PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, CASO DE ESTUDIO: GOBIERNO PROVINCIAL DEL CAÑAR

INFORMATION SECURITY MANAGEMENT PLAN, CASE STUDY: CAÑAR PROVINCIAL GOVERNMENT

https://doi.org/10.5281/zenodo.4142114

AUTORES: Carlos Lema Velecela[1]*

Juan Pablo Cuenca[2]

DIRECCIÓN PARA CORRESPONDENCIA: carlos.lemavelecela@outlook.com

Fecha de recepción: 30 / 04 / 2020

Fecha de aceptación: 08 / 09 / 2020

RESUMEN

El presente trabajo de investigación tuvo como objetivo elaborar un plan de gestión de seguridad de la información para los activos de seguridad del gobierno provincial del Cañar, dedicado a la implementación de proyectos y servicios, con el fin de cubrir los requerimientos de la provincia. El enfoque aplicado es inductivo-deductivo, apoyado en la investigación bibliográfica y descriptiva, junto al método analítico; las técnicas para la recolección de la información fueron: cuestionarios, listas de verificación y entrevistas con los servidores públicos del departamento de Tecnologías de la Información y Comunicación (TIC). Los resultados de la investigación demostraron los riesgos potenciales contra los activos de seguridad de la prefectura del Cañar, siendo la falta de procedimientos de seguridad y la poca importancia de capacitación en temas de ciberseguridad a los servidores que se encuentran laborando en la organización, por lo que es fundamental desarrollar políticas de seguridad de la información, enfocando sus

[1]*Estudiante de Maestría en Tecnologías de la Información. Universidad Católica de Cuenca, carlos.lemavelecela@outlook.com

[2]Magister en Sistemas de Información Gerencial, docente de la Unidad Académica de Tecnologías de la Información y Comunicación, Universidad Católica de Cuenca, jcuenca@ucacue.edu.ec

esfuerzos en el área de la ciberseguridad, precisamente en esta era en la que todas las empresas buscan la innovación tecnológica y por ende el crecimiento de los sistemas de información y servicios a través de internet.

Palabras clave: Activos, amenazas, ciberseguridad, riesgos, vulnerabilidades

ABSTRACT

The purpose of this research work is to prepare an information security management plan for the security assets of the Cañar provincial government, dedicated to the implementation of projects and services, in order to meet the province's requirements. The applied approach is inductive-deductive, supported by descriptive and bibliographic research, together with the analytical method; The techniques for collecting the information were: questionnaires, checklists, and interviews with public servants from the Information and Communication Technologies (ICT) department. The results of the investigation demonstrated the potential risks against the security assets of the Cañar prefecture, being the lack of security procedures and the little importance of training in cybersecurity issues to the servers who are working in the organization, therefore that it is essential to develop information security policies, focusing their efforts on the area of cybersecurity, precisely in this era in which all companies seek technological innovation and therefore the growth of information systems and services through the internet.

Keywords: Assets, threats, cybersecurity, risks, vulnerabilities

INTRODUCCIÓN

Actualmente las organizaciones del mundo usan masivamente sistemas de información, para la automatización, transformación y digitalización de procesos como: planificación, organización, producción, entre otros, mismos que se generan a diario en los departamentos de la organización. No obstante, la digitalización viene por añadidura con inconvenientes relacionados con seguridad de la información, por lo cual, las organizaciones deben implementar políticas, para protección de los datos que antes se almacenaban de manera física y hoy en dispositivos digitales. De esa forma resguardar la información y evitar daños, robo o incluso destrucción de su activo, puesto que un sistema casi siempre es vulnerado con la finalidad de extraer datos valiosos para la organización, entre ellos: credenciales de acceso, infiltraciones en modo espía, instalación de scripts, entre otros. El

empleo de políticas de seguridad ayuda a controlar muchos incidentes, de lo contrario, la organización será un blanco fácil para recibir ciberataques según medios digitales recopilados por el autor.

El artículo tiene como objetivo, describir un plan de gestión de seguridad de la información, con la guía de normas y estrategias para mitigar posibles amenazas en el Gobierno Provincial del Cañar.

En los Estados Unidos de América, los incidentes en los sistemas de información no son desconocidos para el mundo, debido al robo de identidad, terrorismo y el uso de la información con fines criminales, por eso, durante el período del presidente Obama la seguridad de la información fue prioridad, ya que es un problema global y no solo de países desarrollados, la importancia de la seguridad de la información debe ser una preocupación para educadores y líderes de los países, con un plan de formación para los profesionales y personas en general en materia de seguridad para preservar los datos en los sistemas de información (White; Hewitt & Kruck, 2017).

En un plan de seguridad de la información, indistintamente de la actividad de la organización, es primordial la incorporación de procesos, tecnología, y sobre todo el personal interno y externo, ya que empleados actuales y antiguos son considerados como amenaza inicial de los incidentes de seguridad. Por otra parte, la aplicación de políticas y reglamentos de seguridad no es una labor fácil ya que cambiar una cultura organizacional con una cultura propicia de seguridad de la información requiere mucha capacitación y trabajo en conjunto (Da Veiga & Martins, 2015). Adicionalmente, para corroborar lo antes mencionado, una encuesta realizada por (PricewaterhouseCoopers, 2018) ubico que el 47% de los ciberataques en organizaciones de España son realizados por empleados o ex empleados, proveedores el 40,7%, 17,5% por activistas y ciberactivistas, de igual manera, altos directivos de las organizaciones consideran pérdidas de hasta 4,8 millones de dólares anuales al percibir un ciberataque.

Desde otra perspectiva (Hartley et al., 2017) mencionan que, la ciberseguridad en Texas durante los últimos años ha tomado un papel importante para las organizaciones internacionales, así como nacionales y locales. Y que, las tecnologías de información y comunicación han facilitado la interacción entre las personas, pero no todos conocen del

peligro existente en las redes de comunicación y dispositivos que se usa diariamente. Por otra parte, las amenazas contra los principios de la seguridad: confidencialidad, integridad, disponibilidad (CIA, por sus siglas en inglés) se convierten en una preocupación creciente. Pese a lo cual, para controlar los delitos cibernéticos, es necesario realizar ataques controlados contra las vulnerabilidades existentes en las organizaciones, donde se emplea herramientas de software para, analizar los riesgos, las amenazas, vulnerabilidad y las posibles salvaguardas.

En países sudamericanos la incorporación de las tecnologías a todos los aspectos de la vida y actividades cotidianas de las personas, ha aumentado los delitos informáticos, con tareas específicas, robar información y causar daño a datos acumulados en sistemas informáticos. En consecuencia, las organizaciones y profesionales del área deben garantizar la seguridad de los datos, siendo una tarea demasiado importante y además de mucha preocupación para las organizaciones e instituciones públicas y privadas, con el propósito de plantear estrategias de defensa y no perder datos indispensables para el funcionamiento de los sistemas de información. Según el autor, el uso de simuladores y pruebas de penetración basados en modelos preconfigurados, es una forma de encontrar riesgos de seguridad, a fin de invertir demasiado dinero y no alcanzar niveles de seguridad óptimos (Édison et al., 2017).

Según (Gualotuña, Hugo & Quilumbaqui, 2016)en su trabajo de investigación para el sistema nacional de nivelación y admisión (SNNA), exponen que los procesos de negocios de instituciones privadas y públicas se localizan en sistemas de información, como es el caso, el registro para exámenes de admisión a universidades del estado ecuatoriano, por consiguiente, la información es almacenada en dispositivos electrónicos y móviles, siendo estos datos accedidos solo por personas autorizadas, también mencionan algunos incidentes de seguridad, uno de ellos en el Hospital de Ottawa en Canadá, el cual fue afectado con ransomware, desde otro ángulo, en Ecuador, el registro de 366 títulos universitarios en la base de datos de la SENESCYT, y además de la reciente filtración de las pruebas ser bachiller y datos de millones de ecuatorianos de acuerdo al sitio oficial de (ultimas noticias, 2019), por lo tanto, ninguna organización está libre de percibir un ciberataque contra sus sistemas de información.

Las empresas creen estar protegidas al aplicar barreras de protección en sus dispositivos finales, y desarrollar políticas de ciberseguridad de manera empírica, por la experticia de los profesionales que laboran en el área de las tecnologías como es el caso de la organización que se estudia, pero las cosas no son tan sencillas, es necesario un estudio profundo y profesionales expertos en el área de la ciberseguridad para ayudar al descubrimiento de las amenazas existentes, ya sean internas o externas.

El propósito de la investigación es analizar los riesgos existentes contra los activos de seguridad del Gobierno Provincial del Cañar y diseñar algunas salvaguardas que se podrían aplicar a futuro para contrarrestar las amenazas.

METODOLOGÍA

Para el desarrollo de este trabajo, se empleó el método inductivo-deductivo, con un enfoque cuantitativo para la investigación descriptiva, bibliográfica y analítica, empleando un diseño no experimental de corte retrospectivo, con la finalidad de cumplir con el objetivo general de esta investigación.

1. Revisión del estado del arte.
2. Diagnóstico situacional de la empresa, mediante la aplicación de técnicas y métodos de recolección de información.
3. Guía de la metodología MAGERIT y la norma ISO/IEC 27001 para análisis de riesgos.
4. Aplicación de entrevistas y cuestionarios para crear el inventario de activos de seguridad de la empresa.
5. Análisis de las posibles amenazas de los activos de seguridad, según la norma ISO/IEC 27005 y MAGERIT.
6. Categorización de las vulnerabilidades, según la norma ISO/IEC 27005 y pérdidas económicas de los riesgos posibles.
7. Análisis y calificación de los riesgos.
8. Desarrollo de un plan de gestión de seguridad, conforme a la familia de normas ISO/IEC 27000 y MAGERIT para los riesgos encontrados en la empresa.

RESULTADOS

Según la metodología (MAGERIT v3, 2012) y las normas de la familia ISO/IEC 2700 (Lewis, 2018), para iniciar con el desarrollo del trabajo de investigación se realiza un inventario de los activos del Gobierno Provincial del Cañar como se detalla en la tabla 1.

Tabla 1. Inventario de activos de seguridad.

[D] Datos / Información		**[COM] Redes de comunicación**	
Código	**Activo**	**Código**	**Activo**
D001	Copias de respaldo	C001	Red telefónica
D002	Ficheros	C002	Red inalámbrica
D003	Datos de prueba	C003	Red LAN
[S]Servicios		C004	Internet
S001	Correo electrónico	C005	VPN
S002	Página web	**[SI] Soporte de información**	
[SW] Aplicaciones (software)		SI001	Discos duros
SW001	Servidor de correo electrónico	SI002	Memorias extraibles
SW002	Sistema de gestión de base de datos	SI003	Material impreso
SW003	Paquete de office	**[AUX] Equipamiento auxiliar**	
SW004	Antivirus	A001	UPS
SW005	Sistemas operativos	A002	Equipo de climatización
SW006	Gestor de máquinas virtuales	A003	cableado eléctrico
[H] Equpamiento informático (hardware)		A004	Fibra óptica
H001	PCs	A005	Cableado
H002	Periféricos	A006	Rack
H003	Discos duros	A007	Armarios
H004	Impresora multifunción	**[L]Instalaciones**	
H005	Router core	L001	Departamento de TIC
H006	Switch	**[P]Personal**	
H007	Firewall	P001	4 servidores públicos
H008	Servidor	**[K] Claves criptográficas**	
H009	Telefonos fijos	K001	Claves de autenticación
H010	Router (modem)		

Fuente: (Spanish Higher Council for Government, 2012)

Elaboración: El autor

Para la valoración de los activos de seguridad más relevantes de la tabla 1, se consideran las siguientes dimensiones: Confidencialidad (C), Integridad (I), Disponibilidad (D), Trazabilidad (T), Autenticación (A) con una puntuación de 1 (daño mínimo) a 5 (daño mayor) y la justificación para la valoración en la tabla 2.

Tabla 2. Valoración de los activos de seguridad más relevantes.

Valoración [D] Datos / Información			
Activo/Cod	***dimensión***	***valor***	***justificación***
D003	***[I]***	4	No puede ser modificado por nadie más que la persona encargada.
D003	***[C]***	3	Debe venir de una fuente confiable (no copiado de internet).
D003	***[T]***	5	Si fue ejecutado antes de ser revisado.
Valoración [K] Claves criptográficas			
K001	***[C]***	5	Los accesos deben darse por personal unicamente de la organización.
K001	***[D]***	4	El acceso debe estar disponible solo en horarios de oficina.
K001	***[A]***	5	Las claves de acceso deben ser solo de personal autorizado.
K001	***[T]***	5	Si los sistemas de acceso quedan abiertos en horario de oficina.
Valoración [SW] Aplicaciones (software)			
SW001	***[C]***	4	Permitir el acceso al servidor de usuarios confiables y autenticados.
SW001	***[D]***	3	Disponible siempre en horarios de trabajo o si es el caso 24/7.
SW001	***[A]***	5	Permitir el acceso al servidor solo de usuarios con credenciales asignadas y autorizadas.
SW001	***[T]***	5	Si los puertos no utilizados estan abiertos siempre.
SW002	***[I]***	4	Los datos almacenados no deberán ser modificados sin su debida autorización.
SW002	***[C]***	3	Los datos que se almacenan deben ser solo de fuentes autorizadas.
SW002	***[T]***	3	Si no fue diseñado para el crecimiento organizacional.
Valoración [HW] Equipamiento informático (hardware)			
H005	***[D]***	5	El dispositivo deber estar configurado sin errores y listo para desempeñar sus actividades.
H005	***[A]***	4	Para acceder al dispositivo y su software se debe contar con credenciales de acceso autorizado.
H005	***[T]***	3	Si el dispositivo no tiene una fuente de alimentación constante.
H005	***[I]***	5	Los datos de configuración del dispositivo no puede ser modificado.
H005	***[C]***	4	Debe ser configurado por personal autorizado.
H007	***[D]***	5	Los dispositivos deben trabajar en todo momento.
H007	***[A]***	4	Para acceder a los dispositivos, credenciales de acceso.
H007	***[T]***	5	Si los dispositivos no son cofigurados adecuadamente, ACLs.
H007	***[I]***	5	Los datos de configuración no pueden ser modificados
H007	***[C]***	4	La configuración es modificada o actualizada por personal autorizado.
Valoración [COM] Redes de comunicaciones			
C004	***[D]***	4	Muchos sistemas trabajan con acceso a la web. Debería no tener cortes
C004	***[C]***	4	El proveedor del servicio de internet debe ser confiable.
C004	***[T]***	3	Si el servicio no tiene el ancho de banda necesario para la organización
Valoración [SI] Soportes de información			
SI002	***[I]***	4	La información no será modificada o alterada.
SI002	***[T]***	5	Si el dispositivo fue modificado con un virus
SI002	***[C]***	3	Conocer la procedencia del dispositivo.
Valoración [P] Personal			
P001	***[I]***	4	La administración debe ser integra con el fin de llevar todos los procesos de seguridad con transparencia.
P001	***[C]***	4	La información que maneja no puede ser expuesto a ningún otro empleado de la organización.
P001	***[T]***	5	Si no se firma un contrato de confidencialidad.

Fuente: (Spanish Higher Council for Government, 2012).

Elaboración: El autor

Una vez obtenido la valoración, lo siguiente es el análisis de amenazas y vulnerabilidades contra los activos, teniendo en cuenta los parámetros de *Riesgo, Impacto y Probabilidad* de que un factor se materialice, además de la pérdida económica relacionada al grupo de activos, así como se detalla en la siguiente tabla.

Tabla 3. Amenazas, vulnerabilidades y pérdidas económicas.

Activos	R	I	P	Amenaza	Vulnerabilidad	Pérdida
[D] Datos / Información	5	10	3	Desastres Naturales y tecnológicos	Conflictos civiles / exceso de radiación	300 mil
	3	6	5	Errores de usuario	Contraseñas muy debiles o vinculadas a sus datos personales	
	5	6	4	Errores de administrador	Administradores poco experimentados y muy confiados	
	8	8	6	Propagación de software dañino	Uso de técnicas de hacking por ejemplo phishing	
	2	6	2	Alteración accidental de la información	Incapacidad de los usuarios para realizar tareas específicas	
[S] Servicios	2	8	6	Acceso no autorizado	Desbordamiento de búfer o exploits	
	6	6	5	Daños físicos o lógicos	Políticas de seguridad deficientes e inexistentes	
[SW] Aplicaciones (software)	1	3	2	Vulnerabilaciones de las aplicaciones	Vulnerabilidad de denegación de servicios	100 mil
	2	6	5	Errores en el mantenimiento de equipos	Insuficiencia de pruebas en el software	
	3	4	3	Suplantación de identidad	Uso de técnicas de spoofing / sitios web engañosos	
	2	4	3	Abuso de privilegios de acceso	No control de cierre de sesión	
	5	8	6	Mal uso de equipos	Manuales de usuarios erroneos o inexistentes	
[HW] Hardware	5	10	6	Incendio	Provacados o instalaciones ineficientes	200 mil
	4	5	6	Suspensión del suministro eléctrico	Infraestructura impertinente / pagos impuntuales	
	2	3	3	Humedad o temperaturas inadecudas	Ubicación del deparmento de TICs impropio	
	2	2	2	Extravío de equipos	Protección física muy convencionales	
[SI] Soporte de la información	4	5	6	Accesos no controlados	Codigo malicios en el controlador del dispositivo USB	
	5	3	3	Sobremanipulación de los dispositivos	Perdida, daños por agua, luz, humedad, robo	
[COM] Redes de comunciación	4	4	4	Errores en los servicios de comunicación	Fallas en los equipos de telecomunicaciones	250 mil
	3	2	3	Agotamiento de recursos	Ataque de denegación de servicio DOS	
	3	8	6	Falta de análisis en tráfico de red	Espionaje remoto por usuarios externos	
	4	5	3	Interceptación de información	Técnicas de captación de informaciòn	
	6	8	5	Información perdida	Ingreso de personas no autorizadas	
	2	3	4	Ausencia de pruebas de funcionamiento	Falta de asesoramiento	
	5	8	6	Arquitectura insegura	Instalaciones y equipamiento de seguridad no adecuado	
[P]Personal	6	7	5	Ingeniería social	Falta de capacitaciones sobre temas de seguridad	50 mil
	5	8	6	Extorsión	Políticas organizacionales no presentes	
	2	3	3	Personal no comprometido	Ausencia en sus puestos de trabajo	
	5	6	5	Deficiencias en la organización	Procedimientos de contratación ineficientes	
	4	5	6		Personal de limpieza no es supervisado	

Fuente: (ISO Standars, 1991) y (Spanish Higher Council for Government, 2012)

Elaboración: El autor

La siguiente tabla detalla los riesgos evaluados, con una criticidad de: alta, media y baja según la calificación de los empleados de la organización, para obtener un margen de probabilidad e impacto del riesgo.

Tabla 4. Riesgos actuales contras los activos de seguridad.

Tipificación Riesgo	Riesgo evaluado	Observación	Criticidad	P	I	Voto	Calificación (TIC)	Calificación (Admin)	Calificación (Usuario)
R1	No controlar el tráfico y paquetes compartidos a tráves de la red.	No supervisar y realizar pruebas de seguridad periodicamente.	Alto	3.7	4.3	Voto impacto	4.0	5.0	4.0
						Voto probabilidad	4.0	3.0	4.0
R2	Demasiada confianza por los empleados de la organización.	El personal cree que toda la infraestructura del departamento es segura y que no son vulnerables.	Medio	3.3	3.3	Voto impacto	3.0	4.0	3.0
						Voto probabilidad	3.0	3.0	4.0
R3	No disponer de políticas o estandares de seguridad de la información.	Se debería contar con un plan o deseño de un manual de seguridad de la información básico para proteger los activos de la organización.	Alto	5.0	3.3	Voto impacto	3.0	3.0	4.0
						Voto probabilidad	5.0	5.0	5.0
R4	Seguridad cibernetica y falta de procesos para respuesta a incedentes.	Procesos no definidos, no disponer una bitacora de incidentes suscitados en la organización.	Alto	4.0	4.0	Voto impacto	4.0	5.0	3.0
						Voto probabilidad	4.0	4.0	4.0
R5	Sensibles a ingeniería social.	La confianza del personal los hace vulnerables a sufrir ataques contra su integridad.	Alto	3.3	4.7	Voto impacto	5.0	5.0	4.0
						Voto probabilidad	4.0	3.0	3.0
R6	Falta de procedimientos de cifrado y cambio continuo de contraseñas.	El uso de contraseñas cifradas seguras para el acceso a los sistemas de información es clave para la seguridad.	Medio	3.3	3.7	Voto impacto	4.0	3.0	4.0
						Voto probabilidad	4.0	3.0	3.0
R7	Falta de pruebas de seguridad en los sistemas de información.	Al no tener politicas o cronograma de actividades, no se realizan pruebas de seguridad.	Medio	4.0	3.7	Voto impacto	4.0	3.0	4.0
						Voto probabilidad	5.0	4.0	3.0
R8	Instalaciones deficientes de cableado y equipos informáticos.	Los responsables prodrían no tener la experiencia y capacitación necesaria para la administración del departamento.	Alto	5.0	4.7	Voto impacto	5.0	5.0	4.0
						Voto probabilidad	5.0	5.0	5.0
R9	Cambios continuos en reglamentos internos.	La leyes internas cambian para acoplarse a las leyes nacionales.	Alto	5.0	4.0	Voto impacto	3.0	5.0	4.0
						Voto probabilidad	5.0	5.0	5.0
R10	Contratación de personal no capacitado para el área.	Puestos de trabajo innecesarios	Medio	4.0	3.3	Voto impacto	3.0	4.0	3.0
						Voto probabilidad	4.0	4.0	4.0

Fuente: (Spanish Higher Council for Government, 2012)

Elaboración: El autor

Seguidamente se realiza algunas *salvaguardas* del plan de gestión de seguridad para los *riesgos* de la tabla 4, donde las sugerencias pueden llegar a implementarse con el fin de evitar y disminuir el nivel de riesgo presente en la organización, se toma como referencia las normas (ISO Standars, 1991) y MAGERIT**.**

R1

1. Control de acceso de usuarios a la navegación por internet.
2. Acceso de usuarios a los servicios de la organización únicamente a quienes hayan sido autorizados.
3. Monitorización constante de los servicios en red.
4. Monitoreo de la red inalámbrica y creación de usuarios y roles según su responsabilidad y uso.

R2

1. Crear políticas de responsabilidad para que los usuarios aseguren su información.
2. Creación de controles de acceso físico con lectores de huella, llenado de formularios.

R3

1. Desarrollo de políticas para el uso de dispositivos extraíbles.
2. Políticas para el uso de dispositivos móviles.
3. Creación de un marco referencial de políticas según los servicios de la organización.
4. Auditoría externa de seguridad de la información.

R4

1. Creación de un plan de contingencia en caso de existir algún desastre natural o tecnológico.
2. Políticas para evitar el uso de software no autorizado.
3. Políticas para copias de seguridad donde se definan los parámetros de seguridad y el mantenimiento periódico de los respaldos.

R5

1. Desarrollo de políticas para que los puestos de trabajo y monitores estén limpios de material impreso o reseña de algún dato sensible.
2. Políticas de uso de las instalaciones del departamento.

3. Capacitación constante en temas de ciberseguridad.

R6

1. Usar algoritmos de encriptación (SHA, AES, 3DES) para guardar datos relevantes como: contraseñas, datos de acceso a servidores, claves privadas, etc.

R8

1. Ubicación de los equipos sensibles, es decir software y hardware que almacenan datos de usuarios de la organización en un lugar no visible para los demás.
2. Reinstalación del cableado siguiendo los consejos de la norma ISO 11801.

R10

1. Crear políticas para contratación de empleados y servidores del departamento con la intención de asegurar responsabilidades y aptitudes para el rol que están siendo contratados.

La implementación de un SGSI (Sistema de Gestión de Seguridad de la Información) por el momento no sería muy imprescindible, pero sí realizar algunas políticas de seguridad de la información bajo un marco de referencia como la ISO/IEC 27002 que recomienda buenas prácticas para la mitigación de riesgos y posibles ciberataques, además tener en cuenta que, "Si tu empresa gasta más en café que en seguridad TI, serás hackeado. Es más, merecerás ser hackeado" (Raymond).

DISCUSIÓN

A partir de los resultados encontrados, se concuerda que, estándares internacionales como COBIT 5 e ISO/IEC 27000 proporcionan lineamientos con buenas prácticas para la implementación de mejoras, soluciones y proyectos vinculados con la protección de los datos, ya que sin duda los sistemas de información son parte integral del negocio. No obstante, están expuestos a riesgos y la creciente necesidad de crear un marco para el Gobierno de seguridad de la información, mismo que podría aplicarse en cualquier empresa pública o privada (Ochoa Arévalo, 2015). Así pues, párrafos anteriores guardan relación con el autor, donde se indica que las organizaciones de forma global están encaminadas al uso masivo del Internet y están llevando sus procesos masivamente a la web.

(Tejena-Macías, 2018) describe que el uso de una metodología para el análisis de riesgos tiene un mismo objetivo, metodologías como: OCTAVE, MEHARI, MAGERIT, CRAMM,

EBIOS y NIST SP 800-30 contienen características propias y diferentes para las empresas en cada sector. Conforme a lo mencionado por el autor estás metodologías son similares, sin embargo, MAGERIT, es una metodología que se acopla satisfactoriamente a organizaciones gubernamentales, siendo una de ellas la Prefectura del Cañar, sus tareas paso a paso bien identificadas, facilitan el análisis de riesgos en los tres principios de la CIA. Por lo que mucho depende el tipo de organización a la que se va implementar una de las metodologías antes mencionadas.

Además, la metodología MAGERIT tiene su herramienta de evaluación de riesgos llamada PILAR, para el análisis y gestión de los riesgos de los sistemas de información, incluso ayuda a la identificación del nivel de madurez de los procesos de seguridad implementados en la organización con algunas gráficas para mayor facilidad de visibilidad a la hora de identificar si es necesario la implementación de procedimientos de seguridad (Molina Miranda, 2017). Contrastando al autor, MAGERIT es una metodología amigable y fácil de implementarla, pero el uso del software PILAR es recomendable usar cuando existen muchos procedimientos de seguridad, mismos que podrían confundir al momento de realizar tabulaciones y evaluaciones cuantitativas de los riesgos.

Para implementar un SGSI es vital el análisis, evaluación y tratamiento de los riesgos relacionados con la seguridad de la información, de igual forma los requisitos presentes en las normas ISO/IEC 27000 para garantizar los niveles aceptables de seguridad además de la documentación para los controles y posibles nuevos riesgos de la organización (Valencia-Duque & Orozco-Alzate, 2017). En total congruencia con los autores es indispensable un análisis de riesgos previo para la planificación de contramedidas a los ataques de seguridad. Obtener los riesgos potenciales facilitan la implementación de un SGSI o simplemente ayudan a la creación de algunos protocolos para respaldar de forma segura los activos según la investigación de (Arévalo Ascanio et al., 2015).

Así mismo, las organizaciones aún enfrentan problemas para la implementación de una norma ISO/IEC 27001, 27002, COBIT u otras guías de seguridad; en las instituciones públicas el porcentaje de aplicación es bajo a diferencia de las privadas ya que no existe el soporte de altos directivos, empleados no capacitados y no aplicación de políticas de seguridad de la información (Sussy et al., 2015). Los autores mencionan puntos clave y

problemas muy relevantes que existen en las instituciones y más aún si es una organización gubernamental, por ello es necesario conocer el estándar a poner en marcha y capacitar a los usuarios sobre los cambios a ejecutarse. Es importante conocer que la familia de normas ISO/IEC 27000 es replicada por la INEN (Servicio Ecuatoriano de Normalización), mismo que es ajustado al idioma español y particularmente a las exigencias de las empresas públicas del Ecuador y claro una guía a poner en práctica en el Gobierno Provincial del Cañar.

CONCLUSIONES

La revisión del estado del arte aclaró las dudas y la importancia del estudio en el área de la ciberseguridad, tema considerable para cualquier organización que usa sistemas de información para la automatización de sus procesos.

Los resultados de esta investigación mostraron los riesgos potenciales de los activos de seguridad del Gobierno Provincial del Cañar con la guía práctica de la metodología MAGERIT, ya que está enfocada a instituciones gubernamentales y el proceso fue más satisfactorio y ágil durante todo el desarrollo.

Las amenazas encontradas con más peligro de sufrir ciberataques son: la información y servicios digitales de la empresa ya que su perdida estaría aproximadamente en 300mil dólares americanos, sin embargo, para el autor el activo más sensible siempre serán los empleados encargados de la administración y funcionamiento de la organización.

En la discusión de este presente trabajo se describe algunas investigaciones relacionadas a la importancia de desarrollar un análisis de riesgos siguiendo alguna de las metodologías acorde a la organización con la finalidad de realizar protocolos de seguridad de la información.

REFERENCIAS BIBLIOGRÁFICAS

Arévalo Ascanio, J. G., Bayona Trillos, R. A., & Rico Bautista, D. W. (2015). Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: análisis del riesgo de la información. *Revista Tecnura*, *19*(46), 123. https://doi.org/10.14483/udistrital.jour.tecnura.2015.4.a10

Da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers and Security*, *49*, 162–176. https://doi.org/10.1016/j.cose.2014.12.006

Édison, D., Vergara, F., Camilo, F., Riveros, C., Castillo, R. A., Víctor, V. G., Juan Carlos, & Vera Gil. (2017). Seguridad informática organizacional: un modelo de simulación

basado en dinámica de sistemas Informatic organizational security: a simulation model based on systems dynamic. *Scientia et Technica Año XXII*, *22*(2).

Gualotuña, Hugo & Quilumbaqui, M. (2016). *Aplicación de las normas técnicas iso/iec 27001 e iso/iec 27002 para el cumplimiento del esquema gubernamental de seguridad de la información (egsi) en la infraestructura del sistema nacional de nivelación y admisión (SNNA)*. https://bibdigital.epn.edu.ec/handle/15000/15191

Hartley, R., Medlin, D., & Houlik, Z. (2017). Ethical Hacking: Educating Future Cybersecurity Professionals. *Proceedings of the EDSIG Conference*, 1–10. http://proc.iscap.info/2017/pdf/4341.pdf

ISO Standars. (1991). ISO Standards. In *Digital Guide to Developing International Software* (pp. 341–342). https://doi.org/10.1016/b978-1-55558-063-6.50022-1

Lewis, B. (2018). *ISO / IEC 27000 - Norma internacional clave para la seguridad de la información revisada*. https://www.iso.org/news/ref2266.html

Molina Miranda, M. F. (2017). ANÁLISIS DE RIESGOS DE CENTRO DE DATOS BASADO EN LA HERRAMIENTA PILAR DE MAGERIT. *Espiral*, *1*. http://www.revistaespirales.com/index.php/es/article/view/125/68

Ochoa Arévalo, P. A. (2015). Gobierno de Seguridad de la Información, un enfoque hacia el cumplimiento regulatorio. *Revista Tecnológica ESPOL-RTE*, *28*(3), 1–17. http://rte.espol.edu.ec/index.php/tecnologica/article/view/373

PricewaterhouseCoopers. (2018). Strengthening digital society against cyber shocks: Key findings from The Global State of Information Security ® Survey 2018. *Cybersecurity and Privacy*, 21. https://doi.org/10.1038/nrd3793

Spanish Higher Council for Government. (2012). *PAe - MAGERIT v.3: Methodology of analysis and risk management information systems*. https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html?idioma=en

Sussy, B., Wilber, C., Milagros, L., & Carlos, M. (2015). ISO/IEC 27001 implementation in public organizations: A case study. *IEEE*, 1–6. https://doi.org/10.1109/cisti.2015.7170355

Tejena-Macías, M. A. (2018). Análisis de riesgos en seguridad de la información. *Polo Del Conocimiento*, *3*(4), 230. https://doi.org/10.23857/pc.v3i4.809

ultimas noticias. (2019). *Tests de Ser Bachiller fueron vulnerados*. 2019. https://www.ultimasnoticias.ec/las-ultimas/tests-bachiller-vulnerados-denuncia.html

Valencia-Duque, F. J., & Orozco-Alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *Revista Ibérica de Sistemas y Tecnologías de Información*, 1–16. https://doi.org/10.17013/risti.22.73-88

White; Hewitt & Kruck. (2017). Incorporating Global Information Security and Assurance in I.S. Education. In *Journal of Information Systems Education, Vol. 24(1) Spring 2013.* (Vol. 24, Issue 1, pp. 1–9). Springer Singapore. https://doi.org/10.1007/978-981-10-6968-0_1