DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL PROCESO DE GESTIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA DE INSTITUCIONES ACADÉMICAS BASADO EN MAGERIT

DESIGN OF AN INFORMATION SECURITY MANAGEMENT SYSTEM FOR THE PROCESS OF MANAGING THE TECHNOLOGICAL INFRASTRUCTURE OF ACADEMIC INSTITUTIONS BASED ON MAGERIT

Eduardo Alfonso Rosales Montalbán[1]
Raúl José Martelo Gómez[2]
David Antonio Franco Borré[3]

Resumen

Con esta investigación, se diseñó un Sistema de Gestión de Seguridad de la Información (SGSI) en el ámbito de una institución educativa ubicada en Cartagena (Colombia) aplicado al proceso administrativo de gestión de infraestructura tecnológica. Con ello se identificaron aquellos activos a considerar por la organización en su aplicación de un sistema de gestión adecuado a sus políticas, mediante el enfoque de la norma ISO 27001 y la metodología MAGERIT. Se realizaron evaluaciones de los riesgos, mostrando mecanismos de protección además de la caracterización y ponderación de los activos, amenazas y salvaguardas implicados en la gestión de infraestructura de la institución. Los resultados obtenidos muestran mecanismos de control y políticas de seguridad que aportan soluciones a amenazas encontradas como el uso no previsto de la infraestructura, denegación de servicio, y el acceso no autorizado, las cuales representan un nivel elevado de riesgo en la institución, enmarcados en el ciclo de mejoramiento continuo.

Palabras clave: SGSI, Gestión de infraestructura, MAGERIT, ISO 27001, TIC, instituciones académicas.

Abstract

In this research, an Information Security Management System (ISMS) was designed to be applied in the management process of technological infrastructure management of a school located in Cartagena de Indias (Colombia). The above allowed to identify assets to be considered by the organization in the application of a management system appropriate to its policies through the

Fecha de recepción: Mayo de 2019 / Fecha de aceptación en forma revisada: Octubre de 2019

[1]Ingeniero de Sistemas de la Universidad de Cartagena. ORCID: https://orcid.org/0000-0002-2323-3371. Mail: eduardo_22@ingenieros.com

[2]Ingeniero de Sistemas, Especialista en Redes y Telecomunicaciones, Magister en Informática. Docente del Programa de Ingeniería de Sistemas, Universidad de Cartagena. Líder del Grupo de Investigación INGESINFO. ORCID: https://orcid.org/0000-0002-4951-0752. Mail: rmartelog1@unicartagena.edu.co

[3]Ingeniero de Sistemas, Magister en Ciencias Computacionales. Docente del Programa de Ingeniería de Sistemas, Universidad de Cartagena. Líder del Grupo de Investigación GIMATICA. ORCID: https://orcid.org/0000-0001-7500-0206. Mail: dfrancob@unicartagena.edu.co

approach of ISO 27001 and the MAGERIT methodology. Risk analyzes and evaluations were carried out, showing the protection mechanisms in addition to the characterization and weighting of the assets, threats, and safeguards involved in the infrastructure management of the school. The results obtained show control mechanisms and security policies that provide solutions to the threats found: unintended use of infrastructure, system crash due to resource depletion, denial of service, and unauthorized access, which represent a high level of risk in the school, framed in the cycle of continuous improvement.

Keywords: ISMS, Infrastructure Management, MAGERIT, ISO 27001, ICT, academic institutions.

Introducción

La información y tecnología en conjunto son consideradas un activo cada vez más importante para las organizaciones, debido al impacto que genera en los procesos que se ejecutan para el desarrollo y venta de sus productos o servicios, lo cual coadyuva en el incremento del nivel de competitividad e innovación de la misma (Ahmad, et al., 2012). Lo anterior provoca en las instituciones de educación la adopción de políticas que faciliten a la comunidad educativa la aplicación de tecnologías de información en actividades académicas y laborales, con el fin de acceder y utilizar de manera eficiente los datos producidos en estos procesos (Kim, 2013). El apropiamiento de las tecnologías de información conlleva a la aplicación de estrategias enfocadas a la adaptación de esta tendencia, lo cual requiere de la gestión de proyectos de infraestructura institucional, para obtener el mayor beneficio de las herramientas informáticas en el sistema de aprendizaje y procesos administrativos (Bozalek, et al., 2013).

Las instituciones utilizan su presupuesto en la incorporación de una infraestructura capaz de abarcar los parámetros necesarios en la satisfacción de la demanda informática, la cual exige entre otros requerimientos la capacitación de los estudiantes, crecimiento científico y la eficiencia administrativa (Kalpeyeva y Mustafina, 2013; Sastoque, Restrepo y Castro, 2019). En este sentido, las instituciones de educación realizan inversiones en tecnología de información de mejor calidad acorde a las especificaciones de la infraestructura tecnológica, con el fin de permitir un mayor control y mejor flujo de la información en actividades de las áreas de trabajo y reducir los costos que conllevan su ejecución (Porter, et al., 2014). Con la inclusión de esta tecnología, la institución puede organizar y almacenar la información resultante de los servicios académicos y administrativos, con la garantía de confiabilidad e integridad de los datos, además de brindar acceso forma segura (Budel, et al., 2015; Imaquingo, et al., 2019).

No obstante, el acoplamiento de las TI[4] con las instituciones y el entorno representa un riesgo para la información confidencial de las instituciones (García y Moreta, 2018; Molina-Miranda, 2017; Rivera, et al., 2019; Ortiz-Lazo y Vizñay, 2019; Tubío, et al., 2020), por lo cual se deben aplicar esfuerzos en ejecutar mecanismos efectivos de seguridad, con el fin de conservar el buen estado de los archivos almacenados (Bravo y Yoo, 2020; Chander, et al., 2013; Raed, Mohamed, y Tai-Hoon, 2014). Así, mientras crecen los mecanismos para proteger la información, incrementan las amenazas que existen en el ambiente virtual, indicativo de un mayor riesgo para la organización (Martelo, Tovar y Maza, 2018). Además, con el rápido avance tecnológico del mundo, estas amenazas se transforman y adaptan, logrando provenir de fuentes como redes informáticas o internet, que son herramientas muy utilizadas y por lo tanto las

[4] Tecnologías de Información

instituciones requieren de protección adicional ante los riesgos (Narain, et al., 2013; Tejena-Macía, 2018; Vicente, et al., 2014; Velasco, et al., 2018).

Por lo anterior, el propósito de la investigación es diseñar un SGSI[5] en el ámbito de las instituciones educativas, aplicado a los procesos administrativos de gestión de infraestructura tecnológica. Esto permite la identificación de los elementos que debe considerar una compañía para la aplicación de un sistema de gestión alineado a sus políticas internas, de acuerdo a la normatividad internacional para la protección de la información.

Metodología

La investigación fue cuantitativa, con diseño no experimental transeccional descriptivo. Se consideró no experimental por describir y explicar sucesos como se presentan de manera natural, sin alterarlos (Christensen, et al., 2015). Transeccional puesto que se obtuvieron y analizaron las variables de la investigación en un instante de tiempo fijo (Leavy, 2017). Y descriptivo debido a que se evaluaron y detallaron los activos, amenazas y riesgos de la institución con el fin de establecer un SGSI (Babbie, 2011). Con respecto a la recolección de información, como técnica se implementó la entrevista y la observación. La población se conformó por 10 administrativos de la Institución Educativa, los cuales hacen parte de los procesos de gestión administrativa y académica de la institución. Por el tamaño de la población, no fue necesario aplicar muestreo.

Por otro lado, para el análisis se planteó diseñar un SGSI con base en las directrices establecidas en la ISO 27001, donde fue aplicado el modelo del ciclo Deming o PHVA, el cual consiste en un esquema con 4 etapas enfocadas en garantizar el mejoramiento continuo de un sistema y se utiliza MAGERIT como metodología de implementación de las fases Planear y Hacer, del ciclo mencionado. Asimismo, se tiene en cuenta el análisis de riesgos realizado en la metodología MAGERIT, el cual se conforma de los elementos: MOVA[6], MARI[7], DEAP[8], EVSA[9] y ESRI[10]. Considerando lo descrito, el SGSI estuvo basado en el modelo PHVA, junto con la aplicación de la metodología MAGERIT, con el fin de lograr una mejora continua con la incorporación de nuevos requisitos y actividades.

Análisis de Riesgo

Se utilizó la metodología MAGERIT v3.0 para la evaluación de riesgo en la seguridad de la información, dado que está basada en el área informática y es compatible con la ISO 27001. Esta metodología de análisis y gestión de riesgos fue desarrollada para reducir riesgos en la implantación y manejo de las TI, centrada en la Administración Pública. MAGERIT define un método por tareas y actividades definidas en el MAR (Métodos de Análisis de Riesgos) como se muestra a continuación:

LMAR.1 CAAC[11]

MAR.11 – IDAC[12]

MAR.12 – DEAC[13]

[5] Sistema de Gestión de Seguridad de la Información
[6] Modelo de Valor
[7] Mapa de riesgos
[8] Declaración de Aplicabilidad
[9] Evaluación de Salvaguardas
[10] Estado de Riesgo
[11] Caracterización de los Activos
[12] Identificación de los Activos

MAR.13 – VAAC[14]
MAR.2 CAAM[15]
MAR.21 – IDAM[16]
MAR.22 – VAAM[17]
MAR.3 CASAL[18]
MAR.31 – IDSAPE[19]
MAR.32 – VASA[20]
MAR.4 EESRI[21]
MAR.41 – ESIM [22]
MAR.42 – ESTRI[23].

El resultado de estas actividades conforma la documentación del SGSI y constituye la creación del cuerpo normativo tanto de la norma como de la metodología MAGERIT, teniendo como desarrollo la creación de estos documentos con respecto a las actividades (Cuadro 1).

MOVA	MAR.1 CAAC
MARI	MAR.2 CAAM
EVSA	MAR.3 CASAL
DEAP	MAR.4 EESRI
ESRI	MAR.4 EESRI

Cuadro 1. Relación de actividades del MAR y documentos generados

MAR 1. CAAC
IDAC

Se determinaron las características, atributos y clasificación de los diferentes tipos de activos pertenecientes a la institución, por medio de la aplicación de las técnicas observación directa y entrevistas realizada a los funcionarios con relevancia para el sistema. Con la implementación de MAGERIT, se agrupan los activos identificados en el sistema de acuerdo a su naturaleza, con el fin de asignarle un código de identificación (Cuadro 2).

[D] Datos
• [d_scode_si] Código Fuente del sistema integrado • [d_passw] Credenciales de Acceso • [d_DB_incrip] Base de datos de inscripciones y matriculas • [d_DB_encuest] Base de datos de encuestas • [d_DB_si] Base de datos del sistema integrado

[13] Dependencias entre Activos
[14] Valoración de los Activos
[15] Caracterización de las Amenazas
[16] Identificación de las Amenazas
[17] Valoración de las Amenazas
[18] Caracterización de las Salvaguardas
[19] Identificación de las Salvaguardas Pertinentes
[20] Valoración de las Salvaguardas
[21] Estimación del Estado de Riesgo
[22] Estimación del Impacto
[23] Estimación del Riesgo

• [d_drivers] Archivos de configuración y controladores de equipos • [d_doc_infrs] Archivos de documentación de infraestructura • [d_backup_files] Ficheros de Respaldo y Copias de seguridad
[S] Servicios
• [s_mails] Servidor de correos • [s_ftp] Servicio de trasferencia de archivos • [s_web] Servicios del portal web
[SW] Aplicaciones (Software)
• [sw_si] Sistema integrado • [sw_siigo] Sistema de gestión contable • [sw_school] Sistema de gestión académica • [sw_so] Sistemas operativos • [sw_office] Ofimática • [sw_antivirus] Antivirus • [sw_browser] Navegador Web • [sw_dev] Entorno de Desarrollo • [sw_mang] Aplicaciones de Gestión y Monitoreo
[HW] Equipos Informáticos las avanza
• [hw_server] Servidor • [hw_pc_adm] Equipos de informática de uso administrativo • [hw_pc_edu] Equipos de informática de uso educativo • [hw_vbeam] Proyectores • [hw_printer] Impresoras • [hw_firewall] Fortigate • [hw_accespoint] Puntos de acceso • [hw_sw_route] Switches y routers
[COM] Redes de comunicaciones
• [com_pstn] Red telefónica • [com_radio] Red Inalámbrica • [com_lan] Red Local • [com_internet] Internet
[Media] Soportes de información
• [media_net] Almacenamiento en red • [media_hd_ext] Disco externo de respaldo
[AUX] Equipamiento Auxiliar
• [aux_ups] Sistemas de alimentación ininterrumpida • [aux_furnit] Gabinetes y mobiliario

Cuadro 2. Codificación de los activos identificados del sistema

VAAC

Considerando los parámetros de la metodología MAGERIT, se estableció como técnica de valoración un cuadro de índices cualitativos y se determinó su criterio por medio de reuniones con los funcionarios dentro del proceso. Los activos fueron valorados dentro de tres dimensiones independientes:

Disponibilidad: Propiedad de ser accesible y utilizable ha pedido de una entidad autorizada.

Integridad de los datos: Propiedad de proteger la precisión y completitud de los activos.

Confidencialidad de la información: Característica que define la protección de la información frente a individuos, entidades o procedimientos no autorizados.

En el proceso de valoración se establece un índice correspondiente a la dimensión del activo al momento de ser afectada, es decir, su importancia para la organización. El índice de valor se estableció mediante criterios cualitativos ordenados en un cuadro y representados en una escala de 0 a 10, donde cero representa un valor despreciable y 10 un valor de daño extremo para la organización (Cuadro 3).

Valor		Criterio
10	Extremo	Daño extremadamente grave
9	Muy alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Despreciable	Irrelevante

Cuadro 3. Índices de valor de los activos

MAR 2. CAAM
IDAM

Consiste en listar y documentar los riesgos que amenazan los activos, para determinar las medidas pertinentes y garantizar su seguridad. La metodología para la IDAM consiste en seleccionar los activos que conforman el sistema y definir sus amenazas por medio de entrevistas y reuniones con los funcionarios relacionados de forma directa o indirecta con el activo, mediante el catálogo de amenazas proporcionado por MAGERIT como guía de referencia. Se debe tener en consideración que al realizar la IDAM se tiene en cuenta la dimensión de mayor relevancia por lo cual cada activo es importante en la organización y los tipos de fallas que presentaron en el pasado. Asimismo, por cada amenaza identificada se documentó la descripción de su efecto y antecedentes en la organización. Ahora bien, respecto a los errores causantes de pérdidas en la organización, MAGERIT proporciona un cuadro que permite definir la línea entre los diferentes tipos de errores y los ataques relacionados (Cuadro 4).

Error	Ataque
ERUS[24]	
ERAD[25]	
ERMO[26] (log)	Modificación de los registros de actividad
Errores de configuración	Modificación de la configuración
	Suplantación de la identidad del usuario
	ABPRAC[27]

[24] Error de los usuarios
[25] Error del administrador
[26] Errores de monitorización
[27] Abuso de privilegios de acceso

Deficiencia en la organización	USNOPRE[28]
DISOMAL[29]	DISOMAL
Errores de [Re-]encaminamiento	[Re-]encaminamiento de mensajes
Errores de secuencia	Modificación de secuencias
	ACNOAU[30]
	Evaluación de tráfico
	Repudio
Escapes de información	Interceptación de información (escucha)
ALACIN[31]	MODEIN[32]
DEIN[33]	DEIN
Fugas de información	Revelación de información
Vulnerabilidades de los programas	
ERMA[34]	
	Manipulación de programas
ERMA	Manipulación de equipos
CSAR[35]	DESE[36]
Perdida de equipos	Robo
	ATDE[37]
	Ocupación enemiga
INPE[38]	INPE
	Extorción
	Ingeniería social

Cuadro 4. Relación error y ataque

Con lo anterior, se identificaron con mayor facilidad los contextos donde se presentan fallas y los ataques que muestran comportamientos parecidos pero que deben ser tratados de forma diferente, aunque posean la misma consecuencia. Por otra parte, con la evaluación de los activos y el catálogo de amenazas de MAGERIT, se estableció la relación de los activos y las amenazas a las cuales se expone (Cuadro 5).

Activos	Amenazas
[d_scode_si] Código Fuente del sistema Integrado	ERMO, ERESIN[39], MOACIN[40]
[d_passw] Credenciales de	ERUS, ERAD, Escapes de información, ACNOAU,

[28] Utilización no prevista
[29] Difusión de software malicioso
[30] Acceso no autorizado
[31] Alteración accidental de la información
[32] Modificación deliberada de la información
[33] Destrucción de información
[34] Errores de mantenimiento
[35] Caída del Sistema por agotamiento de recursos
[36] Denegación de servicio
[37] Ataque destructivo
[38] Indisponibilidad del personal
[39] Errores de escapes de información
[40] Modificación accidental de información

Acceso	DIIN[41], DEIN
[d_DB_incrip] Base de datos de inscripciones y matriculas	ERAD, ERMO, MOACIN, DEIN, MODEIN, Manipulación de los registros
[d_DB_encuest] Base de datos de encuestas	ERUS, ERAD, ERMO, DEIN, MOACIN, Manipulación de registros, Modificación deliberada de información
[d_DB_si] Base de datos del sistema integrado	ERUS, ERAD, ERMO, DEIN, MOACIN, Manipulación de registros, Modificación deliberada de información
[d_drivers] Archivos de configuración y controladores de equipos	DEIN
[d_doc_infrs] Archivos de documentación de infraestructura	MOACIN, DEIN.
[d_backup_files] Ficheros de Respaldo y Copias de seguridad	MOACIN, DEIN, MODEIN, ACNOAU.
[sw_si] Sistema integrado	ACNOAU, ABPRAC, CSAR, DESE
[sw_siigo] Sistema de gestión contable	CSAR, DESE, DEIN, DIIN, ABPRAC, ACNOAU.
[sw_school] Sistema de gestión académica	CSAR, DESE, DEIN, DIIN, ABPRAC, ACNOAU.
[sw_so] Sistemas operativos	USNOPRE, DESE.
[sw_office] Ofimática	Error de mantenimiento/Actualización de programas, Difusión de software dañino.
[sw_antivirus] Antivirus	DISOMAL, ACNOAU, Error de mantenimiento / Actualización de programas, USNOPRE.
[sw_browser] Navegador Web	Difusión de software Dañino, USNOPRE, Errores del usuario
[sw_dev] Entorno de Desarrollo	USNOPRE, Modificación de secuencia, ACNOAU, Errores del Administración.
[sw_mang] Aplicaciones de Gestión y Monitoreo	USNOPRE, Modificación de secuencia, ACNOAU.
[hw_server] Servidor	Fuego, Agua, DESE, Corte suministro eléctrico, Robo, Humedad, ACNOAU, DESE, Avería, USNOPRE, Error de Mantenimiento, CSAR
[hw_pc_adm] Equipos de informática de uso administrativo	Fuego, Avería, ACNOAU, DESE, Robo, Humedad, USNOPRE, Error de mantenimiento, Manipulación de Equipo.
[hw_pc_edu]Equipos de informática de uso educativo	Fuego, DESE, Humedad, Manipulación de Equipo, Avería, Error de mantenimiento, USNOPRE, Robo.
[hw_vbeam]Proyectores	Humedad, Avería, Humedad, USNOPRE.
[hw_printer]Impresoras	Fuego, Avería, Robo, DESE.
[hw_firewall]Fortigate	Fuego, Agua, Robo, ERAD, ACNOAU, Error en el

[41] Difusión de información

	mantenimiento, CSAR.
[hw_accespoint]Puntos de acceso	Robo, CSAR, ACNOAU.
[hw_sw_route] Switches y routers	Robo, CSAR, ACNOAU, Condiciones de temperatura y humedad, Corte de suministro eléctrico, Avería
[com_pstn]Red telefónica	Fallo del servicio de comunicaciones, USNOPRE.
[com_radio]Red Inalámbrica	Fallo del servicio de comunicaciones, ERAD, CSAR, ABPRAC, ACNOAU, DIIN.
[com_lan]Red Local	Fallo del servicio de comunicaciones, ERAD, CSAR, ABPRAC, ACNOAU, DIIN, DESE.
[com_internet]Internet	Fallo servicio de comunicaciones, USNOPRE, DESE
[media_net]Almacenamiento en red	DESE, Fallo servicio de comunicaciones, USNOPRE, Fallo del servicio de comunicaciones, ERAD, CSAR.
[media_hd_ext]Disco externo de respaldo	Fuego, DEIN, Perdida de Equipo, ACNOAU, DEIN, Robo
[aux_ups]Sistemas de alimentación ininterrumpida	Agua, Fuego, Error en el mantenimiento, Falla de suministro eléctrico, Daño en el equipo.
[aux_furnit]Gabinetes y mobiliario	DESE, Falla en el mantenimiento, Fuego, Avería, Agua, USNOPRE.

Cuadro 5. Relación de IDAM

Caracterización y VAAM

Para la caracterización, se asignó un código de identificación a las amenazas identificadas previamente. En la valoración, se analizó cada dimensión de los activos y se asignó un valor de acuerdo al Cuadro 6, donde se muestra la degradación del valor del activo. También se estimó la probabilidad de ocurrencia de amenazas de acuerdo a un valor cualitativo, el cual se puede evidenciar clasificación del Cuadro 7.

Índice	Categoría	Valor
MA	Muy alta	10
A	Alta	8-9
M	Media	5-7
B	Baja	3-4
MB	Muy baja	1-2

Cuadro 6. Clasificación de la degradación del valor del activo

Índice	Categoría
CS	Casi seguro
MA	Muy alto
P	Posible
PP	Poco probable
MB	Muy bajo
0	

Cuadro 7. Clasificación cualitativa de la probabilidad de ocurrencia de la amenaza

MAR 3. CASAL

Se definieron las salvaguardas, es decir, se seleccionaron mecanismos, técnicas, políticas y procedimientos que ayudan en la protección del activo en caso que surja la amenaza. Existen diferentes clases de protecciones las cuales se agrupan en 3 categorías con base en sus efectos: preventivas, que acotan la degradación y que consolidan los efectos de otras, como se evidencia en el Cuadro 8.

Efecto	Tipo
Preventivas: Disminuyen la probabilidad	[PR] Preventivas [DR] Disuasorias [EL] Eliminatorias
Acotan la degradación	[IM] Minimizadoras [CR] Correctivas [RC] Recuperativas
Consolidan el efecto de las demás	[MN] De Monitorización [DC] De Detección [SW] De Concienciación [AD] Administrativas

Cuadro 8. Clases de protección según su efecto

Tanto a las amenazas como a las salvaguardas se le asigna un nivel de eficacia dentro del sistema. Para determinar la eficacia de una salvaguarda, es necesario evaluar desde la perspectiva técnica (si es suficiente para proteger el activo) y operacional (si es implementada adecuadamente en la institución, si tiene mecanismos bien definidos o si tiene usuarios capacitados para su despliegue). Para la estimación de este valor MAGERIT sugiere medir su eficacia y madurez con base en los niveles establecidos en el Cuadro 9.

Factor	Nivel	Significado
0%	L0	Inexistente
	L1	Inicial / ad hoc
	L2	Reproducible, pero intuitivo
	L3	Proceso definido
	L4	Gestionado y medible
100%	L5	Optimizado

Cuadro 9. Medición de Salvaguardas

MAR.4 EESRI

ESIM

La ESIM consiste en calcular el nivel exposición del sistema ante algún riesgo, teniendo en cuenta el valor de los activos y el deterioro causado por amenazas. En este caso, se calculó el impacto potencial y residual del sistema basado en la VAAC establecidos en el MOVA y las amenazas del MARI. El método de valoración está fundamentado en un análisis de cuadros, mediante el cruce de los valores del activo y la degradación de las amenazas, lo cual produce como resultado un mapa del impacto potencial, que se calcula por cada amenaza sobre cada activo y se registrara en el informe de ESRIs. En este sentido, se observan los cuadros de estimación de variables en el Cuadro 10 y valoración de impacto en el Cuadro 11, que se utilizaron para categorizar la valoración de las variables.

IMPACTO		VALOR DEL ACTIVO				
		MB	B	M	A	Extremo
DEGRADACION	MA	B	M	A	MA	MA
	A	B	M	A	A	MA
	M	B	B	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Cuadro 10. ESIM del riesgo

Índice	Valor
MA	10
A	8-9
M	5-7
B	3-4
MB	1-2

Cuadro 11. Valorización del impacto del riesgo

Respecto al análisis del impacto residual, se realiza el mismo proceso que en la ESIM residual con la diferencia que está basado en las salvaguardas implementadas o proyectadas. Al realizar el análisis del impacto residual se debe tener en consideración que las salvaguardas poseen dos escenarios de estudio: el estado actual del sistema y el estado aceptable de implementación de las salvaguardas.

ESTRI

La ESTRI fue realizada mediante la implementación de la probabilidad de ocurrencia, con un crecimiento proporcional al valor del impacto y la probabilidad de ocurrencia, lo cual permitió generar un mapa de valor para observar con mayor claridad el comportamiento de esta variable. El riesgo posee tres estados de acción: potencial (cuando se hace el análisis ignorando las salvaguardas implementadas o proyectadas a implementar), residual con la eficiencia de las salvaguardas implementadas actualmente, y residual con la eficiencia de las salvaguardas proyectadas a implementar con el desarrollo del sistema de gestión. Por lo anterior, se generó el ESRIs, el cual consiste en un expediente con la documentación de esta actividad, constituido por registros de los valores del impacto potencial y residual, el riesgo potencial y residual por cada dimensión y activo dentro del sistema.

Resultados y discusión

Considerando los elementos de la metodología MAGERIT, se realizaron las entrevistas a los funcionarios de la institución con base en sus actividades regulares e impacto en la seguridad de la información. Se obtuvo el MOVA respecto a las dimensiones de disponibilidad, integridad de datos y confidencialidad, además de una justificación de las razones por las cuales se asignó cada valor correspondiente, generando un documento denominado, MOVA para los activos de la institución, donde se especifican los siguientes datos para cada activo: código, nombre, responsable, dependencias, dimensión, valor y su justificación. Este documento permitió definir la importancia que tienen los activos en la institución, estableciendo que los activos de mayor relevancia para la organización por su impacto en los procesos administrativos y académicos son los servidores, los archivos de respaldo y seguridad, y los mecanismos de acceso al sistema.

Teniendo en cuenta el modelo de MAGERIT, se generó otro documento con el MARI de los activos donde se analizaron las amenazas a las cuales se exponen los activos del sistema, estableciendo que los errores y ataques a los cuales se exponen los activos afectan en su mayoría la disponibilidad para el usuario, por ello existe la necesidad de aplicar medidas que apunten a evitar este problema. De la misma forma, las salvaguardas fueron evaluadas de acuerdo a su impacto para detener los riesgos que afectan a los activos, lo cual se encuentra especificado en el Cuadro 12.

Código: [E.log]	ERMO (log)	
Salvaguarda	ACTUAL	ACEPTABLE
[D.serial] Serialización de registros	L0	L3
[H.tools.LA] HEANLOGS[42]	L2	L4
Código: [E.EscInf]	ERESIN	
Salvaguarda	ACTUAL	ACEPTABLE
[D.serial] Serialización de registros	L0	L3
[H.tools.LA]HEANLOGS	L2	L4
Código: [E.AltInf]	ALACIN	
Salvaguarda	ACTUAL	ACEPTABLE
[D.A] COSEDA[43]	L2	L4
[H.tools.LA] Aseguramiento de la integridad	L0	L3
Código: [E.user]	Errores de los Usuarios	
Salvaguarda	ACTUAL	ACEPTABLE
[D.A] COSEDA	L2	L4
[PS] Gestión del Personal	L3	L5
[PS.AT] FOCO[44]	L1	L4
Código: [A.noAuth]	ACNOAU	
Salvaguarda	ACTUAL	ACEPTABLE
[H.AC] CODEACLO[45]	L3	L5
[H.VM] Gestión de vulnerabilidades	L1	L4
[SW.SC] Se aplican perfiles de seguridad	L1	L3
[COM.wifi] Seguridad Wireless WiFi	L2	L4
[COM.aut] Autenticación del canal	L1	L3
[L.AC] Control de accesos físicos	L3	L5
[PS.AT] FOCO	L1	L4
Código: [E.admin]	ERAD	
Salvaguarda	ACTUA	ACEPTABL

[42] Herramienta para análisis de logs
[43] Copias de seguridad de los datos
[44] Formación y concienciación
[45] Control de acceso lógico

		L	E
[PS] Gestión de Personal		L3	L5
[PS.AT] FOCO		L1	L4
[H.tools.LA]HEANLOGS		L2	L4
[H.AU] Registro y auditoría		L1	L3
Código: [A.divInfo]	DIIN		
Salvaguarda		ACTUAL	ACEPTABLE
[SW.SC] Se aplican perfiles de seguridad		L1	L4
[S.email] protección del correo electrónico		L2	L4
[PS.AT] FOCO		L1	L4
[H.IA] IDAU[46]		L1	L3
Código: [A.destInfo]	DEIN		
Salvaguarda		ACTUAL	ACEPTABLE
[D.A] COSEDA (Backup)		L3	L4
[H.IA] IDAU		L1	L3
[L.AC] Control de accesos físicos		L1	L3
[H.AC] CODEACLO		L3	L5
Código: [A.ManReg]	Manipulación de los registros		
Salvaguarda		ACTUAL	ACEPTABLE
[H.IA] IDAU		L0	L2
[H.tools.LA]HEANLOGS		L2	L4
[D.A] COSEDA (Backup)		L2	L4
[H.AC] CODEACLO		L3	L5
Código: [A.noAcces]	ABPRAC		
Salvaguarda		ACTUAL	ACEPTABLE
[H.tools.LA]HEANLOGS		L2	L4
[H.IA] IDAU		L0	L4
[H.tools.VA] Herramienta de análisis de vulnerabilidades		L1	L3
[D.C] Cifrado de la información		L0	L2
Código: [A.noUse]	USNOPRE		
Salvaguarda		ACTUAL	ACEPTABLE
[PS.AT] FOCO		L1	L4
[PS] Gestión de Personal		L3	L5
[H.IA] IDAU		L1	L4
Código: [A.noServ]	DESE		
Salvaguarda		ACTUAL	ACEPTABLE
[S.dir] Protección del directorio		L1	L3

[46] Identificación y autenticación

[S.www] Protección de servicios y aplicaciones web		L1	L3
[H.tools.VA] Herramienta de análisis de vulnerabilidades		L0	L3
[H.tools.TM] Herramienta de monitorización de trafico		L1	L4
[SW] Protección de las aplicaciones informáticas		L2	L4
Código: [A.noResour]	CSAR		
Salvaguarda		ACTUAL	ACEPTABLE
[HW.A] ASDIS[47]		L0	L3
[MP.Clean] Limpieza de contenidos		L0	L4
[BC] Continuidad del negocio		L0	L3
[COM.CM] Cambios (actualizaciones y mantenimiento)		L2	L4
Código: [A.noAct]	ERMA / Actualización de programas		
Salvaguarda		ACTUAL	ACEPTABLE
[D.A.] Copias de seguridad		L2	L4
[HW] Protección de equipos informático		L1	L3
[PS.AT] FOCO		L1	L3
Código: [E.ModInf]	MODEIN		
Salvaguarda		ACTUAL	ACEPTABLE
[D.A.] Copias de seguridad		L2	L4
[H.IA] IDAU		L1	L3
[H.AC] Control de acceso Físico		L3	L5
[SW.AC] CODEACLO		L1	L3
[SW.SC] Se aplican perfiles de seguridad		L0	L3
Código: [A.DifSoft]	Difusión de software dañino		
Salvaguarda		ACTUAL	ACEPTABLE
[D.serial] Serialización de registros		L0	L3
[H.tools.LA]HEANLOGS		L2	L4
Código: [A.Fire]	Fuego		
Salvaguarda		ACTUAL	ACEPTABLE
[D.A.] Copias de seguridad		L2	L4
[PS] Gestión de Personal		L1	L5
[PS.AT] FOCO		L1	L4
[L.AC] Control de acceso Físico		L3	L4
[AUX.wires] Protección de Cableado		L1	L3
[AUX] Elementos auxiliares		L1	L3
[L] Proteccion de instalaciones		L1	L3
Código: [A.Water]	Agua		
Salvaguarda		ACTUAL	ACEPTABLE

[47] Aseguramiento de la disponibilidad

[D.A.] Copias de seguridad		L2	L4
[PS] Gestión de Personal		L3	L4
[PS.AT] FOCO		L1	L3
[L.AC] Control de acceso Físico		L3	L4
[AUX.wires] Protección de Cableado		L1	L3
[AUX] Elementos auxiliares		L1	L3
[L] Proteccion de instalaciones		L1	L3
Código: [A.fault]	Avería		
Salvaguarda		ACTUAL	ACEPTABLE
[HW] Proteccion de los equipos informáticos		L2	L4
[HW.A] ASDIS		L1	L4
[HW.CM] Cambios (Actualizaciones y mantenimientos)		L3	L4
[PS.AT] FOCO		L1	L4
Código: [A.noEect]	Corte del suministro eléctrico		
Salvaguarda		ACTUAL	ACEPTABLE
[HW.A] ASDIS		L1	L3
[AUX.power] Suministro Eléctrico		L0	L3
Código: [A.Stole]	Robo		
Salvaguarda		ACTUAL	ACEPTABLE
[L.AC] Control de los accesos físicos		L3	L4
[E.4] Personal subcontratado		L2	L4
[HW] Protección de los Equipos informáticos		L2	L4
[H.AU] Registro y auditoría		L1	L4
[H] Protecciones generales		L2	L4
Código: [A.Destrut]	DESE		
Salvaguarda		ACTUAL	ACEPTABLE
[L.AC] Control de los accesos físicos		L3	L4
[E.4] Personal subcontratado		L2	L4
[HW] Protección de los Equipos informáticos		L2	L4
[H.AU] Registro y auditoría		L1	L4
[H] Protecciones generales		L2	L4

Cuadro 12. EVSA

Se evidencia en el Cuadro 12 que las salvaguardas no tienen los niveles adecuados para abordar una amenaza de manera pertinente, indicativo del descuido por parte de la institución hacia la seguridad e integridad de la información. Con base en la información del MOVA, MARI y EVSA se calculó la ESTRI que enfrenta la institución, con el fin de definir políticas que permitan disminuir y mitigar el impacto que generan las amenazas planteadas en los procesos administrativos y académicos. Adicionalmente, se desarrolló la ESTRI considerando el impacto, riesgo potencial y residual de las amenazas sobre los activos de la institución. En relación con la

estimación de riesgo realizada se definen los riesgos que se encuentran en estado crítico o grave, entre los cuales se encuentran:

USNOPRE: Esta amenaza se presentó de forma recurrente en el análisis, con una alta probabilidad de ocurrencia. Los activos que pueden ser afectados por esta amenaza y son relevantes para la organización son: El sistema operativo, navegador web, computadores administrativos, computadores educativos y el internet. Por lo anterior, esta amenaza se encuentra controlada con varias salvaguardas, sin embargo, se deben implementar actividades de mejora en el sistema con el fin de conseguir menos riesgos. En este sentido, se definen recomendaciones y políticas de seguridad que reducen probabilidad de ocurrencia de estas amenazas:

• Hacer uso de una versión licenciada de Windows profesional, preferiblemente las más recientes y hacer uso de la administración de privilegios que estas ofrecen para acotar los accesos de las cuentas de estudiantes, docentes e invitados.

• Crear puntos de recuperación del sistema para proteger la configuración de los equipos y la integridad del sistema operativo.

• Crear un manual de uso de los equipos de cómputo para los integrantes de la comunidad y realizar su respectiva socialización.

• Establecer cuentas de acceso usando la administración de los directorios activos de Windows server. (Esta solución solo aplica para las oficinas administrativas).

• Programar capacitaciones para fortalecer el buen uso de las tecnologías, incluyendo los sistemas operativos, servicios web y ofimática.

• Fomentar el uso de ambientes digitales por medio de la comunicación y la motivación.

• Utilizar bloqueos de publicidad en los navegadores para evitar la probabilidad de que caigan en la técnica de suplantación de identidad 'Phishing'.

• Implementar políticas de bloqueo en el firewall de la red para fortalecer el buen uso del internet, realizar constantes monitorias a los bloqueos más comunes del sistema.

• Definir un procedimiento para el seguimiento de las fallas más comunes por mal uso que se pueda estar realizando.

CSAR: afecta varios activos del sistema, entre los cuales se encuentran algunos que están expuesto a un alto riesgo: El servidor, Firewall y Accespoints. Cada componente responde a servicios de red esenciales por lo cual deben poseer un nivel alto de protección para evitar desborde de memoria en sus sistemas y una falla en su disponibilidad. Debido a su importancia para la organización se presentan las medidas de seguridad para disminuir el impacto y su probabilidad de ocurrencia:

• Implementar alertas de seguridad en el servidor en caso de que los recursos estén llegando a grandes niveles de uso.

• Definir puntos de control tanto en el servidor como en los Accespoint para el servicio DHCP, dependiendo del tipo de uso por dispositivo.

• Definir un procedimiento de monitoreo a los niveles de los recursos de los activos que sean pertinentes.

• Establecer un pool de direcciones estáticas a los dispositivos de alta prioridad en la red.

• Establecer sistemas de recuperación y respaldo en caso de fallas.

DESE: La DESE, del mismo modo que la caída por agotamiento de recursos, influye en la disponibilidad de los dispositivos de red. En este caso, el riesgo crítico afecta al servidor y servicio de red local, y la necesidad de aplicar medidas como las siguientes:

• Políticas de acceso en cada uno de los dispositivos dentro de la red local y establecer privilegios de acuerdo al nivel.

• Asegurar que las contraseñas de la administración de sistemas tengan un alto nivel de protección.

• Implementar un sistema de monitoreo sobre los accesos no autorizados.

• Usar técnicas de encriptación en las contraseñas de administración.

ACNOAU: El ACNOAU es una amenaza grave para los activos en la organización, entre los cuales se encuentran: Los puntos de acceso, computadores de uso administrativo y la red local. Estas amenazas presentan un comportamiento diferente de acuerdo a los activos que afecta. A continuación, se describen las políticas y medidas requeridas para mitigar este riesgo:

• Creación de contraseñas en cada dispositivo instalado.

• Ubicar los dispositivos de red en zonas elevadas de las habitaciones.

• Para proteger la red se deben desactivar los puertos de red que no sean utilizados por ningún dispositivo.

• Se deben activar opciones de registro de logs para verificar si se realizó un ACNOAU.

• Se debe diseñar un procedimiento para hacer seguimiento a este riesgo en específico.

• Establecer un manual de buenas prácticas para la seguridad informática.

• Realizar capacitaciones y socialización del manual para reforzar la cultura de la seguridad de la información.

Lo descrito, denota que las amenazas relacionadas con la interacción de los usuarios y el ambiente laboral son las más comunes. Por lo cual, la organización debe prestar especial atención a la promoción y capacitación del uso de equipos informáticos. No obstante, de manera general el sistema presenta niveles de estimación controlados, con la necesidad de estudiar de manera más detallada su comportamiento, con el fin de conocer factores determinantes en su gestión. La creación de procedimientos de medición permitirá analizar las amenazas calificadas como apreciables dentro del sistema, permitiendo en una siguiente iteración el entendimiento de su afectación y determinar con mayor efectiva su tratamiento. En este sentido, la aplicación de controles de acuerdo a los activos, amenazas y dimensiones contempladas por la organización permite medir la efectividad de las políticas y controles aplicados en sus procesos, mediante la retroalimentación del análisis de riesgos donde se visualicen los peligros a los cuales está expuesto (Enríquez y Hidalgo, 2015).

Considerando lo descrito se puede establecer que la institución educativa para sus procesos de gestión de la infraestructura tecnológica tiene necesidades por resolver, con el fin de garantizar la seguridad informática en sus actividades. Uno de los puntos destacados es la falta de cultura en la aplicación de tecnologías la cual ocasiona riesgos que se pueden controlar con re-inducciones y la promoción de capacitación continua. Por otra parte, la institución posee una alta dependencia de las TIC, esto produce obligación de incluir mecanismos para la disponibilidad de estas herramientas, mediante la creación de medidas de protección, mejora de infraestructura y desarrollo de mejores políticas de usabilidad.

Por último, se destaca la buena relación de la institución con los sistemas de gestión de calidad y los SGSI, puesto que a nivel organizacional posee una estructura documentada sólida de un SGC, que facilita el control de versión de documentos y genera un buen acoplamiento con la implementación del SGSI. Esto presenta similitud con lo expuesto por Martelo, Madera y Betín (2015), porque mencionan que para la utilización adecuada de un SGSI es necesario resolver problemas en los procesos de descentralización y desorganización de la información que se produce en las actividades de la institución, lo cual ocasiona una elevada complejidad para el desarrollo de la SGSI.

Conclusiones

De acuerdo a los resultados obtenidos se definen las siguientes conclusiones: 1) se establecieron actividades de organización documental del proceso y los activos involucrados en el análisis de riesgos y la inclusión de responsabilidades que responden a los requerimientos de los activos de la organización. 2) Con el análisis realizado, se identificaron amenazas que representaron el mayor riesgo para los activos, resaltando aquellas reiterativas de manera transversal en el proceso y a la organización, con factores causales como el USNOPRE, CSAR, DESE y el ACNOAU. 3) Se definió un plan para el tratamiento y la gestión de riesgos que facilita la protección de la infraestructura, con el cual se establecen mecanismos de detección y alertas que mitigan sus efectos en la organización. Lo anterior permite un seguimiento comportamental, para adoptar procesos de mejora continua y seguimiento en la institución. 4) La implementación de documentos, formatos y registros requeridos en la organización permite aumentar los niveles de seguridad de la información institucional, mediante la determinación de indicadores de desempeño que se configuran en el ciclo laboral de quienes hacen parte de la gestión documental en la institución, fundamentados en la flexibilidad de la normal 27001.

Referencias bibliográficas

Ahmad, A., Maynard, S. B., y Park, S. (2012). Information security strategies: towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing*, 25(2), 357–370.

Babbie, E. (2011). *The Basics of Social Research*, Fifth Edition. Belmont, CA: Wadsworth Publishing Group.

Bozalek, V., Ng'ambi, D. y Gachago, D. (2013). Transforming teaching with emerging technologies: Implications for higher education institutions. *South African Journal of Higher Education*, 27(2), 419-436.

Bravo, M., y Yoo, S. (2019). Developing an Information Security Management System for Libraries Based on an Improved Risk Analysis Methodology Compatible with ISO/IEC 27001. *1st International Conference on Advances in Emerging Trends and Technologies* (págs. 371-379). Quito: Springer. doi:10.1007/978-3-030-32033-1_34.

Budel, D., Turek, I. y Cichon, S. (2015). Multidimensional management of a higher education institution. *International Journal of Arts & Sciences*, 08(02), 199–213.

Chander, M., Jain, S. y Shankar, R. (2013). Modeling of information security management parameters in Indian organizations using ISM and MICMAC approach. *Journal of Modelling in Management*, 8(2), 171-189.

Christensen, L., Burke, R. y Turner, L. (2015). *Research Methods, Design, and Analysis*. Harlow: Pearson Education Limited.

Enríquez, V. y Hidalgo, P. (2015). Metodología de Valuación de Riesgos Como Parte del Sistema de Gestión de Seguridad de la Información (SGSI) Aplicado a un Data Center de Alta Gama. *Revista Politécnica*, 36(1), 45.

García, F., y Moreta, L. (2018). Modelo de Madurez para el Análisis de Riesgos de los Activos de Información basado en las Metodologías MAGERIT, OCTAVE y MEHARI; con enfoque a Empresas Navieras. *7th International Conference on Software Process Improvement*, (págs. 29-39). Jalisco. doi:10.1109/CIMPS.2018.8625848.

Kalpeyeva, Z.B. y Mustafina, A.K. (2013). IT-infrastructure of university based on cloud computing. *IJCSI International Journal of Computer Science Issues*, 10 (5-1), 176-179.

Imaquingo, D., Herrera-Granda, E., Herrera-Granda, I., Arciniega, S., Verónica, G., y MacArthur, O.-B. (2019). Evaluación de sistemas de seguridad informáticos universitarios Caso de Estudio: Sistema de Evaluación Docente. *Revista Ibérica de Sistemas e Tecnologias de Informação*, 8(E22), 349-362.

Kim, E. B. (2013). Recommendations for information security awareness training for college students. *Information Management & Computer Security*, 22(1), 115–126.

Leavy, P. (2017). *Research design, quantitative, qualitative, mixed methods, arts-based, and community-based participatory research approaches*. Nueva York: The Guildford Press.

Martelo, R., Madera, J. y Betín, A. (2015). Software para Gestión Documental, un Componente Modular del Sistema de Gestión de Seguridad de la Información (SGSI). *Información tecnológica*, 26(2), 129-134.

Martelo, R., Tovar, L. y Maza, D. (2018). Modelo Básico de Seguridad Lógica. Caso de Estudio: el Laboratorio de Redes de la Universidad de Cartagena en Colombia. *Información tecnológica*, 29(1), 3-10.

Molina-Miranda, M. (2017). Análisis de riesgos de centro de datos basado en la herramienta pilar de mageritanálisis de riesgos de centro de datos basado en la herramienta pilar de magerit. *Espirales revista multidisciplinaria de investigación*, 1(11), 1-11.

Narain, A., Picot, A., Kranz, J., Gupta, M.P. y Ojha, A. (2013). Information Security Management (ISM) Practices: Lessons from Select Cases from India and Germany. *Global Journal of Flexible Systems Management*, 14, 225–239.

Ortiz-Lazo, J., y Vizñay, J. (2019). Análisis de riesgo y vulnerabilidades de la red de datos, en un ISP, utilizando el estándar ISO/IEC 2007:2008. Caso de estudio: Empresa Sistelcel. *Polo del Conocimiento: Revista científico - profesional*, 4(7), 174-195.

Raed, L., Mohamed, H., y Tai-Hoon, K. (2014). Quantitative Risk Management for Communication and Information Systems: State-of-the-Art and Challenges. *7th International Conference on Advanced Software Engineering & Its Applications*. Haikou: Institute of Electrical and Electronics Engineers Inc. doi:10.1109/ASEA.2014.16.

Rivera, J., Herrera, V., Naranjo, X., y Narváez, C. (2019). Gestión de Riesgos de TIC en hospitales públicos. *Revista Iberica de Sistemas e Tecnologias de Informacao*, 2019(E20), 280-291.

Porter, W., Graham, C., Spring, K. y Welch, K. (2014). Blended learning in higher education: Institutional adoption and implementation. *Computers & Education*, 75, 185-195.

Sastoque, J., Restrepo, L. y Castro, A. (2019). Diseño de modelo financiero para análisis de NIC 41 y la información contable en empresas ganaderas bovinas. En E. Martínez, A. Antúnez, J. Luna, V. Meriño, C. Martínez, I. Rincón (Comp), *Gestión del conocimiento perspectiva multidisciplinaria. Vol.12* (pp. 159-182). Zulia, Venezuela: Fondo Editorial Universitario de la Universidad Nacional Experimental Sur del Lago Jesús María.

Tejena-Macía, M. (2018). Análisis de riesgos en seguridad de la información. *Polo del Conocimiento: Revista multidisciplinar de innovación y estudios aplicados*, 3(4), 230-244.

Tubío, P., López, C., y Rivas, J. (2020). Improving information security risk analysis by including threat-occurrence predictive models. *Computers and Security*, 88, 1-10. doi:doi.org/10.1016/j.cose.2019.101609.

Velasco, J., Ullauri, R., Pilicita, L., Jacome, B., Saa, P., y Moscoso-Zea, O. (2018). Benefits of implementing an ISMS according to the ISO 27001 standard in the ecuadorian manufacturing industry. *3rd International Conference on Information Systems and*

Computer Science (págs. 294-300). Quito: Institute of Electrical and Electronics Engineers Inc. doi:10.1109/INCISCOS.2018.00049

Vicente, E., Mateos, A., y Jiménez-Martín, A. (2014). Risk analysis in information systems: A fuzzification of the MAGERIT methodology. *Knowledge-Based Systems*, 66, 1-12. doi:10.1016/j.knosys.2014.02.018.