REVISTA ELECTRÓNICA SOBRE TECNOLOGÍA, EDUCACIÓN Y SOCIEDAD
ISSN: 2448 - 6493
CTES

Artículos científicos

Gestión de la Seguridad de la Información para el área de Estudios Avanzados ubicada en el Estado de México

Information Security Management for the Advanced Studies area located in the State of Mexico

Sarai Salgado Montero
Universidad Autónoma del Estado de México, México
sarai.salgadom23@outlook.com
https://orcid.org/0009-0000-3752-6020

Araceli Romero Romero*
Universidad Autónoma del Estado de México, México
aromeroruaemex@gmail.com
https://orcid.org/0000-0002-0328-0525

Resumen

Las tecnologías de la información en los últimos años han tenido un crecimiento exponencial, estas se han vuelto indispensables tanto para las organizaciones como para las personas. La información, la cual, en la actualidad es común que este contenida en equipos tecnológicos, se ha convertido en un activo medular en las organizaciones para el cumplimiento de sus objetivos, de ahí el motivo de protegerla. A pesar de lo mencionado, un gran porcentaje de las organizaciones, aun no dimensionan la importancia de la implementación de controles para la seguridad de la información, como las soluciones técnicas y la concientización de las personas y prestan atención cuando son vulnerados, por tanto, toman acciones de forma reactiva y no preventiva. Algunos riesgos en la seguridad de la información son: fuga de información, ransomware, ingeniería social, virus, etc., lo cual puede tener como consecuencia, interrupción en las actividades diarias, pérdidas monetarias, problemas de reputación, entre otros. El sector Educativo, no es menos importante y mucho menos está exento de ser víctima de ataques o de tener vulnerabilidades en la seguridad de la información, por lo tanto, es necesario incluir un programa para fortalecer la seguridad de la información en sus procesos.

En consecuencia, el objetivo de este artículo es resaltar la importancia de la seguridad de la información y de fortalecer el área de Estudios Avanzados a través de una propuesta de desarrollo de un marco de gestión de la seguridad de la información, utilizando mejores prácticas que existen en el mercado.

Palabras clave: *Gestión de la Seguridad de la Información, Estudios Avanzados, mejores prácticas.*

REVISTA ELECTRÓNICA SOBRE TECNOLOGÍA, EDUCACIÓN Y SOCIEDAD
ISSN: 2448 - 6493
CTES

Abstract

Information technologies in recent years have had exponential growth; they have become indispensable for both organizations and people. Information, which is currently contained in technological equipment, has become a core asset in organizations to achieve their objectives, hence the reason for protecting it. Despite the above, a large percentage of organizations still do not appreciate the importance of implementing controls for information security, such as technical solutions and people's awareness, and pay attention when they are violated, therefore, they take actions reactively and not preventively. Some risks in information security are: information leaks, ransomware, social engineering, viruses, etc., which can result in interruption in daily activities, monetary losses, reputation problems, among others. The Educational sector is no less important and much less exempt from being a victim of attacks or having vulnerabilities in information security, therefore, it is necessary to include a program to strengthen information security in its processes.

Consequently, the objective of this article is to highlight the importance of information security and to strengthen the area of Advanced Studies through a proposal for the development of an information security management framework, using best practices that exist. in the market.

Keywords: *Information Security Management, Advanced Studies, best practices.*

Resumo

As tecnologias de informação nos últimos anos tiveram um crescimento exponencial, tornaram-se indispensáveis tanto para as organizações como para as pessoas. A informação, que atualmente se encontra contida em equipamentos tecnológicos, tornou-se um ativo fundamental nas organizações para atingirem os seus objetivos, daí a razão para a protegerem. Apesar do exposto, um grande percentual de organizações ainda não valoriza a importância da implementação de controles para segurança da informação, como soluções técnicas e conscientização das pessoas, e prestam atenção quando eles são violados, portanto, tomam ações de forma reativa e não preventiva. Alguns riscos na segurança da informação são: vazamento de informações, ransomware, engenharia social, vírus, etc., que podem resultar em interrupção das atividades diárias, perdas monetárias, problemas de reputação, entre outros. O setor Educacional não é menos importante e muito menos isento de ser vítima de ataques ou de ter vulnerabilidades na segurança da informação, portanto, é necessário incluir um programa para fortalecer a segurança da informação nos seus processos.

Consequentemente, o objetivo deste artigo é destacar a importância da segurança da informação e fortalecer a área de Estudos Avançados através de uma proposta para o desenvolvimento de um framework de gestão da segurança da informação, utilizando as melhores práticas existentes. no mercado.

Palavras-chave: *Gestão de Segurança da Informação, Estudos Avançados, melhores práticas.*

Fecha Recepción: Junio 2023 **Fecha Aceptación:** Diciembre 2023

Introducción

Desde la antigüedad, diversos pueblos en el mundo fueron incluyendo métodos para cuidar su información, por ejemplo, en Mesopotamia en sus escritos utilizaban la técnica de sustitución y solo las personas que tenían el código podían leerlo; en la antigua Grecia utilizaban una técnica de criptografía llamada escítala; en el siglo XVIII inventaron la Rueda de Jefferson, utilizada para cifrar mensajes secretos; en el siglo XX la máquina Enigma que era un dispositivo utilizado para cifrar mensajes secretos; por mencionar algunos. (*Pasado, presente y futuro de la seguridad de la información | Empresas | INCIBE*, s/f)

Actualmente la información es un activo de valor incalculable que ayuda a las organizaciones a cumplir con sus objetivos; es considerada el oro de la se seguridad informática, dado que es lo que se debe proteger. (Romero Castro et al., 2018, p. 14)

La seguridad de la información es un reto muy importante tanto para el gobierno, empresas y las personas, de acuerdo con un reporte de vulnerabilidades, en 2023 hubo un pico histórico de 29,065 vulnerabilidades, lo cual es un 15% más de las reportadas en 2022.(*Cuáles son las vulnerabilidades más relevantes detectadas en 2023*, s/f)

Es un hecho que la tecnología está avanzando a pasos agigantados, los ataques informáticos han venido creciendo, pero también es importante mencionar que algunas organizaciones no han dado la importancia a la implementación de medidas básicas de seguridad. Según ENISA (The European Union Agency for Cybersecurity) menciona que hay una característica común de los ciberataques modernos, y esta es, que en la mayoría de ellos con controles básicos de seguridad informática como mantener el software actualizado, el uso contraseñas seguras, cifrado de datos confidenciales y copias de seguridad en la nube serían suficientes para que los ordenadores no sean víctimas de esos incidentes. Un ejemplo es el ataque de tipo Ransomware WannaCry el cual fue denominado “homenaje a la negligencia” donde se vieron afectados más de 400,000 equipos en más de 150 países por la falta de actualización de software. (European Union Agency for Cybersecurity., 2023, p. 4) Al hablar de Ransomware, ESET (Enjoy Safer Technology) compañía de seguridad informática menciona, que en el año 2023 México fue uno de los países más golbeados de Latinoamerica, con más de mil empresas afectadas, entre los rubros gubernamental, farmaceutico, financiero, entro otras. (*Los ataques ransomware en America Latina que marcaron el 2023*, s/f)

Otro claro ejemplo es la CVE-2017-11882, que es una vulnerabilidad de Microsoft 2017 explotada en correos electrónicos, la cual existe desde el año 2017 y que aun teniendo al alcance los parches de seguridad, en el año 2022 y 2023 se encontró dentro del top de las más explotadas. (*CVE-2017-11882*, s/f)

Es evidente que debemos poner atención en el aseguramiento técnico de la infraestructura y sevicios, pero es impresindible tomar en cuenta la cocientización y la formación de las personas, un ejemplo es un informe realizado por Nordpass en 2023, en el cuál menciona que los usuarios se siguen aferrando a contraseñas débiles y predecibles, por mencionar algunas, a nivel global se encuentra la contraseña “123456” con un recuento de 4,524,867, la contraseña “admin” con un recuento de 4,008.850, la contraseña “12345678” con un recuento de 1,371,152. (*Contraseñas más utilizadas en 2023*, s/f)

Considerando la importancia de la seguridad de la información en las organizaciones, el objetivo general de esta investigación es el Desarrollo de un Marco de Gestión de la Seguridad de la información a través de la aplicación de buenas prácticas en el departamento de Estudios Avanzados ubicada en el Estado de México. Los objetivos específicos para lograrlo es 1) Elaborar el estado del arte acerca de la Gestión de la Seguridad de la Información. 2) Analizar el estado actual de la Jefatura de Estudios Avanzados en el tema de Seguridad de la Información. 3) Diagnosticar a través de una evaluación de riesgos en el tema de seguridad de la información del área de Estudios Avanzados. 4) Determinar las herramientas necesarias que permitan conformar un Marco de Gestión de la Seguridad de la Información en la institución. 5) Establecer un Marco de Gestión de la seguridad de la información a través de la aplicación de buenas prácticas en una Jefatura de Estudios Avanzados ubicada en el Estado de México.

La investigación fue realizada en una Jefatura de Estudios Avanzados ubicada en el Estado de México, cuyo principal objetivo es promover y difundir estudios a nivel especialidad, maestría y doctorado, en las ciencias Administrativas, Contables e Informáticas, contribuyendo a la formación de capital humano y la generación de investigación aplicada; se encuentra conformada por personal administrativo, profesores, alumnos y personal de TI.

Seguridad de la Información

La Seguridad de la Información, según la ISO/IEC (2016) es definida como “aquellos procesos, buenas prácticas y metodologías que busquen proteger la información y los sistemas de información del acceso, uso, divulgación, interrupción, modificación o destrucción no autorizado”, el nivel de seguridad debe relacionarse con el valor del activo. (Vega, Edgar, 2021, pp. 9–10)

Las dimensiones de la seguridad de la información o pilares como también se le conocen son los siguientes: la disponibilidad, la integridad y la confidencialidad. (Vega, Edgar, 2021, p. 6). La disponibilidad se refiere a poder utilizar los servicios cada vez que sea necesario, la carencia de ésta es la interrupción del servicio; la integridad es mantener la información completa, exacta, es decir, que no haya sido manipulada, que este corrupta o incompleta; la confidencialidad, nos habla de que la información debe llegar solamente a las personas autorizadas. (Amutio, Miguel Angel et al., 2012a, p. 9)

Algunas buenas prácticas en Seguridad de la Información.

MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) versión 3 es una metodología de análisis y gestión de riesgos, elaborada por el Consejo Superior de Administración Electrónica del Gobierno de España, es de carácter público, por lo tanto, puede ser utilizada libremente. Los objetivos de esta metodología son: 1. Concientizar a la alta dirección de las organizaciones de la existencia de riesgos y la necesidad de gestionarlos; 2. Brindar un método sistemático para analizar los riesgos que implican el uso de las TIC. 3. Ayudar al tratamiento oportuno de riesgos y mantenerlos bajo control. 4. Preparar a la Organización para procesos de auditorías, certificaciones, etc. Esta

metodología consta de los siguientes libros: Libro I: Método, Libro II: Catálogo de Elementos, Libro III: Guía de Técnicas. (*PAe - MAGERIT v.3*, s/f)

INCIBE (Instituto Nacional de Ciberseguridad), es una institución española cuyo objetivo es elevar la ciberseguridad apoyando a los organismos gubernamentales, empresas privadas y a la ciudadanía. INCIBE realiza investigaciones en temas de ciberseguridad, promueve eventos de ciberseguridad, brinda herramientas, materiales, proporciona capacitaciones, cuenta con apoyo telefónico para la ciudadanía.(*INCIBE | INCIBE*, s/f)

La Norma ISO 27001:2013 proporciona una guia para la construcción de un Sistema de Gestión de la Seguridad de la información. Los elementos básicos del estándar son: las cláusulas de requisitos y los controles de seguridad. La norma ISO 27001 en su Anexo A muestra una lista de 114 controles de seguridad, estos se encuentran agrupados en 35 objetivos de control, y están considerados en 14 dominios. (*¿Cuál es la idea central de aplicar ISO 27001?*, s/f)

COBIT 5 es un marco de referencia, el cual contiene "un conjunto de propósitos definidos y controles de TI que tiene como principio la implementación de un marco para el gobierno y gestión de TI". Dentro de los documentos de la familia COBIT, se encuentra "COBIT 5 para seguridad de la información" este se especializa en la seguridad de la información, en el se plantea la seguridad de la información como una disciplina transversal. (*COBIT para la seguridad en las organizaciones*, s/f)

Materiales y métodos

El enfoque elegido para esta investigación es el cuantitativo, el cual es utilizado para consolidar las creencias, establecer patrones de comportamiento de una población y probar teorías. (Hernández Sampieri & Fernandez-Collado, 2014, p. 14). El alcance de la investigación es el descriptivo, cuyo objetivo es explorar y detallar las propiedades y características inherentes a un fenómeno determinado (Hernández Sampieri & Fernandez-Collado, 2014, pp. 92–93)

Las técnicas de recolección de datos que se utilizaron fueron la revisión bibliográfica, y la recolección de datos por medio de instrumentos de medición aplicados en el lugar de estudio. En cuanto a la población se tomo una muestra de 35 personas.

La dimensiones e indicadores para el diagnóstico se muestran a continuación en la tabla 1:

Tabla1. Dimensiones e indicadores para diagnosticar la seguridad de la información.

Dimensiones	Indicadores
Dimensión 1 Grado de conocimiento de los activos esenciales (Información y Servicios)	**Indicador 1** Grado de conocimiento acerca de los activos referentes a los datos e información de valor en una Jefatura de Estudios Avanzados.
	Indicador 2 Grado de conocimiento acerca de los activos referentes a los servicios e infraestructura de valor en una Jefatura de Estudios Avanzados
Dimensión 2 Grado de conocimiento en seguridad de la información en las personas	**Indicador 1** Grado de conocimiento en la aplicación de seguridad de la información con base a los estándares ISO 27001 e ISO 17769 en una Jefatura de Estudios Avanzados
	Indicador 2 Grado de Conocimiento de la Cultura de la Seguridad de la Información en una Jefatura de Estudios Avanzados

Fuente: Elaboración propia 2023

Para el Análisis del estado actual en el tema de seguridad de la información de la Jefatura de Estudios Avanzados, se realizaron los siguientes instrumentos:

Instrumento 1. Identificación de activos de información. Este instrumento ayuda a conocer los activos de valor referentes a la información que se maneja en el lugar de estudio. Los reactivos de este cuestionario fueron elaborados basándose en la Metodología MAGERIT v3 en el libro 2 Catálogo de elementos. Este instrumento fue dirigido al personal administrativo de la Jefatura de Estudios Avanzados.

Instrumento 2. Identificación de activos de infraestructura y servicios. Este instrumento nos ayuda a conocer los activos referentes a la infraestructura y servicios con los que cuenta el lugar de estudio. Los reactivos de este cuestionario fueron elaborados basándose en la Metodología MAGERIT v3 en el libro 2 Catálogo de elementos. Este instrumento fue dirigido al personal de Tecnologías de la Información de la Jefatura de Estudios Avanzados.

Instrumento 3. Grado de conocimiento en seguridad de la información en las personas. Este instrumento nos ayuda a conocer el grado de conocimiento tanto en la aplicación de controles de seguridad de la información como en la cultura de la seguridad de la información en el lugar de estudio. Contiene reactivos manejados en la Tesis de Maestría "Plan Estratégico para Fortalecer la Cultura de la Seguridad de la Información a través de buenas prácticas en un Organismo Público en el Estado de México". (Salgado, 2022) mismos que hacen referencia al Estándar ISO 27001 e ISO 17769 en cuanto a controles de seguridad y el trabajo de Alnatheer (2012) concerniente a la cultura de la seguridad de la información.

Para esta investigación se realizó una adecuación para los siguientes perfiles: personal administrativo, profesores y alumnos.

Cada instrumento se aplicó de acuerdo con el perfil para el que fue diseñado, la información fue analizada con el software estadístico IBM SPSS Statics 21.

A continuación, se expondrán algunos de los de los datos más relevantes del análisis realizado:

Con el Instrumento "Identificación de activos de información", se abordaron varios puntos, tales como el manejo de aplicaciones o sistemas de información, la identificación de propietarios de activos de información, la clasificación de la información, la presencia de información valiosa, la gestión de datos personales, así como el cumplimiento de políticas de información, entre otros aspectos relevantes.

Una pregunta central formulada que se realizó, la cual se relaciona con el núcleo de la investigación y la razón de ser del presente proyecto, es si en el área existe información importante que requiera protección, y la respuesta unánime del personal que maneja los procesos en el área afirman que en el área existe información de valor. Asimismo, también mencionan que se resguardan datos personales.

En el tema de clasificación de la información, el área maneja una clasificación de información en sus procesos, lo cual es una gran ventaja, porque además de identificar de manera eficaz los activos de información, es un punto clave al momento de generar estrategias y crear controles para preservar la seguridad de la información.

Acerca de la Criptografía, el 75% de las personas no utiliza algún mecanismo criptográfico, sin embargo, el 75% de las personas mencionan que consideran que sería útil utilizar un mecanismo Criptográfico para cierta información considerada como crítica.

En relación con la información de los sistemas de información, la totalidad del personal maneja aplicaciones o sistemas de información para realizar sus actividades, concerniente al tema de propietarios de activos de información, el área es dueña y responsable de la información que genera en los sistemas, pero no son administradores de los aplicativos e infraestructura donde están contenidos.

Los contenedores donde se resguarda la información del área de investigación y Estudios Avanzados son: PCs, nube y discos externos.

En cuanto a medios electrónicos con los que el personal realiza sus labores se encuentran: PCs, memorias USB, almacenamiento de red y CD-ROM; y en lo que se refiere a medios "no electrónicos" guardan información en material impreso.

Por último, los servicios que ocupa el personal para realizar su trabajo, son los siguiente: servicio de internet, correo electrónico, almacenamiento de archivos y transferencia de archivos.

Con el Instrumento "Identificación de activos de infraestructura y servicios", se identificó la siguiente información: equipos donde se encuentra información sensible, hardware con el que se realiza el intercambio y almacenamiento de información (disco duro, san, nube, usb, etc.), equipos de red para servicios (modem, switches, teléfonos IP, etc.), servicios (internet, correo electrónico, transferencia de archivos, etc.), telecomunicaciones (red de internet, red de datos, etc.), equipos de usuarios (laptop, impresoras, escáner) e instalaciones.

Con el Instrumento "Grado de conocimiento en seguridad de la información en las personas" con respecto al indicador Grado de conocimiento en la aplicación de seguridad de la información con base a los estándares ISO 27001 e ISO 17769 se evaluaron temas como capacitación y concienciación en las personas, políticas de las seguridad de la información, política de conducta o ética, política de información confidencial, políticas de control de acceso, política de intercambio de información, respaldos de información, contraseñas seguras, conocimiento acerca de ataques a correo electrónico, ataques homográficos, ransomware, virus, spyware, robo de identidad, privacidad en redes sociales, conceptos básicos de seguridad de la información (disponibilidad, integridad, confidencialidad), roles y responsabilidades, entre otras. A continuación, se mencionan algunos de los resultados de los ítems:

En cuanto a si han tenido una capacitación formal en seguridad de la información el 25% contesto que nunca, 34% indicó que raramente, el 22% ocasionalmente. Se pregunto la frecuencia con la que se promueve la concientización de la seguridad de la información a través de elementos como avisos, posters, trípticos, entre otros y el 43% indicó que raramente el 36% comento que ocasionalmente, el 4.5% nunca. Se consultó si la institución ofrece una buena formación de seguridad de la información y educación, el 13.6% dijo que nunca, el 29.5% casi nunca, el 34% dijo que a veces.

En el tema de políticas de seguridad de la información, se preguntó si conocían si existe una política de la seguridad de la información en la institución el 11% comento que no, el 40.9% dijo que poco sabe. Se indagó si se realizan los esfuerzos necesarios para educar a los miembros sobre nuevas políticas de seguridad, el 18% dijo que nunca, el 29% casi nunca, el 34% a veces. En cuanto al conocimiento de una política de control de acceso el 22% comenta que no conoce, el 25% raramente, el 34% ocasionalmente. Acerca del manejo de una política para el intercambio de información el 29% comenta que no la maneja, otro 29% casi nunca, un 22% a veces.

En cuanto a la aplicación de técnicas para la seguridad de la información se preguntó la frecuencia con la que aplican estándares de seguridad de la información, el 22% dijo que nunca, otro 22% mencionó que raramente. Otra pregunta fue la frecuencia con la que realizan un respaldo de su información más importante, el 6% dijo que nunca lo hace, el 22.7% raramente, el 29% ocasionalmente. En cuanto a las contraseñas en el equipo el 63% dijo que siempre manejaba, el 15% con frecuencia, pero el 29% conoce poco acerca de las características de una contraseña segura, el 11% a menudo deja sus contraseñas en papel, en un post-it o archivos de computadora, el 15% con frecuencia lo hace, el 15% a veces.. El 79% no comparte contraseñas con otras personas, el 43% raramente cambia las contraseñas que le fueron asignadas por su institución, el 20% nunca y el 27% ocasionalmente. En cuanto a conceptos más actuales se preguntó que tanto conocen el concepto de ingeniería social, el 40% contesto que poco, el 27% nada. También se preguntó el conocimiento que tienen de las estafas que se realizan en internet el 45% dijo que poco y el 2% nada. En cuanto a correo electrónico se preguntó la frecuencia con la que han recibido un correo electrónico fraudulento, el 18% comenta que muy frecuentemente, el 27% frecuentemente, el 22% ocasionalmente. En cuanto al conocimiento de la activación de la verificación en dos pasos en sus cuentas de correo electrónico el 13% no tiene conocimiento, el 38% tiene poco

conocimiento. Se pregunto el conocimiento que tenían acerca de los ataques homográficos es decir páginas donde el dominio de la página falsa se escribe similar o visualmente igual a la página original, el 25% no tiene conocimiento, el 45% poco. El 11% considera que no tienen conocimientos para poder identificar un correo apócrifo, el 34% tienen poco conocimiento. El 52% no conoce el termino Ransomware, el 27% tiene poco conocimiento. El 54% no tiene conocimiento sobre técnicas para evitar el Ransomware, el 25% conoce poco. El 31% dijo que se no sentía a salvo de ser víctima de un ataque de Ransomware, el 43% dijo que poco. El 40% comentó que no tiene conocimiento acerca del spyware keylogger, el 31% tiene poco conocimiento. El 41% tienen poco conocimiento acerca de cómo se infectan los dispositivos de virus, 4% no saben.

A continuación, se muestran algunos resultados del indicador Conocimiento de la Cultura de la Seguridad de la información, con este indicador se analizan los factores que conforman e influyen en la Cultura de la Seguridad de la Información. Con respecto a la responsabilidad el 36% muy frecuentemente se hace responsable de los resultados de sus decisiones y acciones que toman en cuanto a la seguridad de la información el 40.9% frecuentemente. El 31% raramente es consciente de las responsabilidades para la seguridad de la información el 27% ocasionalmente. El 29% raramente esta consiente de los riesgos de no seguir las políticas de la seguridad de la información, el 25% ocasionalmente y el 11% nunca. Al preguntar acerca de la alta dirección el 31% nos dice que está a veces percibe la seguridad de la información como una parte importante, el 15% menciona que casi nunca y el 4% nunca. El 27% piensa que la alta dirección a veces considera que la seguridad de la información es una prioridad en la institución, el 15% casi nunca y el 6% dice que nunca. El 34% considera que a veces las palabras y acciones de la alta dirección demuestran que la seguridad de la información es una prioridad el 15% cas nunca y el 6% nunca. El 29% dice que la alta dirección a veces brinda un apoyo fuerte y consistente a un programa de seguridad de la información, el 34% casi nunca y el 6% nunca. En el área de conocimiento el 31% comenta que ocasionalmente se le dan a conocer las políticas de la seguridad de la información en su institución, el 25% comenta que raramente y el 11% nunca. En cuanto a la adherencia a las políticas de seguridad de la información, el 40% comenta que ocasionalmente sus compañeros de alrededor se adhieren a las políticas de seguridad de la información el 13% dice que raramente y el 11% nunca. En el tema capacitación, el 40% nunca ha sido requerido para asistir a un curso de capacitación acerca de controles de la seguridad de la información, el 31% raramente, el 18% ocasionalmente.

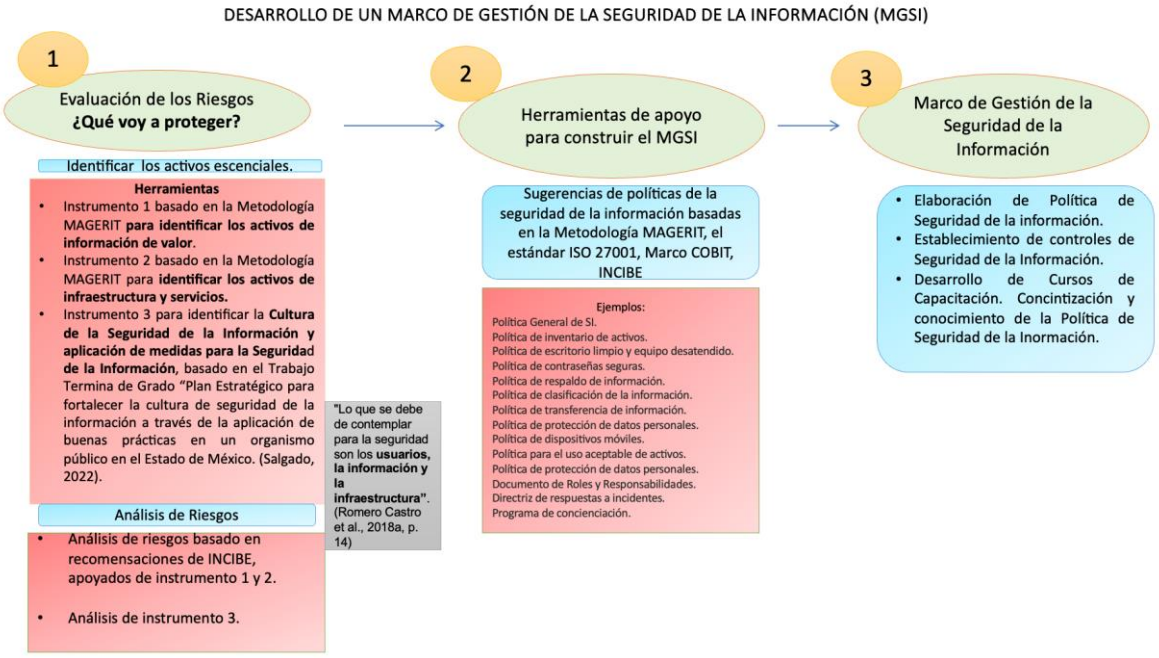
Resultados

De acuerdo con los resultados obtenidos en el análisis, se identificó que existe información de valor que es necesario proteger, además se identificaron los activos tecnológicos que la contienen, servicios, equipos auxiliares, etc., se analizó un elemento muy importante que son las personas, donde nos muestra que existe una amplía área de oportunidad para que las personas generen conocimientos acerca de cómo proteger la información de la institución y su información personal, además de generar una cultura de la seguridad de la información positiva.

Por esta razón, en este artículo se propone el desarrollo de un Marco de Gestión de la seguridad de la información, para fortalecer la seguridad de la información, mediante controles para salvaguardar los datos que se manejan, los equipos que lo contienen y las personas que los utilizan.

Mediante la revisión bibliográfica y el análisis realizado, se generó la propuesta que se presenta en la figura 1.

Figura 1. Pasos para el desarrollo de un Marco de Gestión de la Seguridad de la Información.



Fuente: Elaboración propia 2023

El *primero paso* para el Desarrollo de un MGSI es la *Evaluación de Riesgos*, aquí es el momento en el cual se identifica que se va a proteger. Los tres instrumentos mencionados anteriormente en el análisis de esta investigación tuvieron un doble propósito, el primero es analizar el estado de la seguridad de la información, y el segundo es recabar información para la elaboración de la Evaluación de Riesgos.

La evaluación de riesgos fue efectuada, basándose en las recomendaciones de INCIBE (*¡Fácil y sencillo! Análisis de riesgos en 6 pasos | Empresas | INCIBE*, s/f); para esto, se realizó un catálogo de los activos de información, infraestructura y servicios, que fueron obtenidos de los instrumentos 1 y 2; posteriormente fue elaborado un catálogo de las amenazas basado en la Metodología MAGERIT Libro II Catálogo de Elementos (Amutio, Miguel Angel et al., 2012b), incluyendo el nombre de la amenaza, el tipo de activo (hardware, software, media, etc.), la descripción, la dimensión (integridad, disponibilidad, confidencialidad), los datos agregados al catálogo fueron en relación a los activos con los que cuenta la institución, un ejemplo se muestra en la tabla 2.

Tabla 2. Ejemplo de organización del catálogo de amenazas basado en la Metodología MAGERIT Libro II

Amenaza	Tipo de activo	Descripción	Dimensión
Fuego	HW, MEDIA, AUX,L	incendios: posibilidad de que el fuego acabe con recursos del sistema.	Disponibilidad
Daños por agua	HW, MEDIA, AUX,L	inundaciones: posibilidad de que el agua acabe con recursos del sistema.	Disponibilidad
Desastre Natural	HW, MEDIA, AUX,L	otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras	Disponibilidad
Fallos en los equipos o programas	HW, MEDIA, SW, AUX	avería del hardware, falla de funcionamiento del hardware	Disponibilidad
Corte del suministro eléctrico	HW, MEDIA, AUX	Fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.	Disponibilidad

Fuente: Elaboración propia 2023

Para el cálculo del valor del riesgo, se emparejo cada activo con las amenazas que le corresponden y por cada amenaza se calculó el riesgo, para este cálculo se utilizó la propuesta generada por INCIBE, utilizando la formula RIESGO = PROBABILIDAD x IMAPACTO, para calcular el valor de la probabilidad se tomaron en cuenta los valores de la tabla 3 y para calcular el valor del impacto, se tomaron los valores de la tabla 4. En la tabla 5 se muestra un ejemplo del cálculo de riesgo.

Tabla 3. Datos para calcular la probabilidad de un riesgo

Cálculo de la probabilidad		
Cualitativo	Cuantitativo	Descripción
Baja	1	La amenaza se materializa a lo sumo una vez cada año
Media	2	La amenaza se materializa a lo sumo una vez cada mes
Alta	3	La amenaza se materializa a lo sumo una vez cada semana

Fuente: Tomado de INCIBE (*¡Fácil y sencillo! Análisis de riesgos en 6 pasos | Empresas | INCIBE*, s/f)

Tabla 4. Datos para calcular impacto

Tabla para el cálculo de impacto		
Cualitativo	Cuantitativo	Descripción
Bajo	1	El daño derivado de la materialización de la amenaza no tiene consecuencias relevantes para la organización
Medio	2	El daño derivado de la materialización de la amenaza tiene consecuencias reseñables para la organización
Alto	3	El daño derivado de la materialización de la amenaza no tiene consecuencias graves reseñables para la organización

Fuente: Tomado de INCIBE (*¡Fácil y sencillo! Análisis de riesgos en 6 pasos | Empresas | INCIBE*, s/f)

Tabla 5. Ejemplo de cálculo de Riesgo

No.	Activo	Amenaza	Probabilidad	Impacto	Riesgo
1	4 EQUIPOS DE CÓMPUTO CON …	Fuego	1	3	3
2	4 EQUIPOS DE CÓMPUTO CON …	Daños por agua	1	3	3
3	4 EQUIPOS DE CÓMPUTO CON …	Desastre Natural	1	3	3
4	4 EQUIPOS DE CÓMPUTO CON …	Fallos en los equipos o programas	2	2	4
5	4 EQUIPOS DE CÓMPUTO CON …	Corte del suministro eléctrico	1	2	2

Fuente: Elaboración propia 2023

Para el análisis de la seguridad de la información en las personas, se tomaron en cuenta los resultados de la aplicación del instrumento 3 *Grado de conocimiento en seguridad de la información en las personas*, que fueron mostrados en el apartado de este artículo Materiales y métodos.

Con la Información de la Evaluación de Riesgos que se realizó, se logra identificar los activos en los tres rubros: información, infraestructura y personas, a su vez se reconocen las amenazas y riesgos, además de la prioridad para integrar controles de seguridad.

El *segundo paso* consiste en buscar las herramientas necesarias que nos van a ayudar a construir la política para la seguridad de la información, la elección de buenas prácticas para implantar controles de seguridad de la información y herramientas como apoyo para un programa de concienciación y de educación en seguridad de la información. El material que fue revisado fue la norma ISO 27001:2013, la Metodología MAGERIT v3, el marco COBIT 5 para la seguridad de la información y la página de INCIBE.

A continuación, se presentan algunos controles y políticas sugeridos para establecer en la organización, esto se realizó con el sustento del estándar ISO 27001:2013, en su

apartado Objetivos de Control y Controles, con MAGERIT versión 3.0 Libro II Catálogo de elementos en su apartado Salvaguardas y COBIT 5 para seguridad de la información.

Tabla 6. Controles de seguridad sugeridos

Controles	**Acciones**
Protección de los equipos de HW	Plan de actualización y mantenimiento de equipos
	Perfiles de seguridad en los equipos (configurar cuenta de administrador y cuenta de usuario)
	Agregar equipos a active directory
	Configuración de copias de seguridad
	Revisión de fallos de corriente (revisión de No-break)
Gestión de activos	Identificar todos los activos, actualizar inventario
	Asignar un propietario a los activos
Protección de los elementos auxiliares	Revisión de Instalación
	Suministro eléctrico (revisión de No-break)
	Protección del cableado
Red	Segmentación de red
Control de acceso	Configuración de permisos en active directory
	Elaboración y firma carta de responsabilidad de usuarios y contraseñas asignadas
	Configuración de control de contraseñas (Configuración en active directory)
	Configuración de usuario administrador y usuario final en los equipos
Controles contra código malicioso	Instalación de antivirus
	Instalación de IDS
Gestion de incidentes de seguridad	Procedimiento para notificación de eventos de seguridad de la información
	Procedimiento para la evaluación y decisión sobre los eventos de seguridad de la inforamción
	Documentación de evidencias
Control de los accesos físicos	Control de acceso a oficinas donde se encuentra información de valor

Fuente: Elaboración propia 2023

Tabla 7. Políticas de seguridad sugeridas

Políticas
Política General de Seguridad de la información
Política de actualización y mantenimeinto de equipos
Politica de pantalla limpia y medios desmontables
Política para la asignación de equipos o terminación de vida (borrado seguro)
Política de respaldos
Política para salida de equipos del edificio
Política de manipulacipon de soportes (limpieza de soportes de información, borrado seguro o destrucción de información cuando ya no vayan a ser necesarios, protección contra accesos no autorizados)
Política de protección criptográfica de contenido de información en soportes de información
Política de uso aceptable de activos
Política de termino de devolución de activos al finalizar empleo
Política de contraseñas seguras
Política de copias de seguridad
Política de instalación de software por usuarios
Política de control de accesos (Revocación de permisos al finalizar empleo, equipos, sistemas, servicios; carta de responsabilidad de usuarios y contraseñas asignadas
Política para el intercambio de información (Firmar acuerdos de confidencialidad o no revelación)
Política de acceso a la red
Política de uso de correo electrónico
Política de uso de conducta ética
*Deben ser revisada y aprobada por la alta dirección

Fuente: Elaboración propia 2023

Una parte imprescindible en la seguridad de la información son las personas, para ello se debe formarlas y concientizarlas, con apoyo de los resultados obtenidos hasta el momento con del instrumento que mide la dimensión “Grado de conocimiento en seguridad de la información en las personas”, con el soporte COBIT 5 para seguridad de la información y las herramientas brindadas en INCIBE se determinaron temas y herramientas, como primera base, a continuación, se mencionan algunas:

Temas	Herramientas
• Capacitación para el conocimiento de las políticas de seguridad de la información • Terminología básica de la seguridad • Seguridad en correo electrónico (ataques homográficos, activación de verificación en dos pasos, fraudes por corrreo electrónico, etc.) • Ingenieria social • Suplantación de identidad • Tipos de virus • Responsabilidad con la seguridad de la información	• Videos tutoriales • Realizar infografías de temas de seguridad de la información • Establecimiento de fondos de pantalla por medio de active directory • Uso de herramientas como Gophish • Difusión por medio de redes sociales desde la cuenta oficial de la institución acerca de temas como políticas de seguridad, temas actuales de seguridad, términos, consejos, etc. • Colocar posters • Capacitación personal • Apoyo de herramientas disponibles en www.incibe.es

Discusión

Mediante la presente investigación es clara la necesidad de las organizaciones de incorporar controles de seguridad de la información, además de formar y concientizar a las personas que son las que hacen uso de las tecnologías de la información y de la información. Para esto la opción que se presenta es el desarrollo de un Marco de Gestión de la Seguridad de la Información. Para lograr esto se realizó un análisis a través de los distintos instrumentos mencionados y el uso de metodologías, a través de los cuales se dio un diagnóstico del estado actual de la seguridad de la información en cuanto a información, infraestructura y personas; a través de estándares y buenas prácticas mencionadas en el trabajo se seleccionaron los controles y políticas necesarias para conformar el marco. Es importante mencionar que una pieza clave para este tipo de proyectos es el apoyo y concientización de la alta dirección. También es importante contar con personal que tenga un perfil informático

Para generar seguridad en nuestras organizaciones, es importante en primer momento concientizarnos sobre el tema de comenzar a trabajar en ella, además de saber que existen metodológicas, estándares, buenas prácticas, que pueden ayudar a lograrlo, si bien no se puede lograr la totalidad de la seguridad es importante ir cerrando la brecha entre vulnerabilidades y amenazas para lograr un riesgo aceptable.

Conclusión

La Seguridad de la información es un tema importante, de interés, que también debe ser gestionada por los organismos del sector educativo, ya que como cualquier empresa cuentan con activos de información de valor, infraestructura, servicios y personas, y no está exenta de vulnerabilidades, amenazas y riesgos, por lo tanto es necesario la implantación de controles de seguridad de la información, generación de políticas y esfuerzos en concientización y educación en seguridad de la información en las personas.

El desarrollo de un Marco de Gestión de la Seguridad de la Información es un instrumento que va a ayudar a fortalecer la seguridad de la información en las organizaciones, en este presente trabajo de investigación, se da una propuesta de como generarlo, se citan buenas prácticas como la Metodología MAGERIT v3, información de INCIBE, la norma ISO 27001, COBIT 5 para la seguridad de la información, de las cuales podemos tomar información valiosa sin casarnos específicamente con alguna.

Uno de los objetivos principales fue beneficiar a la institución donde se realizó la investigación, pero también es ayudar a las personas a conocer acerca del tema y al personal en Tecnologías de la Información que tenga intenciones de implementar controles de seguridad en sus organizaciones.

Futuras investigaciones

En trabajos posteriores se recomienda un seguimiento detallado de la instalación de los controles y aplicación de las políticas posteriormente para evaluar y analizar el nivel éxito, para esto se propone incluir temas como desarrollar auditorías internas o externas, ciclo de vida de las políticas y mejora continua del marco de gestión de la seguridad de la información.

Agradecimientos

Se agradece al Consejo Mexiquense de Ciencia y Tecnología (COMECYT), por el apoyo económico a través del programa “Investigadoras e Investigadores COMECYT EDOMÉX”.

Referencias

Alnatheer, Mohammed A. (2012). *Understanding and Measuring Information Security Culture in Developing Countries: Case of Saudi Arabia*.

Amutio, Miguel Angel, Candau, Javier, & Mañas, José Antonio. (2012a). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método*. Ministerio de Hacienda y Administraciones Públicas. https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Amutio, Miguel Angel, Candau, Javier, & Mañas, José Antonio. (2012b). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos*. Ministerio de Hacienda y Administraciones Públicas. https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

COBIT para la seguridad en las organizaciones. (s/f). Recuperado el 2 de noviembre de 2023, de https://www.welivesecurity.com/la-es/2015/08/04/practicas-cobit-seguridad-organizaciones/

Contraseñas más utilizadas en 2023: N vistazo a la seguridad digital en América Latina. (s/f). Recuperado el 6 de febrero de 2024, de https://www.welivesecurity.com/es/contrasenas/contrasenas-mas-utilizadas-2023-seguridad-digital-latinoamerica/

¿Cuál es la idea central de aplicar ISO 27001? (s/f). Recuperado el 10 de noviembre de 2023, de https://www.welivesecurity.com/la-es/2015/07/02/idea-central-aplicar-iso-27001/

Cuáles son las vulnerabilidades más relevantes detectadas en 2023. (s/f). Recuperado el 26 de febrero de 2024, de https://www.welivesecurity.com/es/seguridad-corporativa/vulnerabilidades-mas-relevantes-2023/

CVE-2017-11882: La vulnerabilidad más explotada en correos con malware en LATAM. (s/f). Recuperado el 6 de febrero de 2024, de https://www.welivesecurity.com/es/concientizacion/vulnerabilidad-cve-2017-11882-correos-maliciosos-america-latina/

European Union Agency for Cybersecurity. (2023). *Cybersecurity education initiatives in the EU Member States: December 2022.* Publications Office. https://data.europa.eu/doi/10.2824/486119

¡Fácil y sencillo! Análisis de riesgos en 6 pasos | Empresas | INCIBE. (s/f). Recuperado el 1 de octubre de 2023, de https://www.incibe.es/empresas/blog/analisis-riesgos-pasos-sencillo

Hernández Sampieri, R., & Fernandez-Collado, C. F. (2014). *Metodología de la investigación* (P. Baptista Lucio, Ed.; Sexta edición). McGraw-Hill Education.

INCIBE | INCIBE. (s/f). Recuperado el 2 de agosto de 2023, de https://www.incibe.es/

Los ataques ransomware en America Latina que marcaron el 2023. (s/f). Recuperado el 5 de febrero de 2024, de https://www.welivesecurity.com/es/ransomware/ataques-ransomware-america-latina-marcaron-2023/

ISACA (2012) COBIT 5 para seguridad de la Información.

ISO27001:2013 "Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de la seguridad de la información – Requisitos"

PAe - MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. (s/f). Recuperado el 27 de octubre de 2023, de https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Pasado, presente y futuro de la seguridad de la información | Empresas | INCIBE. (s/f). Recuperado el 17 de febrero de 2024, de https://www.incibe.es/empresas/blog/pasado-presente-y-futuro-de-la-seguridad-de-la-informacion

Romero Castro, M. I., Figueroa Morán, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzúles, G. R., Álava Mero, C. J., Murillo Quimiz, Á. L., & Castillo Merino, M. A. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades*. Editorial Científica 3Ciencias.

Salgado, S. (2022). *Plan estratégico para fortalecer la cultura de seguridad de la información a través de la aplicación de buenas prácticas en un organismo público en el Estado de México*.

Vega, Edgar. (2021). *Seguridad de la Información* (Primera edición). Área de Innovación y Desarrollo,S.L.