos resultados guardan similitud con los recopilados por Fernández y Mayta (2017), por cuanto los autores fundamentaron que la metodología Magerit permitió reconocer una serie de amenazas que representan un riesgo significativo para los activos de las empresas pertenecientes al sector en estudio; así pues, entre las amenazas destacó la pérdida de los informes de las operaciones, así como los registros de los clientes y usuarios e informes de las transacciones y operaciones económicas y financieras, aparición de virus en los sistemas informáticos, etc.

De igual manera, los resultados obtenidos permitieron conocer que la gran cantidad de amenazas ocasionado que existan altos niveles de riesgo a los que se encuentran expuestos los activos de información de la empresa Induamerica Chiclayo S.A.C., los mismos que afectan en gran medida los principios de seguridad. Estos resultados son análogos a los expuestos por Talavera (2015) concluyendo que existe un alto nivel de riesgos de los activos de información, donde uno de los más significativos fue la falta de actualización de los sistemas de información debido a que estos ya no permiten cubrir la totalidad de necesidades que presenta la entidad, asimismo existen casos de fuga de información de forma constante a razón de que no existe un control efectivo para garantizar el ingreso de personal autorizado a las bases de datos con información relevante sobre la entidad. Además, los resultados permitieron evidenciar que los controles de seguridad acordes para la empresa Induamerica Chiclayo S.A.C., Región Lambayeque, 2020, tomando como base la norma ISO/IEC 27001:2013 permiten asegurar que la información relacionada con el desarrollo de las actividades y gestión de la empresa pueda ser obtenida y empleada por personal debidamente autorizado por la alta dirección de esta. Estos resultados se asemejan a los alcanzados por Benites (2019), pues el autor resalta la importancia de garantizar la seguridad de la información, la misma que es considerada como un compromiso y responsabilidad de todos los colaboradores de los distintos niveles jerárquicos que comprenden la empresa.

CONCLUSIONES

Los activos de información de la empresa Induamerica Chiclayo S.A.C. se clasifican en 8 tipos, por cuanto se analizó activos más graves de la organización [D] Datos/Información, [HW] Equipamiento informático, [L] Instalaciones, el cual se encuentra expuesto a una serie de amenazas naturales, errores y fallos intencionados, de origen industrial y ataques intencionado, principalmente a causa de la ausencia

de controles acorde con las necesidades de la empresa. En cambio, los activos se exponen [E.2] Errores del administrador, [A.6] Abuso de privilegios de acceso, [A.19] Divulgación de información, [A.15] Modificación deliberada de la información, [E.19] Fugas de información, [E.8] Difusión de software dañino, [N.7] Fenómeno Sísmico, [I.1] Fuego y [N.2] Daños por agua. Existen altos niveles de riesgo a los que se encuentran expuestos. Finalmente, el modelo de políticas de seguridad basados en la Norma ISO 27001:2013 es sumamente importante para la empresa por cuanto establecerá controles riesgos a los que se encuentran expuestos los activos de información del área de TI de la empresa.

AGRADECIMIENTOS

A los profesionales encargados de la verificación en cada una de las etapas del estudio y la retroalimentación presentada. También, a la empresa Induamerica Chiclayo S.A.C por las facilidades necesarias para llevar a cabo la investigación.

REFERENCIAS BIBLIOGRÁFICAS

- Aguirre, J. (2018). Sistema web para la gestión de la seguridad de la información alineada a la norma ISO/IEC 27001 en la empresa de Servicios Informáticos S.A.C - La Molina [Tesis de pregrado, Universidad César Vallejo]. http://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/35308/Aguirre_VJM.pdf?sequence=1&isAllowed=y
- Altamirano, J. y Bayona, S. (2017). Information security policies: A systematic review of theories explaining their compliance. *Revista Ibérica de Sistemas y Tecnologías de Información*. 1(25), 112-134. <https://dx.doi.org/10.17013/risti.25.112-134>
- Amutio, M. (2015). Magerit: Versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. MHAP. <https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html>
- Baca, G. (2015). Proyectos de sistemas de información. Grupo Editorial Patria. <https://books.google.com.pe/books?id=N9BUCwAAQBAJ&printsec=frontcover&hl=es#v=onepage&q&f=true>
- Benites, C. (2019). Implementación de un Sistema de Gestión de Seguridad de la Información - Norma ISO 27001 para la Fábrica Radiadores Fortaleza [Tesis de pregrado, Universidad Tecnológica del Perú]. <https://repositorio.utp.edu.pe/handle/20.500.12867/1933>

- Beynon, P. (2018). *Sistemas de información: Introducción a la informática en las organizaciones*. Editorial Reverte. <https://books.google.com.pe/books?id=5jbeDwAAQBAJ&printsec=frontcover&hl=es#v=onepage&q&f=true>
- Cantillo, M. y Buitrago, A. (2018). *Nuevas miradas y enfoques de diversas investigaciones - Tomo II*. Universidad Santiago de Cali
- Concytec. (2018). *Reglamento de calificación, clasificación y registro de los investigadores del Sistema Nacional de Ciencia, Tecnología e innovación Tecnológica - Reglamento Renacyt*. https://portal.concytec.gob.pe/images/renacyt/reglamento_renacyt_version_final.pdf
- De la Peña, N. (2015). *Gestión y control de los sistemas de información*. Editorial Learning. <https://books.google.com.pe/books?id=6cJWDwAAQBAJ&printsec=frontcover&dq=procesamiento+de+los+datos+en+informaci%C3%B3n&hl=es&sa=X&ved=2ahUKEwiOucnO4d7qAhWBJ7kGHWI3CRkQ6AEwAHoECAAQAQg#v=onepage&q=procesamiento%20de%20los%20datos%20en%20informaci%C3%B3n&f=true>
- De Pablos, C., López-Hermoso, J., Martín-Romo, S. y Medina, S. (2019). *Organización y transformación de los sistemas de información en la empresa (4° ed.)*. ESIC Editorial <https://books.google.com.pe/books?id=hnCLDwAAQBAJ&pg=PT434&dq=datos+e+informaci%C3%B3n&hl=es&sa=X&ved=2ahUKEwi96P-Q5N7qAhUuE7kGHQKsA74Q6AEwAXoECAMQAQg#v=onepage&q=informaci%C3%B3n&f=true>
- Fernández, M. (15 de febrero de 2020). *Ciberataques que matan a las empresas*. Diario El País. https://elpais.com/economia/2020/02/14/actualidad/1581694252_444804.html
- Fernández, A. y Mayta, J. (2017). *Diseño de un modelo sistémico de gestión de riesgos de la seguridad de la información integrando la metodología MAGERIR y la Norma ISO 27002:2013 en empresas financieras [Tesis de pregrado, Universidad Católica de Santa María]*. <http://tesis.ucsm.edu.pe/repositorio/bitstream/handle/UCSM/6772/71.0596.IS.pdf?sequence=1&isAllowed=y>
- Jiménez, D. (2020). *Más del 50% de las empresas en España sufrieron ataques de Ransomware en la nube pública el año pasado*. <https://es.cointelegraph.com/news/more-than-50-of-companies-in-spain-suffered-ransomware-attacks-in-the-public-cloud-last-year>
- Joyanes, L. (2015). *Sistemas de información en la empresa*. Alfaomega Editorial

- Mahfuth, A., Salman, Y., Asmidar, A. y Nor'ashikin, A., (2017). A systematic literature review: Information security culture. International Conference on Research and Innovation in Information Systems. 1-6. 10.1109/ICRIIS.2017.8002442
- Malagón, N. y Figueroa, O. (2016). Propuesta de políticas de seguridad de la información para la institución educativa de educación básica y media del departamento de Boyacá, basadas en la norma ISO 27001:2013. <https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/11881/1/24167182.pdf>
- Miguel, J. (2016). Protección de datos y seguridad de la información (4° ed.). ESIC Editorial. <https://books.google.com.pe/books?id=To6fDwAAQBAJ&pg=PA14&dq=Protecci%C3%B3n+de+datos+y+seguridad+de+la+informaci%C3%B3n&hl=es&sa=X&ved=2ahUKEwj13P3c7N7qAhUOJLkGHUxQDhUQ6AEwAHoECAQQA#v=onepage&q=Protecci%C3%B3n%20de%20datos%20y%20seguridad%20de%20la%20informaci%C3%B3n&f=false>
- Miranda, M., Valdés, O., Pérez, I., Portelles, R. y Sánchez, R. (2016). Methodology for the implementation of automated management of computer security controls. Revista Cubana de Ciencias Informáticas. 10(2), 14-26.
- Pachao, W. (2019). Implementación de un sistema de gestión de la seguridad de información en empresa de Outsourcing Helpdesk, Arequipa 2017-2018 [Tesis de pregrado, Universidad Continental]. https://repositorio.continental.edu.pe/bitstream/20.500.12394/7202/1/IV_FIN_108_TI_Pachao_Pizarro_2019.pdf
- Pardo, M. (2015). Modelo de Gestión de Seguridad de la Información para la Universidad de Loja basado en la norma ISO/IEC 27001 [Tesis de pregrado, Universidad Nacional de Loja]. <https://dspace.unl.edu.ec/jspui/bitstream/123456789/11277/1/>
- Postigo, A. (2020). Seguridad informática: Informática y comunicaciones - Sistemas Microinformáticos y Redes. Ediciones Paraninfo. <https://books.google.com.pe/books?id=UCjnDwAAQBAJ&printsec=frontcover&hl=es#v=onepage&q&f=true>
- Reyes, A., Maderni, G. y Silva, G. (2015). El gobierno de la seguridad de la información como instrumento de gestión. Revista del Laboratorio Tecnológico de Uruguay. 33-41. <https://ojs.latu.org.uy/index.php/INNOTEC-Gestion/article/view/9/8>
- Rivero, D. (2018). Metodología de la investigación (3° ed.). Editorial SHALOM

-
- Rodríguez, L., Cruzado, C., Mejía, C. y Alarcón, M. (2020). Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana. *Propósitos y Representaciones*. 8 (3), 1-7.
- Talavera, V. (2015). Diseño un sistema de gestión de seguridad de la información para una entidad estatal de salud de acuerdo a la ISO/IEC 27001:2013 [Tesis de pregrado, Pontificia Universidad Católica del Perú]. <http://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/6092>
- Valencia, F. & Orozco, M. (2017). A methodology for implementing an information security management system based on the family of ISO/IEC 27000 standards. *Revista Ibérica de Sistemas e Tecnologías de Información*. 1(22), 73-88. <https://dx.doi.org/10.17013/risti.22.73-88>
- Yañez, N. (2017). Sistema de gestión de seguridad de la información para la Subsecretaría de Economía y Empresas de menor tamaño. <http://repositorio.uchile.cl/bitstream/handle/2250/147976/Sistema-de-gestion-de-seguridad-de-la-informacion-para-la-Subsecretaria-de-Economia-y-Empresas.pdf?sequence=1&isAllowed=y>