Vol.7 No.3 (2023): Journal Scientific MQRInvestigar ISSN: 2588–0659
https://doi.org/10.56048/MQR20225.7.3.2023.3220-3236

Security Operations Center, as a cybersecurity management model for the Hospital Especialidades de Portoviejo, Manabí-Ecuador.

Security Operations Center, como modelo de gestión de ciberseguridad para el Hospital Especialidades de Portoviejo, Manabí-Ecuador.

Autores:

Ing. Muñoz-Zambrano, Cristóbal
ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FELIX LÓPEZ
Egresado, maestría en ciberseguridad
Portoviejo – Ecuador
cristobal.munoz@espam.edu.ec
https://orcid.org/0009-0001-4632-5244

Ing. Zambrano-Rendón, Aura Dolores, Mg.
ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FELIX LÓPEZ
Docente Tutor del área
Portoviejo – Ecuador
azambrano@espam.edu.ec
https://orcid.org/0000-0002-2784-9202

Citación/como citar este artículo: Muñoz-Zambrano, Cristóbal., y Zambrano-Rendón, Aura Dolores. (2023) Security Operations Center, como modelo de gestión de ciberseguridad para el Hospital Especialidades de Portoviejo, Manabí-Ecuador.
MQRInvestigar, 7(3), 3220-3236.

https://doi.org/10.56048/MQR20225.7.3.2023.3220-3236

Fechas de recepción: 26-JUL-2023 aceptación: 30-AGO-2023 publicación: 15-SEP-2023

https://orcid.org/0000-0002-8695-5005
http://mqrinvestigar.com/

Resumen

Un Security Operations Center es una central de seguridad informática que previene, monitorea y controla la seguridad en sistemas informáticos. Éste como modelo de gestión se refiere a un componente esencial que supervisa, analiza y coordina las actividades relacionadas con la seguridad de la información. Sin embargo, solo se puede aplicar si previamente se ha realizado un diagnóstico que se encargue de evaluar el estado actual de los sistemas, la infraestructura y las prácticas de seguridad de una organización, para obtener un total conocimiento de la misma. □s por ello que a través de las normas ISO 27001 e ISO 27002, se identificarán las fortalezas, oportunidades, debilidades, amenazas, y activos existentes del Hospital de □specialidades de Portoviejo, así como también sus riesgos asociados. Posterior a ello, se evaluarán dichas amenazas potenciales según su nivel de riesgo, estableciendo procedimientos que ejerzan la implementación de controles en función de las políticas y procedimientos establecidos, de modo que sirvan como respuesta a incidentes, incluyendo la identificación, mitigación y recuperación. □n definitiva, la ciberseguridad como modelo de gestión es un enfoque estratégico que protegerá la información y los activos digitales de una organización, colaborando con la mejora continua, y promoviendo una cultura de seguridad en toda la organización.

Palabras clave: Security Operations Center, modelo, ciberseguridad, seguridad, controles, normas, información, riesgos, mitigación, organización.

Abstract

A Security Operations Center is an information security center that prevents, monitors and controls the security of information systems. As a management model, it refers to an essential component that supervises, analyzes and coordinates activities related to information security. However, it can only be applied if a diagnosis has been previously carried out to evaluate the current state of an organization's systems, infrastructure and security practices, in order to obtain a full understanding of the organization. Therefore, through the ISO 27001 and ISO 27002 standards, the strengths, opportunities, weaknesses, threats, and existing assets of the Portoviejo Specialties Hospital will be identified, as well as their associated risks. Subsequently, these potential threats will be evaluated according to their level of risk, establishing procedures that exercise the implementation of controls based on established policies and procedures, so that they serve as a response to incidents, including identification, mitigation and recovery. In short, cybersecurity as a management model is a strategic approach that will protect the information and digital assets of an organization, collaborating with continuous improvement, and promoting a culture of security throughout the organization.

Keywords: Security Operations Center, model, cybersecurity, security, controls, standards, information, risks, mitigation, organization.

Introducción

La información y los procesos que la llevan a cabo, así como sus sistemas y redes, de acuerdo a Pérez (2019) son aspectos importantísimos para las entidades, por lo que requieren ser protegidos frente a riesgos y amenazas que afecten los 4 principios fundamentales de la seguridad informática, siendo éstos, según Briceño (2021), la disponibilidad, confidencialidad, integridad y autenticación de la información, aspectos vitales para lograr los objetivos que las organizaciones poseen. □s así como surge la idea de salvaguardar dichos datos.

Se conoce como ciberseguridad a la acción de proteger los sistemas informáticos, redes, dispositivos y datos de amenazas cibernéticas, teniendo como objetivo principal garantizar que se cumplan los 4 principios fundamentales de la seguridad informática de la información y los recursos digitales, mencionados anteriormente. La ciberseguridad abarca una amplia gama de actividades, que incluyen desde protección contra ataques cibernéticos, hasta asegurar la seguridad de la información enfocándose en proteger la información valiosa y sensible de una organización, evitando su divulgación no autorizada o su manipulación (Becerril, 2021).

Para disminuir estos posibles riesgos es necesario realizar la implementación de controles de seguridad, o modelos que gestionen la protección de la información mediante procedimientos viables. Dichos controles son medidas y mecanismos implementados para proteger los sistemas, datos, redes y recursos digitales de posibles amenazas y riesgos cibernéticos. □stos controles buscan garantizar la confidencialidad, integridad, disponibilidad y autenticación de la información, así como mantener la continuidad operativa y proteger los activos digitales de una organización.

□xisten varios tipos de controles de seguridad, tal como el Security Operations Center (SOC) o Centro de Operaciones de Seguridad, el cual refiere a un equipo o lugar centralizado en una organización que se dedica a monitorear, detectar, analizar y responder a las amenazas e incidentes de seguridad informática en tiempo real (Deepesh, 2022). □l SOC tiene como objetivo principal proteger la infraestructura de tecnologías de la información y los activos digitales de la organización contra ataques cibernéticos y garantizar la continuidad del negocio.

Para la aplicación de dicho control es necesario tomarlo como modelo de gestión, para brindar un enfoque estructurado y sistemático que permita planificar, organizar, dirigir y controlar los recursos y procesos de una organización con el objetivo de lograr sus metas y objetivos de manera efectiva y eficiente, además de precautelar la seguridad de la información (Morales, 2019). Éstos proporcionan una guía para la toma de decisiones y la implementación de acciones que permitan el logro de los resultados deseados. Altamirano (2019) manifiesta que existen diferentes modelos de gestión según el ámbito de aplicación, las características de la organización y los objetivos específicos que se persigan. □ntre éstos

se encuentra el Modelo de Gestión de Riesgos, con el objetivo de minimizar las posibles consecuencias negativas.

La elección del modelo más adecuado dependerá de los objetivos de la organización, su cultura, recursos disponibles y el tipo de resultados que se deseen lograr, es así como se debe llevar un control de seguridad según el área en la que se ha de trabajar. Por tanto, este artículo presentará un diagnóstico para el modelo de gestión de ciberseguridad con el Security Operations Center, para el Hospital □specialidades de Portoviejo, Manabí – □cuador, tomando en cuenta que su viabilidad y eficiencia dependerá de la evaluación de éste mediante las normas ISO 27001 y 27002, las cuales establecen los requisitos para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) en una organización.

Material y métodos

La metodología propuesta contempla la evaluación de un diagnóstico para la implementación del modelo de gestión del SOC para el Hospital de □specialidades de Portoviejo, la cual consta de las siguientes fases:

- ❖ Fase 1. Se realizará el diagnóstico utilizando la Norma ISO 27001, trabajando con las cláusulas 4, 5, 6, 7 de la misma.
- En el punto 4 de la ISO 27001 se analizará el contexto de la organización, a través de un esquema FODA. Éste, de acuerdo a Torres (2019), es una matriz que sirve como herramienta de planificación estratégica utilizada para evaluar las fortalezas, debilidades, oportunidades y amenazas de una entidad, ya sea una empresa, un proyecto, una persona o una organización. Sus siglas hacen referencia a las iniciales con las que empieza los aspectos que evalúa, mencionados con anterioridad. Dicho análisis será de ayuda para comprender la misión, visión, valores y objetivos estratégicos de la organización, así como también su modus operandi.
- En el punto 5 se indicará la revisión de políticas existentes dentro de la organización, siendo éste un aspecto de vital importancia puesto que se evaluará si las políticas están alineadas con los objetivos generales, además de corroborar también éstas siguen siendo relevantes y adecuadas para las operaciones actuales de la organización (Casa *et al*, 2021). De este modo se comprobará el cumplimiento el propósito de las políticas.
- Por su parte, en el punto 6 de la norma se analizarán las acciones para tratar los riesgos en los activos más valiosos. Por ello se presentarán dichos activos existentes en la organización, y conjunto a ello, se mostrará la evaluación de los riesgos que pueden surgir. Para tratar dichos riesgos, se lo realizará por fases: primero identificar los riesgos existentes, posterior a ello evaluarlos con la metodología AMFE, la misma que, de acuerdo a Lema (2019), es un método cualitativo que permite identificar de

manera sistemática una relación de fallos posibles categorizándolos según su prioridad, con sus consiguientes efectos, de esta manera se puede focalizar su acción sobre aquellos que perjudiquen en mayor grado a la unidad en estudio. Por último, tratar los riesgos con la Norma ISO 27002, la cual, como estándar internacional, proporciona pautas y mejores prácticas para el establecimiento, implementación, mantenimiento y mejora de un SGSI (Patiño *et al*, 2019).

La versión que se aplicará es la ISO/IEC 27002:2022.

- En el punto 7 de la ISO 27001 se encuentra el Soporte, aquel que señala que para el buen funcionamiento del SGSI, la organización debe contar con los recursos, competencias, conciencia, comunicación e información documentada pertinente en cada caso, por ello se mostrará una lista de los recursos que han de emplearse para controlar la seguridad de su información (Ramos *et al,* 2023).

❖ Fase 2. Se realizará la estructura del SOC, contemplando las fases de su implementación con su respectiva duración. La estructura y la organización de un SOC puede variar según el tamaño de la organización, la industria y los recursos disponibles. Sin embargo, la función principal de éste es garantizar la seguridad cibernética y la respuesta efectiva a amenazas de seguridad en la infraestructura de TI de la organización (Vielberth *et al,* 2020).

Resultados

Fase N°1:
Determinación de diagnóstico de cláusulas 4, 5, 6 y 7 de la ISO 27001

Cláusula 4: Contexto de la organización

Conocer el entorno en el que se desenvuelve una organización no sólo puede representar una necesidad ligada a un marco normativo, tal como lo requiere la Norma ISO 27001, sino que también es necesario comprender profundamente de su entorno interno y externo, así como de los factores que pueden influir en la seguridad de la información de la organización si se quiere lograr elementos diferenciadores que permitan mejorar su desempeño para diferentes alcances que ésta ha asumido. Toda entidad se encuentra inmersa en un contexto que puede ser social, político, tecnológico, económico, legal, entre otros (Rodríguez *et al,* 2023).

Existen diversas herramientas que permiten inspeccionar el contexto de una organización, entre éstas se encuentra la aplicación de la matriz FODA, aquella que es una herramienta de análisis utilizada en la planificación estratégica de una organización, negocio o proyecto (Huilcapi y Gallegos, 2020). FODA es un acrónimo que se refiere a fortalezas, oportunidades, debilidades y amenazas. Es así como la matriz FODA permitió diagnosticar las del Hospital de Especialidades de Portoviejo, y en base a ello se pudo comprender el contexto de la organización a luz de la norma ISO 27001.

Tabla 1.

FODA del Hospital de Especialidades de Portoviejo

FORTALEZAS	OPORTUNIDADES
▪ Flexible y adaptable a las necesidades de los servidores en el hospital. ▪ No permite intromisiones de otros usuarios a los equipos. ▪ Tiene cortafuegos, IPS/IDS, soluciones de detección de brechas, sondas. ▪ El sistema protege la confidencialidad e integridad de la información corporativa. ▪ Permite mantener servicios de sincronización con la nube. ▪ Permite generar respaldos de seguridad en tiempo real.	▪ Mejorar los recursos tecnológicos garantizando el cuidado de la información. ▪ Presenta un sistema de gestión de eventos e información de seguridad. ▪ Mediante el proceso de innovación se puede detectar y prevenir malwares e incidentes de seguridad cibernética. ▪ Vigilancia constante de todo lo relacionado con las medidas preventivas.
DEBILIDADES	**AMENAZAS**
▪ Perdidas de equipos dentro del Hospital. ▪ Inversión muy mínima para potenciar el sistema se seguridad informática. ▪ Equipos considerados como obsoletos para las necesidades digitales actuales.	▪ Acceso de entidades externas que pueden interferir con las operaciones. ▪ Utilización errónea de los servidores y los datos. ▪ Propagación de un virus dentro de la red

Nota. Elaboración a partir del análisis efectuado en el Hospital de Especialidades de Portoviejo.

Cláusula 5: Revisión de políticas existentes

Éstas se refieren a las directrices, normas y reglas establecidas por una organización para guiar sus acciones, decisiones y operaciones, definiendo la manera en que la institución se comporta y opera en diversos aspectos. Los establecimientos de salud también tienen políticas establecidas para establecer una base coherente en la gestión de la organización. A continuación se mostrarán las políticas bajo las que opera el Hospital de Especialidades de Portoviejo.

- ✓ Acceso universal: Está comprometido con el principio de acceso universal a la atención médica. Esto implica que todos los individuos, independientemente de su origen étnico, género, nivel socioeconómico o cualquier otra característica, deben tener igualdad de acceso a los servicios de salud.

- ✓ Prevención y promoción de la salud: Se centra en la prevención de enfermedades y la promoción de la salud en la población. Esto incluye campañas de vacunación, educación sobre hábitos saludables, detección temprana de enfermedades y control de factores de riesgo.
- ✓ Atención integral: Ofrecer una variedad de servicios médicos, desde atención primaria hasta servicios especializados. Esto permite abordar las necesidades médicas y de salud de manera integral.
- ✓ Equidad: Se esfuerzan por reducir las disparidades en la salud y garantizar que todas las personas tengan igualdad de oportunidades para acceder a servicios de salud de calidad.
- ✓ Eficiencia y calidad: Están comprometidos con la prestación de servicios eficientes y de alta calidad. Esto puede incluir la implementación de mejores prácticas clínicas, la capacitación continua del personal médico y la inversión en tecnología médica adecuada.
- ✓ Investigación y evaluación: Se basan en datos y evidencia científica, llevan a cabo investigaciones epidemiológicas y evaluaciones de programas para tomar decisiones informadas y mejorar la calidad de la atención.
- ✓ Respuesta a emergencias y desastres: Estar preparados para responder a emergencias y desastres, como epidemias, desastres naturales u otras situaciones que requieran una atención médica especializada y coordinada.

Bajo estas políticas se evaluará si se alinean con los objetivos generales de la organización, y se corroborará si siguen siendo relevantes para las operaciones actuales, de este modo se comprobará el cumplimiento el propósito de las políticas.

Tabla 2.

Evaluación de los objetivos generales de la organización

OBJETIVOS GENERALES	POLÍTICAS Y SU ALINEACIÓN RESPECTO A LOS OBJETIVOS		RELEVANCIA (ALTA, MEDIA Y BAJA)
	Acceso universal	SÍ	ALTA

Asumir el compromiso de mejorar de manera continua la calidad, accesibilidad y confiabilidad de sus procesos asistenciales para dar respuestas oportunas, eficaces, eficientes y humanizadas a toda persona que demande atención sanitaria. Con especial atención a la población más vulnerable (por cuestiones de enfermedad, sociales, de edad, de sexo, económicas, étnicas, etc.),	Prevención y promoción de la salud	SÍ	ALTA
	Atención integral	SÍ	ALTA
	Equidad	SÍ	ALTA
	Eficiencia y calidad	SÍ	ALTA
	Investigación y evaluación	SÍ	ALTA
	Respuesta a emergencias y desastres	SÍ	ALTA

Fuente: Elaboración propia (2023)

Con dicha evaluación se puede constatar que se está dando cumplimiento a los objetivos generales de la organización, puesto que las políticas bajo las que opera, trabajan por conseguir los objetivos planteados, que van desde la búsqueda de accesibilidad, confiabilidad de sus procesos, hasta la atención a poblaciones más vulnerables. También se observa que la relevancia del cumplimiento de dichas políticas es de vital importancia, por lo que se determinó "alta" como valor máximo en dicho aspecto.

Cláusula 6: Acciones para tratar los riesgos

Para realizar esta cláusula de la Norma ISO 27001 es necesario trabajar por fases, como se mencionaba anteriormente. Este aspecto comprenderá 3 fases importantes para estudiar qué acciones tomar para tratar los riesgos:

1. **Identificación de los riesgos existentes**

   Este es un proceso importante en la gestión de cualquier entidad, ya sea una organización, proyecto o cualquier otro tipo de actividad. Para llevar a cabo una identificación efectiva de los riesgos existentes,

   Como activo más valioso identificado se encuentra el *datacenter* de la organización, el cual constituye los registros médicos electrónicos que se encuentran en una instalación física diseñada para alojar servidores, sistemas de almacenamiento y otros componentes de tecnología de la información de pacientes.

   Éste está denominado como Departamento de tecnología, que cuenta con un sistema se llama SYS, que es el que realiza toda la gestión hospitalaria. En cuanto al sistema operativo, trabaja con Linux, y en la parte de seguridad trabaja con la herramienta de Cisco ASA.

En este *datacenter,* aunque utiliza firewall, ips y vpn, se pueden presentar múltiples riesgos en donde la seguridad de la información se ve afectada. Entre éstos se encuentran:

- Fallo de Energía
- Sobrecalentamiento
- Fallas en el Equipo
- Acceso no Autorizado
- Ataques Cibernéticos
- Desastres Naturales
- Fallo de Red
- Fallo de Equipos de Respaldo
- Errores Humanos

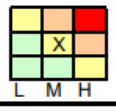
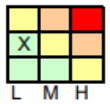
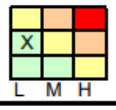
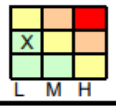
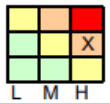
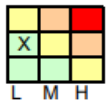
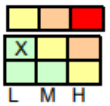
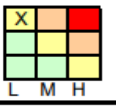
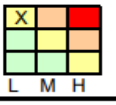
2. **Evaluación de riesgos con la metodología AMFE**

Una vez que los riesgos están identificados, es necesario evaluarlos más a fondo, por ello, en esta fase se trabajará conjuntamente con la metodología sistemática AMFE, la misma que es utilizada para identificar, evaluar y priorizar los posibles modos de falla en un producto, proceso o sistema.

A continuación, la evaluación aplicada:

Tabla 3.

Evaluación de riesgos con la metodología AMFE

Número de Riesgo	Amenaza /riesgo	Probabilidad	Severidad	Nivel	Matriz de riesgo
1	Fallo de energía	Medium	Serious	Medium	
		2	2		
2	Sobrecalentamiento	Low	Serious	Low	
		1	2		
3	Fallas en el equipo	Low	Serious	Low	
		1	2		
4	Acceso no autorizado	Low	Serious	Low	
		1	2		
5	Ataques cibernéticos	High	Serious	High	
		3	2		
6	Desastres naturales	Low	Serious	Low	
		1	2		
7	Fallo de red	Low	Serious	Low	
		1	2		
8	Fallo de equipo de respaldo	Low	Very Serious	Medium	
		1	3		
9	Errores humanos	Low	Very Serious	Medium	
		1	3		

Fuente: Elaboración propia (2023)

En dicha matriz se constató el nivel de riesgo (Low: bajo, Medium: medio, y High: alto) que contraía cada una de las amenazas presentadas, donde solo un riesgo presenta el nivel más alto, que es el de Ataque cibernético.

3. **Tratamiento de los riesgos con la Norma ISO 27002:2022**

En esta última fase, gracias a las 2 anteriores, se podrá finalmente definir el tratamiento que han de recibir los riesgos probables en la gestión de ciberseguridad del Hospital de Especialidades de Portoviejo, desarrollando estrategias de mitigación

y estableciendo, gracias a la Norma ISO 27002, un plan de acción para manejarlos de manera efectiva.

Cabe recalcar que, para la mitigación de estos riesgos, los hospitales deben implementar las medidas presentadas a continuación. Estos planes deben ser periódicamente revisados, probados y actualizados para garantizar la protección y la continuidad de las operaciones críticas del Hospital de Especialidades.

Tabla 4.

Tratamiento de los riesgos con la Norma ISO 27002:2022

No.	Amenaza/Riesgo	Acciones de mitigación
1	Fallo de energía	Utilizar sistemas de respaldo de energía
2	Sobrecalentamiento	Utilizar sistemas de enfriamiento redundantes
3	Fallas en el equipo	Controles de acceso físico y lógico
4	Acceso no autorizado	Verificar los accesos al sistema
5	Ataques cibernéticos	▪ Capacitarse en soluciones de seguridad cibernética ▪ Aplicar Firewalls y Antivirus ▪ Controles de acceso que limiten quién puede acceder a los sistemas ▪ Políticas de uso de dispositivos personales ▪ Evaluación de vulnerabilidades y pruebas de penetración
6	Desastres naturales	Realizar planes de continuidad y recuperación ante desastres.
7	Fallo de red	▪ Redundancia de enlaces ▪ Redundancia de conmutadores y enrutadores ▪ Ancho de banda suficiente ▪ Diversidad de rutas ▪ Diseñar aplicaciones y sistemas con tolerancia a fallos
8	Fallo de equipo de respaldo	▪ Mantenimiento regular ▪ Pruebas de carga y conmutación ▪ Monitorización remota ▪ Establecer planes de respuesta ante incidentes
9	Errores humanos	▪ Procedimientos documentados ▪ Acceso controlado ▪ Separación de funciones

		▪ Configuraciones automatizadas ▪ Cultura de responsabilidad notificando errores

Fuente: Elaboración propia (2023)

Cláusula 7: Soporte

Seguidamente se mostrará una lista de los recursos que han de emplearse para proteger la seguridad de la información de la organización en cuestión, mediante la aplicación de respectivos controles de la ISO 27001. Dando como resultado que el control A. 12 es el más empleado, siendo éste indispensable para la Seguridad de las operaciones.

Tabla 5.

Soporte. Recursos para proteger la seguridad de la información

No.	Recursos	Control
1	Inventario de activos	A.8.1.1
2	Gestión de usuarios	A.9.1
3	Gestión de trazas	A.12
4	Monitoreo de los sistemas	A.12.4.3
5	Protección contra programas maliciosos	A.12.2
6	Detección de vulnerabilidades y gestión de parches	A.12
7	Configuraciones de seguridad y revisión de políticas	A.5.1.2
8	Respaldo de información	A.12.3.1
9	Seguridad física	A.11.1.2
10	Gestión de incidentes	A.16

Fuente: Elaboración propia (2023)

Su tiempo de operación que inicia desde los 2 meses, y culmina desde los 18.

Fase N°2:

Para la elaboración del SOC como modelo de gestión de ciberseguridad para el Hospital de Especialidades de Portoviejo, Manabí – Ecuador, se establecieron 2 fases importantísimas en las que, a través de su respectiva evaluación con las normas ISO 27001 y 27002, se pudieron contemplar los resultados en la fase 2, que muestra la estructura del SOC, el mismo que brindará la capacidad de detectar, responder y mitigar amenazas cibernéticas de manera

efectiva, contribuyendo a mantener la integridad y la disponibilidad de los sistemas y la información crítica.

Las fases para la implementación del SOC para la gestión de ciberseguridad para el Hospital de Especialidades de Portoviejo son las siguientes:

- Evaluación (2-12 meses): Esta fase se desprende todo en CSIRT dependientes de lo establecido por el Ministerio de Salud Pública, en este punto se establece todo lo referente a la organización, sumado al órgano de gobierno y los requerimientos propios del diseño.

- Diseño (3-6 meses): consolidar un grupo de trabajo para construir el SOC, obteniendo el apoyo necesario de todos los miembros de la organización, estableciendo políticas viables en la organización.

- Capacidad operativa (10-18 meses): se trabaja en todo lo relacionado a las pruebas de las herramientas adquiridas parcialmente en todo lo relacionado con el funcionamiento, además el equipo básico que manipulará el SOC comenzará a trabajar con algunos de los servidores operativos.

- Capacidad operativa completa (a partir de 18 meses) El SOC está operativo, y puede ser empleado de forma adecuada por el equipo, puesto que estaría completo dentro del Hospital de Especialidades de Portoviejo.

Discusión

Establecer un diagnóstico respecto a un modelo de gestión es importante en diversos contextos, proporciona una base sólida para tomar decisiones informadas, diseñar estrategias efectivas y comprender la situación actual de un problema, situación o sistema. Altamirano (2019) menciona que un modelo desde el ámbito de ciberseguridad ofrece una visión integral de controles de seguridad de la información, considerando todos los controles automatizables y no automatizables. Este modelo no constituye una nueva propuesta de controles y procesos de gestión, sino que brinda un enfoque de automatización, integración y síntesis a las propuestas existentes, para disminuir la complejidad de la gestión y aumentar la efectividad de los controles de seguridad de la información en donde se encuentran activos valiosos para la organización, que no deberían ser vulnerados o atacados.

Ávalos et al (2023) con el planteamiento de un modelo de Gestión en Seguridad Digital para la aplicación en entidades peruanas del sector Público teniendo como marco los estándares y buenas prácticas reconocidas tales como ISO/IEC 27001:2013, fortaleció las capacidades de prevención y respuesta en seguridad digital en las instituciones públicas peruanas, además de permitir alinearse a la normativa vigente. Por otro lado, Chulde y Defaz (2021) en su diagnóstico realizado en el SOC como modelo de ciberseguridad IADI para el Sistema de Gestión Académica Ignug del Instituto Superior Tecnológico Yavirac, se pudo constatar que se solventa el problema de seguridad a largo plazo, por lo tanto, se presenta un plan a corto

plazo, considerando los activos críticos más relevantes para dicha organización, seleccionándolos de la matriz de calor de riesgos y proponiendo los controles más viables de corrección, recuperación, administración, eliminación y concienciación.

Ávila et al (2023) refiere, por su parte, que los controles de ciberseguridad desempeñan un papel fundamental en la protección de la información, sistemas y activos digitales de una organización frente a amenazas cibernéticas. La importancia de estos controles radica en la capacidad que tienen para mitigar riesgos, prevenir ataques y garantizar la confidencialidad, integridad y disponibilidad de la información. Sin la utilización de éstos sería más complicado establecer un Security Operations Center (SOC). Los controles de seguridad y el SOC como modelo de gestión están estrechamente relacionados en el ámbito de la ciberseguridad.

Conclusiones

Los modelos de gestión de ciberseguridad son de vital importancia para proteger los activos digitales y la información sensible de una organización. El Security Operations Center, como modelo crítico de la estrategia de ciberseguridad para el Hospital de Especialidades de Portoviejo, Manabí – Ecuador, permitió garantizar el cumplimiento normativo, y preservar la confianza de los pacientes, esto gracias al cumplimiento de las funciones del SOC, que abarcan desde diseño para monitoreo, detección, análisis y respuestas a amenazas, hasta tratar ataques cibernéticos en tiempo real. La evaluación de dicho modelo se realizó mediante las normas ISO 27001 y 27002, las cuales jugaron un papel fundamental en el diagnóstico realizado, trabajando con las principales cláusulas de la ISO 27001 para conocer cada aspecto de la organización, evaluando riesgos con la metodología AMFE, y tratándolos con la ISO 27002.

El diagnóstico permitió reconocer los riesgos mayormente presentados en el Hospital de Especialidades, así como también, los recursos que éste tiene con los que se pueden realizar óptimos controles que proporcionen pautas y recomendaciones detalladas para la implementación de medidas de seguridad en diferentes áreas. Es por ello que en la estructura del SOC se contemplan dichas medidas, que están reguladas por fases a seguir, garantizando que, si se da cumplimiento a este, se podrán detectar de forma temprana incidentes y ayudar a mantener la infraestructura digital segura y eficiente de la organización.

Referencias bibliográficas

Altamirano, D. M. A. (2019). Modelo para la gestión de la seguridad de la información y los riesgos asociados a su uso. *Avances*, 21(2), 248-263.

Ávalos Mendoza, M. R., Castilla Tasaico, J. L., y Gordillo López, C. P. (2023). Diseño de un modelo de gestión en seguridad digital para la aplicación en entidades peruanas del sector público.

Ávila, P. D. F., Chalán, A R., Figueras, G., y Ávila, M. (2022). Cybersecurity Policies for Network Switching Devices in Hospital Data Centers: A Case Study. ESPOCH Congresses: The Ecuadorian *Journal of S.T.E.A.M*, 2(2), 507–518. https://doi.org/10.18502/espoch.v2i2.11413

Becerril, A. A. (2021). Retos para la regulación jurídica de la Inteligencia Artificial en el ámbito de la Ciberseguridad. *Revista IUS*, 15(48), 9 – 34. https://doi.org/10.35487/rius.v15i48.2021.705

Briceño, E. V. (2021). *Seguridad de la Información:* Editorial Área de Innovación y Desarrollo, S.L. https://doi.org/:https://doi.org/10.17993/tics.2021.4

Bustamante, G. S., Valles, C. M. A., y Cuellar, R. I. E. (2021). Políticas basadas en la ISO 27001:2013 y su influencia en la gestión de seguridad de la información en municipalidades de Perú. *Enfoque UTE*, 12(2). https://doi.org/10.29019/enfoqueute.743

Casa, A. C. L., Gavilanez, M. L. G., Caiza, C. C. C., y Moreano, J. A. C. (2021). Importancia de políticas de seguridad Informática de acuerdo a las ISO 27001 para pequeñas y medianas empresas del Ecuador. *Ciencias de la Ingeniería y Aplicadas*, 5(2), 82-98.

Chulde, L. y Defaz, H. (2021). Diseño del Modelo de Ciberseguridad IADI para el Sistema de Gestión Académica Ignug del Instituto Superior Tecnológico Yavirac. *Ecuadorian Science Journal,* 5(3). https://doi.org/10.46480/esj.5.3.160

Deepesh, S. N. W. (2022). Integrated Network and Security Operation Center: A Systematic Analysis. *IEEE Access*, 10, 27881 – 27898. 10.1109/ACCESS.2022.3157738

Huilcapi, S. I., y Gallegos, D. N. (2020). Importancia del diagnóstico situacional de la empresa. *Revista Espacios,* 41 (40).

Lema, S. P. R. (2019). Implementación de análisis modal de fallos y efectos (AMFE). *Tecnología: glosas de innovación aplicadas a la pyme*, 8(1), 64-75.

Morales, M. N. Z. (2019). Modelo de gestión de riesgos de seguridad de la información: Una revisión del estado del arte. *Revista Peruana de Computación y Sistemas*, 2(2), 43-60.

Patiño, S., Caicedo, A., y Guaña, E. R. (2019). Modelo de evaluación del Dominio Control de Acceso de la norma ISO 27002 aplicado al proceso de Gestión de Bases de Datos. *Revista Ibérica de Sistemas e Tecnologías de Informação*, 22, 230-241.

Pérez, M. J. (2019). La protección de los datos personales en el registro de dispositivos de almacenamiento masivo de información. *Revista Brasileira de Direito Processual Penal*, 5(3), 1297-1330. https://www.redalyc.org/articulo.oa?id=673971417006

Ramos, M. R. G., Cahuaya. A. R., y Llanqui. A. R. R. (2023). Política informática y la gestión de la seguridad de la información en base a la norma ISO 27001. *Innovación y Software,* [s. l.], 4 (1), 96–106. https://doi.org/10.48168/innosoft.s11.a57

Rodríguez, G. R. D. L. C., Fernández, R. A. M., y De Los Santos, A. C. M. (2023). Seguridad de la información en el comercio electrónico basado en ISO 27001: Una revisión sistemática. *Innovación y Software,* 4(1), 219-236. https://doi.org/10.48168/innosoft.s11.a79

Torres, A. M. G. (2019). Análisis FODA. http://biblioteca.udgvirtual.udg.mx/jspui/bitstream/123456789/3016/1/An%C3%A1lisis_FODA.pdf

Vielberth, M., Böhm, F., Fichtinger, I., & Pernul. G. (2020) Security Operations Center: A Systematic Study and Open Challenges. *IEEE Access,* 8, 227756-227779. https://doi.org/10.1109/ACCESS.2020.3045514

Conflicto de intereses:
Los autores declaran que no existe conflicto de interés posible.
Financiamiento:
No existió asistencia financiera de partes externas al presente artículo.
Agradecimiento:
N/A
Nota:
El artículo no es producto de una publicación anterior.