Dom. Cien., ISSN: 2477-8818
Vol. 8, núm. 2. Abril-Junio, 2022, pp. 139-164



DOI: http://dx.doi.org/10.23857/dc.v8i1.2638

Ciencias de la Educación
Artículo de Investigación

# *Política de seguridad para acceso a la red LAN de la Universidad de Cuenca*

# *Security politics for access to the Universidad de Cuenca LAN network*

# *Política de segurança para acesso à rede LAN da Universidade de Cuenca*

Diego Fernando Paredes-Beltrán [I]
diego.paredes.53@est.ucacue.edu.ec
https://orcid.org/0000-0002-9662-5544

Jorge Fernando Illescas-Peña [II]
jorge.illescas@ucacue.edu.ec
https://orcid.org/0000-0001-9316-1118

**Correspondencia:** diego.paredes.53@est.ucacue.edu.ec

*__Recibido:__ 25 de febrero del 2022 *__Aceptado:__ 19 de marzo de 2022 __* Publicado:__ 01 de abril de 2022

I. Estudiante de la Maestría en Ciberseguridad, Universidad Católica de Cuenca, Cuenca, Ecuador.
II. Docente de la Maestría en Ciberseguridad, Universidad Católica de Cuenca, Cuenca, Ecuador.

## Resumen

Los ataques y problemas de seguridad en una empresa se generan tanto desde el interior como del exterior de la misma, pero en muchos casos se preocupa menos de la red interna, ya que las empresas la consideran segura y menos vulnerable. En el presente artículo, se define una política de seguridad para la red LAN de la Universidad de Cuenca mediante el marco de trabajo MaGMa y apegado a la norma ISO/IEC 27001. Se aplica el marco de trabajo MaGMa para cuantificar la posición que tiene la Universidad de Cuenca con respecto al control del acceso a su red interna. Los resultados demuestran que la Universidad tiene hoy una implementación limitada para el caso de uso indicado, así como un gran potencial de crecimiento con inversión en herramientas que mejoren los controles a la red. Con esta información se plantean puntos para ser agregados a las políticas generales de la seguridad de la información de la Universidad de Cuenca, acorde a las necesidades de la institución, generando buenas prácticas en el control de acceso a usuarios, visibilidad horizontal y vertical del tráfico de usuarios para predecir huecos de seguridad, vulnerabilidades y evitar ataques informáticos mediante recolección, análisis de logs y correlación de eventos.

**Palabras clave:** Seguridad de la información; NAC; políticas de seguridad; ciberseguridad; MaGMa; SGSI; SOC.

## Abstract

Security issues and attacks inside an organization are caused due to internal and external factors, however in most cases it concerns less about internal network, as organizations consider it enough secure and less vulnerable. In this document, security policies are defined for the Local Area Network of Universidad de Cuenca, with MaGMa framework and complying with ISO/IEC 27001 standard. MaGMa framework is applied in order to quantify its position towards the control of internal network. Results show that Universidad de Cuenca has a limited implementation for this use case, hence a great potential of growth with the adequate investment in technology and tools that upgrades the network controls. This information is used to créate new statements to be attached to the general information security policies document of Universidad de Cuenca, along with the institution needs, fostering Access control best practices, horizontal and vertical sight of network user traffic for security gaps and vulnerabilities detection, and prevent cyberattacks with data collection and analysis as well as events correlation.

**Keywords:** Information Security; NAC; security policies; cybersecurity; MaGMa; ISMS; SOC.

## Resumo

Ataques e problemas de segurança em uma empresa são gerados tanto de dentro quanto de fora dela, mas em muitos casos ela se preocupa menos com a rede interna, pois as empresas a consideram segura e menos vulnerável. Neste artigo, uma política de segurança para a rede LAN da Universidade de Cuenca é definida através da estrutura MaGMa e anexada à norma ISO/IEC 27001. A estrutura MaGMa é aplicada para quantificar a posição da Universidade de Cuenca em relação ao controle de acesso à sua rede interna. Os resultados mostram que a Universidade hoje possui uma implementação limitada para o caso de uso indicado, bem como um grande potencial de crescimento com investimento em ferramentas que melhoram os controles de rede. Com essas informações, propõe-se adicionar pontos às políticas gerais de segurança da informação da Universidade de Cuenca, de acordo com as necessidades da instituição, gerando boas práticas no controle de acesso de usuários, visibilidade horizontal e vertical do tráfego de usuários para prever falhas de segurança , vulnerabilidades e prevenir ataques de computador coletando, analisando logs e correlacionando eventos.

**Palavras-chave:** Segurança da informação; NAC; política de segurança; cíber segurança; Magma; SGSI; SOC.

## Introducción

Como describe (Doig Díaz et al., 2019) la transformación digital y el incremento de uso de información y medios para utilizarla son más diversos y globales, por ello, la información personal y corporativa están expuestas a varios niveles de acceso, incrementando el riesgo de robo de información. Este riesgo puede materializarse debido a errores humanos, los cuales son aprovechados por ciberdelincuentes por lo que es necesario tomar medidas de seguridad que aseguren la información de la empresa.

En este sentido es importante generar políticas de seguridad de la información que vayan acorde al avance tecnológico, así como al giro del negocio de cada empresa. El objetivo de la seguridad de la información es garantizar el correcto desarrollo de los procesos del negocio protegiendo los sistemas de manera adecuada. Una protección fiable en el ámbito informático permite mejorar la percepción de los usuarios hacia la empresa, las políticas sirven de apoyo para identificar de manera temprana riesgos y generar de manera adecuada los controles necesarios para mantener la adecuada protección

mejorando la imagen empresarial, además de la reputación y confianza de los usuarios apoyando el crecimiento estratégico. El objetivo principal de una política de seguridad es garantizar la continuidad del negocio, y prevenir los incidentes de seguridad que se puedan presentar con el fin de mantener la confidencialidad, integridad y disponibilidad de la información importante de la empresa. La importancia de las políticas de seguridad de la información y la gestión de vulnerabilidades se ha vuelto tan importante como la misma información, como dice (Alonso Ricardo et al., 2019) hoy en día, la seguridad de la información juega un papel muy importante en las organizaciones bien sean pequeñas, medianas o grandes.

En general, muchas de ellas olvidan la importancia e incluso en algunas ocasiones la seguridad es algo desconocido, así como para el recurso humano responsabel de los procesos estratégicos de la Universidad de Cuenca.

## Referencial teórico

### Normativas ecuatorianas sobre seguridad de la información

La Universidad de Cuenca, al ser una entidad pública, tiene la obligación de cumplir con las normativas legales impuestas por los diferentes organismos de control. Por ello, para la generación de políticas, se consideran las siguientes normativas legales:

El artículo 1 de la Ley Orgánica de Protección de Datos Personales dispone que *"El objeto y finalidad de la presente ley es garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección. Para dicho efecto regula, prevé y desarrolla principio, derechos, obligaciones y mecanismos de tutela".*

Las Normas de Control Interno de la Contraloría General del Estado en su sección 410-04 establece que *"La máxima autoridad de la entidad aprobará las políticas y procedimientos que permitan organizar apropiadamente el área de tecnología de información y asignar el talento humano calificado e infraestructura tecnológica necesaria"* y su sección 410-10 establece requisitos de Seguridad de tecnología de información.

Por último, la Constitución de la República en su artículo 66 numeral 19 reconoce *"El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo,*

*procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley"*

**Seguridad de la Información**

**Información y Datos Sensible en una organización.** Las organizaciones deberían preocuparse por la información financiera, la propiedad intelectual, los detalles de empleados o la información confiada por terceros. Algunos ejemplos de datos que las organizaciones deben proteger son:

- Información financiera - Números de tarjetas de crédito, números de cuentas bancarias, etc.
- Propiedad intelectual - Secretos comerciales, diseños de productos, planes de marketing, etc.
- Detalles de empleados, docentes y estudiantes - Nombres, direcciones, salarios, horarios de cursos, calificaciones, modelos de examen etc.
- Información confiada por terceros - Datos de clientes, información confidencial producto de acuerdos, etc.

En el caso de la Universidad de Cuenca, además de su personal administrativo, docente e investigador, tiene bajo su responsabilidad la conectividad de los 16.000 estudiantes que se forman en la institución, Estos a su vez, representan un tráfico potencialmente hostil para a la infraestructura e información sensible de la Universidad. Es por ello que también se deben establecer y ejecutar procedimientos para la protección de los datos personales de todos y cada uno de los estudiantes matriculados en la Universidad.

**Centro de Operaciones de Seguridad (SOC).** Un centro de operaciones de seguridad (SOC) es el equipo o departamentodonde los profesionales de seguridad pueden monitorear y analizar la seguridad de las redes y sistemas de una organización. Los miembros del SOC utilizan una variedad de herramientas y técnicas para detectar ataques e intrusión, y luego analizarlos para determinar su origen y gravedad.

Mediante la implementación de un SOC, las organizaciones pueden mejorar su postura en materia de seguridad en general gracias a que disponen de un equipo dedicado exclusivamente al monitoreo y análisis de la seguridad de las redes y sistemas de la organización. El equipo SOC también puede colaborar con otras partes de la organización para ayudar a mitigar cualquier amenaza que sea identificada.

**Análisis de Riesgos en Seguridad.** El análisis de riesgos en seguridad de la información como menciona (Estupiñan et al., 2013) es una excelente herramienta para generar planes de contingencia y continuidad del negocio, debido a que permite a las empresas mitigar el riesgo y garantizar el rendimiento de los sistemas informáticos.

Aunque es imposible eliminar por completo el riesgo, un correcto análisis de riesgos no ayuda a minimizarlos de tal manera que no generen un daño mayor a los sistemas de información.

**Ataques Informáticos Comunes.** Al tener acceso a Internet, los usuarios de una organización están expuestos constantemente a varias amenazas informáticas (Maroto, 2009). En estos días, tener una red corporativa sin ningún mecanismo de seguridad informática representa un altísimo riesgo de ser víctima de robo de datos confidenciales, tales como contraseñas y números de tarjetas de crédito. Otros ataques pueden incluir el robo de información sobre clientes o empleados, sabotaje informático para causar daños graves a una empresa, o intentar obtener acceso ilegal a sistemas protegidos.

En el caso de las personas particulares, el robo de identidad es un problema cada vez más común. Los ladrones pueden obtener fácilmente la información necesaria para usurpar la identidad de una persona a través de diversas vías (Internet, correo electrónico no deseado, phishing, redes sociales, etc.), lo que les permite realizar transacciones fraudulentas en su nombre o acceder a sus cuentas bancarias u otros servicios.

**Malware**. Los ataques de malware son una amenaza seria para las empresas ya que pueden causar daños extensivos en los sistemas y datos datos (Kokulu y col., 2019). Además, el malware es difícil de detectar y eliminar, por lo que es importante que las organizaciones tengan un plan de seguridad completo que incluya software antivirus y otras medidas de protección.

Algunos signos evidentes de que una organización está experimentando un ataque de malware incluyen:

- Caída inesperada o degradación en el rendimiento de un servidor o pc de cualquier miembro.
- Archivos o programas no autorizados que aparecen en los sistemas.
- Mensajes del software antivirus indicando que se ha detectado malwareen el sistema.

Los ataques de malware pueden resultar en la pérdida o destrucción de datos, pérdidas financieras y daños a la reputación de una organización. Además, las infecciones de malware pueden ser difíciles

de detectar y eliminar, por lo que a menudo causan daño a largo plazo en los sistemas y datos de una organización.

Los ataques de malware pueden ser prevenidos mediante la instalación de software antivirus en todos los sistemas y dispositivos, y manteniéndolo actualizado. Además, las organizaciones deben tener un plan de seguridad integral en marcha que incluya otros medidas de protección como cortafuegos, sistemas de detección de intrusiones y soluciones para filtrar spam.

**Ataque de denegación de servicio DDoS.** Un ataque DDoS es un tipo de ataque en el que el atacante busca sobrecargar la red de una organización con tráfico procedente de múltiples fuentes. Esto puede causar que la red se sobrecarge y sea inusable, impidiendo a usuarios legítimos acceder al sistema o a los datos.

Los ataques DDoS están convirtiéndose en más comunes y sofisticados, por lo que es importante para las organizaciones tener medidas en place para protegerse contra ellos. Una forma de hacerlo es utilizando un servicio que pueda filtrar el tráfico ilícito e impedir que la red se sobrecargue.

Algunos signos comunes de advertencia de que una organización podría estar experimentando un ataque DDoS incluyen un aumento repentino en el tráfico de la red asi como la lentitud en las respuestas o incapacidad para acceder a websites o servicios.

Un ataque DDoS puede impedir el acceso legítimo de usuarios a los sistemas o datos de una organización, lo que puede causar considerable disrupción en las operaciones institucionales, pérdida financiera y de datos. Los ataques DDoS pueden ser prevenidos mediante el uso de un servicio que pueda filtrar el tráfico ilegal y prevenir la red de colapsarse. Además, las organizaciones deben asegurarse de tener un ancho de banda suficientemente grande para manejar grandes cantidades de tráfico si están esperando un ataque DDoS.

**Ataque por fuerza bruta**. Un ataque por fuerza bruta es un tipo de ataque en el que el atacante usa herramientas automatizadas para intentar adivinar las credenciales de acceso a sistemas o datos de una organización. Si el atacante tiene éxito, podrá obtener acceso al sistema y robar o dañar información.

Los ataques por fuerza bruta son una forma común de acceder a los sistemas y datos, por lo que es importante que las organizaciones tengan políticas de contraseñas sólidas en lugar para hacer más difícil para los atacantes puedan adivinar las contraseñas. Además, las organizaciones deben usar

medidas de autenticación como la autenticación de dos factores que hagan más difícil para los atacantes entrar en el sistema.

Los ataques de fuerza bruta pueden resultar en el robo de credenciales de inicio de sesión, lo que puede ser utilizado por los atacantes para obtener acceso a sistemas y datos. Además, ataques de fuerza bruta también pueden causar pérdidas financieras o daños a la reputación de una organización. Los ataques de fuerza bruta pueden ser prevenidos mediante la utilización de contraseñas fuertes, y mediante el uso de medidas de autenticación como la autenticación en dos factores.

**Phishing**. El fraude por correo electrónico o phishing es un tipo de ataque en el que el atacante envía mensajes fraudulentos por correo electrónico o mensajes de texto con el objetivo de engañar a los usuarios para que revelen sus credenciales de inicio de sesión o información sensible. El objetivo del ataque por phishing es obtener acceso a los sistemas y datos de una organización, por lo que es importante que los usuarios estén conscientes de los signos que indican que un email puede ser una estafa. Los ataques de phishing pueden resultar en el robo de información sensible como contraseñas, números de tarjetas de crédito y números de seguridad social. Esta información puede ser utilizada por los atacantes para obtener acceso a sistemas y datos o para cometer fraudes identities.

Algunos de los signos más comunes que indican que un correo electrónico puede ser un ataque por phishing incluyen:

- Mensajes urgentes que solicitan información personal, como contraseñas o números de tarjetas de crédito.
- Enlaces o archivos adjuntos que aparentemente provienen de fuentes legítimas pero en realidad son maliciosos.
- Errores ortográficos y gramaticales en el cuerpo del correo electrónico.
- Solicitudes para información confidencial que se envían a través de correos electrónicos no solicitados o mensajes de texto.

Los ataques por phishing pueden ser prevenidos mediante la educación de los empleados sobre cómo identificar correos electrónicos sospechosos y enseñándoles que no hagan clic en enlaces ni abran archivos adjuntos de fuentes desconocidas. Una adecuada gestión de certificados de seguridad políticas de firewall del lado del equipo SOC contribuye a mantener el orden y la confianza de los usuarios.

**Ataque por ingeniería social**. Un ataque por ingeniería social es un tipo de ataque en el que un atacante usa el engaño para obtener información de usuarios incautos. A menudo, los ataques por ingeniería social involucran técnicas como llamadas telefónicas, correos electrónicos o conversaciones en persona en las que el atacante intenta engañar al usuario para que le dé información sensible.

Los ataques por ingeniería social son muy efectivos debido a que explotan la naturaleza humana y nuestra propensión natural a confiar en los demás. Las organizaciones deberían educar a sus empleados sobre los peligros de los ataques por ingeniería social y cómo detectarlos antes de que puedan hacer daño.

Algunos signos comunes de advertencia que un correo electrónico o conversación puede ser un ataque por ingeniería social incluyen:

- Llamadas telefónicas extrañas de personas que afirman ser de organizaciones legítimas, pero que en realidad están tratando de obtener información sensible.
- Solicitudes inesperadas de información personal, como contraseñas o números de tarjetas de crédito.

Los ataques por ingeniería social pueden resultar en el robo de información sensible, como contraseñas, números de tarjetas de crédito y números de seguridad social. Además, los ataques por ingeniería social también pueden causar pérdida financiera o daño a la reputación de una organización.

En la Universidad, los ataques por ingeniería social se pueden prevenir educando a empleados, docents y estudiantes sobre los peligros de las estafas por ingeniería social y enseñándoles cómo detectarlos.

## Metodología

Dentro de una organización es necesario establecer herramientas, metodologías y marcos de referencia para definir acciones y procesos que todos los miembros de las diferentes áreas puedan aplicar. La seguridad de la información no es la excepción, por lo cual se requiere la definición de una metodología que sirva de guía a la hora de planear, implementar y monitorear las acciones de seguridad.

Existen diversas metodologías para la seguridad de la información, cada una con sus propias características y fortalezas. Entre ellas, se ha escogido el marco de referencia con la herramienta MaGMa, ya que se presenta como una herramienta para identificar cuán bien una organización se defiende frente a amenazas contra la seguridad de la información (van Os, 2020 [Online])

**MaGMa.** Acrónimo de Gestión, Crecimiento y Evaluación por sus siglas en inglés, es un marco de referencia diseñado para definir y tener control sobre amenazas de bajo y alto nivel, y todo el procedimiento y herramientas para hacerles frente, lo que se conoce como casos de uso.

**Ciclo de vida del caso de uso MaGMa.** El objetivo de la MaGMa es dotar a las organizaciones con un conjunto claro y coherente de procesos, procedimientos y prácticas que les permitan garantizar que los datos estén protegidos contra amenazas internas y externas. La metodología define las siguientes etapas:

- Planificación y Construcción: En este paso se identifican y evalúan todas las amenazas a la seguridad de la información, así como los riesgos relacionados. También se determinan los objetivos de seguridad y el nivel deseado de protección para cada categoría de datos. Durante este paso se definen los controles necesarios para cumplir con los objetivos planteados en el análisis anterior. Esta etapa incluye tanto controles operacionales como tecnológicos.
- Fase Operacional: En esta etapa se ponen en marcha los controles diseñados en el paso anterior, junto con medidas para mitigar posibles riesgos asociados al mismo. También hay que considerar aquí la formación del personal encargado del cumplimiento con las políticas y procedimientos establecidos dentro del marco MaGMa.
- Mantenimiento: Una vez implementados, es importante mantener un seguimiento constante de los controles para asegurarse de que siguen siendo efectivos. Esta etapa también incluye la realización de auditorías periódicas para verificar el cumplimiento con las políticas y procedimientos establecidos.
- Desmontaje Cuando finalice el ciclo de vida de la información, es necesario desmontar los controles implantados y proceder a su destrucción o eliminación.

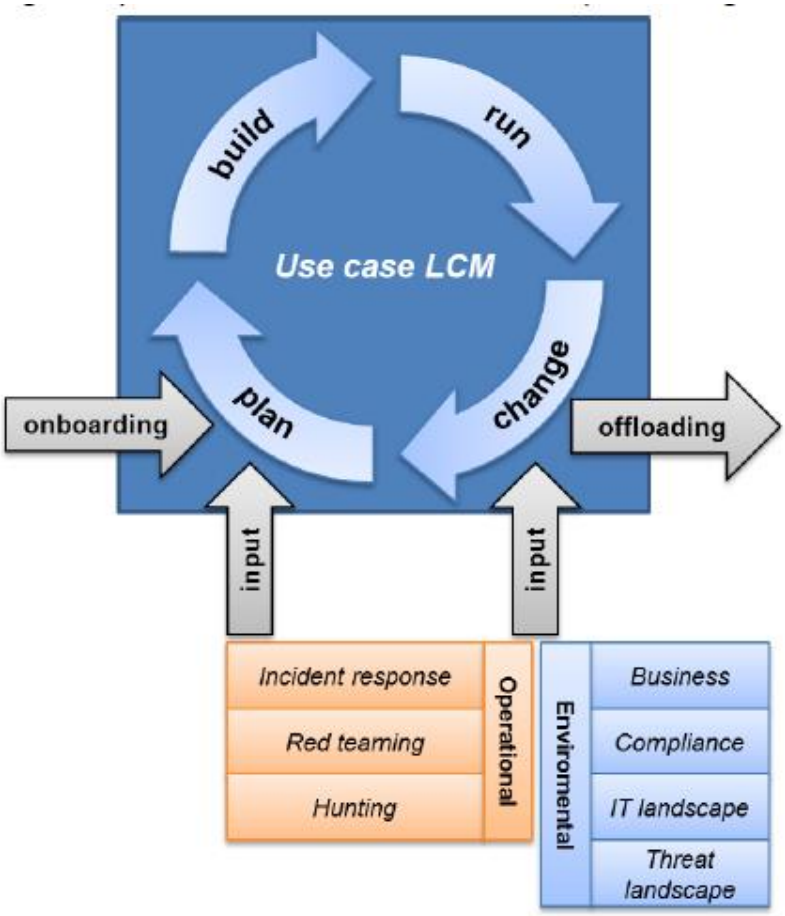


**Figura 1.** Ciclo de vida de un caso de uso.

**Herramienta MaGMa y su aplicación dentro de una organización.**

**Modelo MaGMa.**

En cada caso de uso se deben definir los elementos que lo conforman. Los elementos se clasifican en tres capas:

Capa de negocio. Hace referencia a los elementos que obedecen a las necesidades de la organización. Se define el proósito del caso de uso así como los sectores interesados.

Capa de amenaza. Define hacia qué amenaza se hace frente.

Capa de implementación Consiste en las operaciones que serán realizadas para hacer frente al problema. Se definen las herramientas y los mecanismos para el monitoreo, detección y estudio de las amenazas.

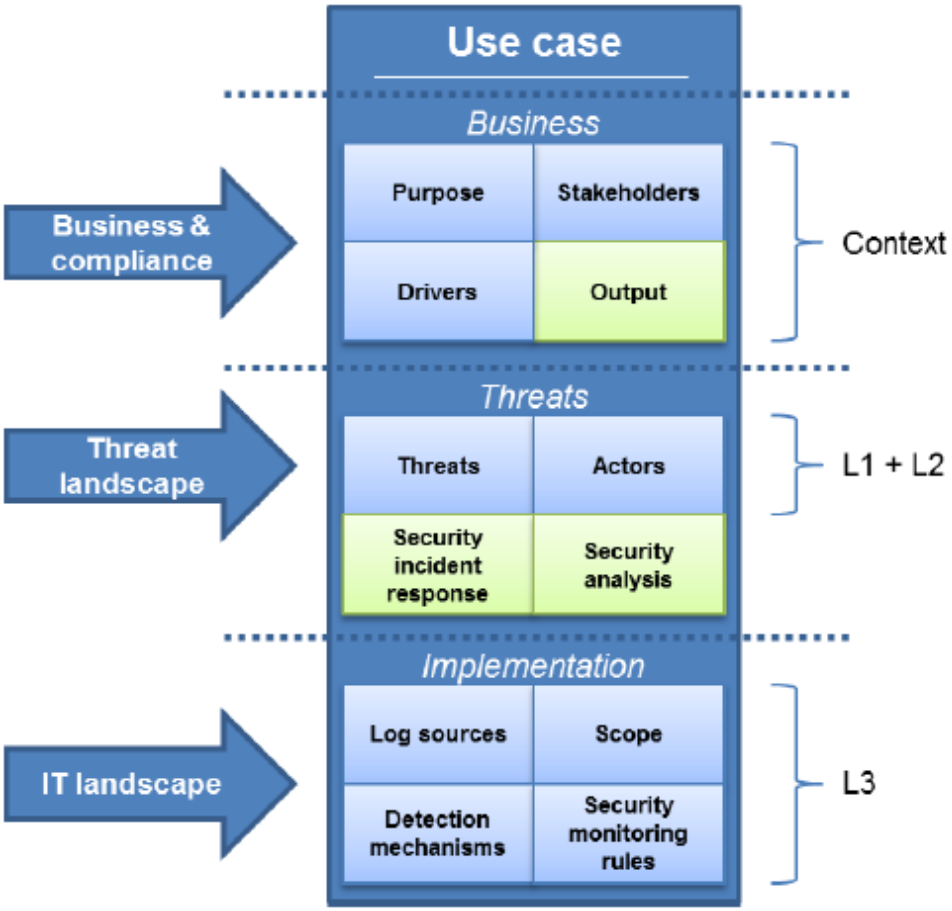


**Figura 2.** Modelo de caso de uso.

**Aplicación de casos de uso.** Para hacer una aplicación correcta de la herramienta, esta viene con un número predeterminado de casos de uso L1, L2 y L3, los cuales son interrelacionados y se encuentran contenidos dentro de las capas de amenaza e implementación.

Casos de uso L1. Casos de uso que describen situaciones transversales a todos los departamentos de la organización.

Casos de uso L2. Casos de uso que describen amenazas puntuales, las cuales están relacionadas y contenidas en un caso de uso L1.

Casos de uso L3. Casos de uso que describen las acciones, herramientas y tecnología implementadas a nivel operacional para hacer frente a una amenaza específica, descrita en la lista de casos de uso L2.

Como se ha mencionado, la herramienta MaGMa, viene contenida con varios casos de uso predeterminados, entre los cuales se cuentan 12 casos de uso L1, 62 casos de uso L2 y 169 casos de uso L3. Entre los casos de uso L1 se cuentan las 7 fases del modelo Cyber Security Kill Chain (Hutchins y col., 2011), y los casos de uso L3 están basados en la matriz MITRE ATTCK elaborada para uso empresarial (Strom y col., 2018).

Para aplicar estos casos de uso se hace uso de las siguientes métricas:

- Efectividad. Métrica. que busca cuantificar la efectividad del mecanismo de detección de una amenaza. Un ejemplo es la alta efectividad que tiene un antivirus local en detectar malware y troyanos en la red, pero baja efectividad en filtrar tráfico.
- Implementación. Determina a qué nivel el mecanismo de detección está implementado. Por ejemplo, una herramienta de firewall perimetral no está implementada al 100% si no tiene configuradas las políticas de forma correcta.
- Cobertura. Con esta métrica se quiere cuantificar el alcance que tiene el mecanismo de detección sobre la amenaza. En el caso del firewall perimetral, este tiene una cobertura del 100% si todo el tráfico de la empresa esta enrutado para pasar a través de él.
- Peso. Esta métrica se computa a partir de las métricas de efectividad, implementación y cobertura.
- Potencial. Nos indica cuánto puede mejorar la organización si se invierte en herramientas que mejoren las medidas de implementación y cobertura, y es obtenida a partir del cálculo de ellas.

En la herramienta, un caso de uso L1 tiene *X* casos de uso L2 relacionados y un caso de uso L2, a su vez, tiene *Y* casos de uso L3 relacionados. Dicho esto, los valores de las métricas de efectividad, implementación y cobertura deben ser ingresadas a nivel de un caso de uso L3, basado en la información y estimación del equipo SOC, y a partir de estos datos se calculan las métricas de los casos de uso L1 y L2 de forma automática.

## Resultados y discusión

### Definición Casos de Uso

Para relacionar la herramienta MaGMa con los requerimientos de la Universidad de Cuenca, se han creado nuevos casos de uso L1, L2 y L3 que no están predefinidos en la herramienta.

Para interrelacionar los casos de uso, se crea un identificador único que describa esta conexión. Para los casos de uso L1, se crea un identificador único con dos letras en mayúsculas (ejemplo: AA); para los casos de uso L2, se agrega al identificador del caso de uso L1 con el que se relaciona, y se agrega un guión medio seguido de tres letras en mayúscula relacionados con el caso de uso L2 (ejemplo AA-BBB); y para los casos de uso L3, se agrega la información del identificador L2 con el que se relaciona, seguido de un guión medio y dos dígitos, que generalmente empiezan desde 01 (ejemplo: AA-BBB-01).

### Definición de casos de uso L1

Para el acceso a la red LAN en la Universidad de Cuenca, se definen dos casos de uso L1 que no están predefinidos en la herramienta MaGMa, relacionados con el acceso y conexión de nuevos usuarios hacia los puntos de red universitarios así como las redes WiFi disponibles dentro de los campuses, y con el acceso físico a las instalaciones críticas como centros de datos y oficinas. Los casos de uso L1 son Acceso a la red LAN (AL). Consiste en cualquier acceso o permiso que pueda afectar la vulnerabilidad de la red LAN en la Universidad de Cuenca.

**Daño a Infraestructura Fïsica (DI).** Se define como cualquier daño de infraestructura que pueda comprometer el acceso a los servicios universitarios y sus telecomunicaciones.

En la figura 3 se observa el ingreso de estos casos de uso en la herramienta, así como la asignación de los identificadores únicos para cada caso de uso.

| Visión Estratégica | |
|---|---|
| ID Caso Uso L1 | Caso de Uso |
| AL | Acceso Red LAN |
| DI | Daño a Infraestructura Física |

**Figura 3.** Definición de casos de uso L1.

**Definición de casos de uso L2**

Los casos de uso L2 son amenazas particulares que están contenidas y relacionadas dentro de un caso de uso L1 específico. Por ese motivo, se definen amenazas específicas tales como el ingreso de intrusos a las instalaciones o a la red, causas de fuerza mayor e indisponibilidades.

Los casos de uso L2 son los siguientes:

Causas de fuerza mayor (DI-CFM). Daños a la infraestructura causados por terremotos, huracanes, actos terroristas, etc. los cuales son de caracter fortuito y cuya causa está fuera del alcance de la organización

Ingreso de personal no autorizado (DI-PNA). Se refiere al ingreso a personal no autorizado a las instalaciones físicas de centros de datos en la Universidad de Cuenca.

- Daños por corte de energía (DI-CDE). Daños causados por cortes de energía, como pérdida de información sensible no respaldada, así como también daños a equipos y servidores por falta de refrigeración Intrusos en la red LAN (AL-INT). Intrusos en la red LAN, con permisos no autorizados o privilegios especiales, quienes pueden inflingir daños a la universidad como robo o pérdida de datos, filtración de información confidencial, entre otros.
- Indisponibilidad de la red LAN (AL-IND). Indisponibilidad de la red LAN por parte del proveedor, o por cortes internos en enlaces de fibra óptica, los cuales imposibilitan la comunicación entre dependencias e impiden la comunicación entre dependencias y el acceso a los servicios universitarios.

En la figura 4 se expone el ingreso de estos casos de uso descritos a la herramienta MaGMa.

| Nombre de Caso de Uso L1 | ID Caso Uso L1 | ID Caso Uso L2 | Nombre Caso Uso |
|---|---|---|---|
| Daño a Infraestructura Física | DI | DI-CFM | Causas de fuerza mayor |
| Daño a Infraestructura Física | DI | DI-PNA | Ingreso de personal no autorizado |
| Daño a Infraestructura Física | DI | DI-CDE | Daños por corte de energía |
| Acceso Red LAN | AL | AL-INT | Intrusos en la red LAN |
| Acceso Red LAN | AL | AL-IND | Indisponibilidad de la red LAN |

**Figura 4.** Definición y descripción de casos de uso L2 relacionados con los casos de uso L1.

**Definición de casos de uso L3**

Estos casos de uso definen las acciones a nivel operacional establecidas para hacer frente a las amenazas expuestas en los otros casos de uso. Se define a mayor detalle los casos de uso L2, en forma de los mecanismos de detección y operación que la universidad usa actualmente.

Aquí, el equipo SOC ingresa los valores de las métricas de efectividad, implementación y cobertura, a partir de los cuales se calculan las métricas de peso y potencial para todos los casos de uso. Los casos de uso L3 definen así el rendimiento de las tecnologías y herramientas que están actualmente funcionando en la universidad. Los casos de uso L3 ingresados en la herramienta MaGMa son los siguientes:

- Respaldo de información (DI-CFM-01). Respaldo de información por diferentes medios: redundancia en discos, redundancia geográfica de centros de datos, respaldos magnéticos y respaldo en nube.
- Control de acceso de personal (DI-PNA-01). Control de acceso de personal con tarjetas RFID, acompañado del correspondiente sistema de seguimiento de logs de entrada y salida a las instalaciones.

- Mantenimientos preventivos en Data Center (DI-CDE-01). Mantenimientos preventivos para sistemas de respaldo de energía (UPS), y sistemas de aire acondicionado en centros de datos.
- Implementación y gestión de una herramienta de Network Access Control NAC (AL-INT-01). mplementar herramientas de control de acceso a la red, tales como asignación de VLANs, permisos limitados basados en rol, y monitoreo de tráfico con mayor alcance.
- Monitoreo activo de los logs del Firewall Perimetral (AL-INT-02). Monitoreo y análisis de la información generada por los logs del firewall perimetral, en busca de comportamientos sospechosos, búsqueda de responsables en caso de incidentes, anticipación o predicción de ataques riesgosos.
- Implementación de un SIEM. En la figura 5 se muestra el ingreso de los casos de uso L3 a la herramienta MaGMa

| ID Regla | Nombre Técnico de Caso de Uso |
|---|---|
| DI-CFM-01 | Respaldo de información |
| DI-PNA-01 | Control de acceso de personal |
| DI-CDE-01 | Mantenimientos preventivos en Data Center |
| AL-INT-01 | Implementación y gestión de un NAC (Network Access Control) |
| AL-INT-02 | Monitoreo activo de los logs del Firewall Perimetral |

**Figura 5.** Definición y descripción de casos de uso L3 relacionados con los casos de uso L1 y L2.

**Ingreso de estimación de valores de métricas para los casos de uso L3**

El equipo SOC ingresa los valores de las métricas de efectividad, implementación y cobertura de los casos de uso L3 con respecto al estado actual de la tecnología con la que cuenta la universidad. La herramienta toma estos valores de porcentaje y calcula las métricas de peso y potencial que tienen los

mecanismos de detección descritos en los casos de uso L3. La figura 6 muestra las entradas de porcentajes a cada una de las métricas y se observa asimismo el resultado de las métricas de peso y potencial para cada caso de uso L3.

| ID Regla | Efectividad % | Implementación % | Cobertura % | Peso (eff*impl*cvrge) | Potencial (eff-weight) |
|---|---|---|---|---|---|
| DI-CFM-01 | 50% | 75% | 50% | 19% | 31% |
| DI-PNA-01 | 95% | 100% | 100% | 95% | 0% |
| DI-CDE-01 | 80% | 100% | 75% | 60% | 20% |
| AL-INT-01 | 90% | 10% | 33% | 3% | 87% |
| AL-INT-02 | 70% | 20% | 10% | 1% | 69% |

**Figura 6.** Efectividad, implementación y cobertura de los casos de uso L3, así como peso y potencial resultantes de cada uno de ellos.

El respaldo de información (DI-CFM-01) por lo general tiene una efectividad media (50 %), puesto que la pérdida de información no suele ser total en la mayoría de los casos, y cubre un hecho que no sucede con frecuencia. Si hablamos de la implementación, en el caso de la Universidad es del 75 %, puesto que hay respaldos con redundancia geográfica, con cintas magnéticas y dentro de los equipos de almacenamiento (RAID), pero no se cuenta con respaldos en la nube. La cobertura es del 50% puesto que no se respalda la totalidad de la información que se genera día a día, sino que sólo se respalda la información sensible y crítica para el funcionamiento normal de las operaciones de la Universidad.

Con respecto al control de acceso de personal (DI-PNA-01) su efectividad es muy alta puesto que además de los guardias de seguridad, se cuenta con un sistema de acceso mediante tecnologías RFID, con las cuales se asegura que sólo personal autorizado ingresa a los centros de datos y sitios donde

está la infraestructura de telecomunicaciones, por ello se le dá un porcentaje del 95 %. La implementación y cobertura son del 100% puesto que este sistema está en todos los sitios críticos y se controla el acceso a cualquier persona que quiera a ingresar a los lugares mencionados.

Los mantenimientos preventivos en los centros de datos (DI-CDE-01) se llevan una efectividad del 80%, puesto que si bien los mantenimientos frecuentes y continuos ayudan a que la mayor parte del tiempo el equipamiento funcione de manera correcta, no se puede evitar que fallen por algún caso fortuito. La implementación es total (100 %) puesto que se hacen mantenimientos todos los años, como parte de una política universitaria, aunque la cobertura es del 75% ya que la mayoría de los equipos reciben mantenimiento.

El uso de una herramienta de NAC (AL-INT-01) no está implementada en la Universidad, aunque se hace en algunos casos a través de la asignación de vlans según el rol, por eso se le asigna un 10 %, y cubre solo a ciertos empleados (cobertura de 33 %). Su efectividad es muy alta para reforzar la seguridad de en las redes y la información de la Universidad.

El monitoreo activo de los logs del Firewall Perimetral (AL-INT-02) se lo realiza cuando existen problemas en la comunicación o el acceso a los servicios universitarios, por ello su implementación se estima en un 20% y su cobertura en 10 %, aunque se sabe que su efectividad es alta (70 %) porque se pueden prevenir muchos ataques haciendo un monitoreo y análisis activo de los logs del firewall, pero el área de la seguridad es muy cambiante y pueden existir ataques a pesar de ello.

De entre todas los casos de uso L3, se puede ver que el potencial es muy alto para los casos de uso (AL-INT-01) y (AL-INT-02), es decir que la inversión en la implementación de un sistema de NAC y de monitoreo activo de los logs de firewall es necesaria para reforzar el acceso a la red LAN en la Universidad de Cuenca.

La figura 7 presenta las métricas resultantes de los casos de uso L2.

| ID Caso Uso L2 | Casos de Uso L3 relacionados | Efectividad Promedio | Implementación Promedio | Cobertura Promedio | Peso Promedio | Potencial Promedio |
|---|---|---|---|---|---|---|
| DI-CFM | 1 | 50% | 75% | 50% | 19% | 31% |
| DI-PNA | 1 | 95% | 100% | 100% | 95% | 0% |
| DI-CDE | 1 | 80% | 100% | 75% | 60% | 20% |
| AL-INT | 2 | 80% | 15% | 22% | 2% | 78% |
| AL-IND | 0 | 0% | 0% | 0% | 0% | 0% |

**Figura 7.** Métricas resultantes para los casos de uso L2.

Por su parte, la figura 8, detalla las métricas resultantes para los casos de uso L1.

| Caso de Uso | Efectividad | Implementación | Cobertura | Peso | Potencial |
|---|---|---|---|---|---|
| **Acceso Red LAN** | 40% | 8% | 11% | 1% | 39% |
| **Daño a Infraestructura Física** | 75% | 92% | 75% | 58% | 17% |

**Figura 8.** Métricas resultantes para los casos de uso L1.

La figura 9, detalla la efectividad, implementación y cobertura para los casos de uso L1, la figura 10 muestra su peso y potencial.

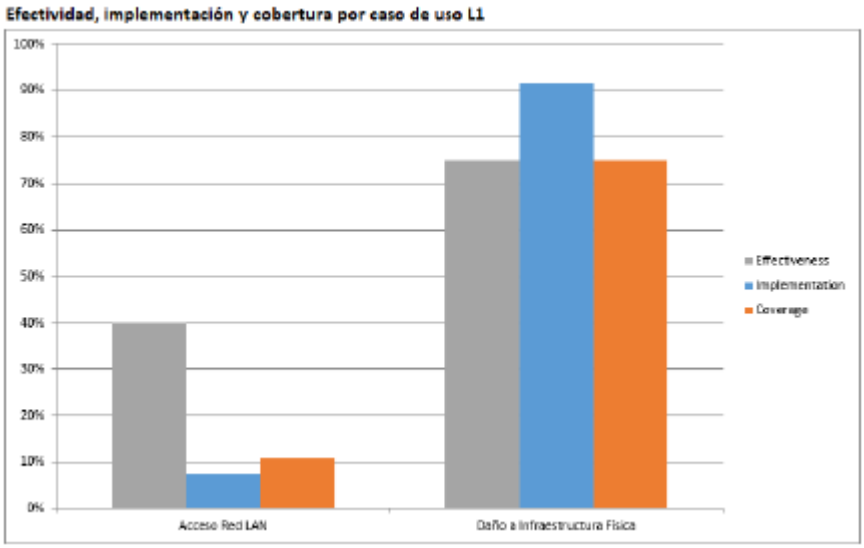


**Figura 9.** Efectividad, implementación y cobertura resultante para los casos de uso L1.

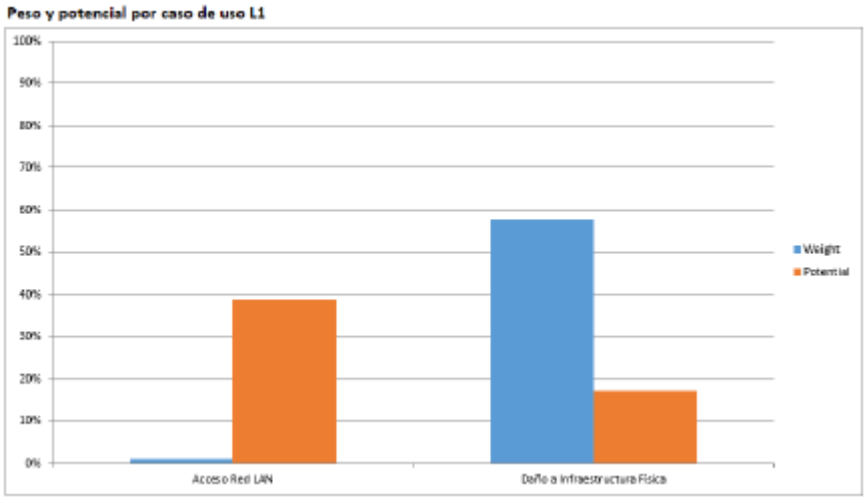


**Figura 10.** Pesos y potencial resultante para los casos de uso L1.

El la figura 11 se puede observar la cantidad de casos de uso de L2 y L3 para cada caso de uso L1.

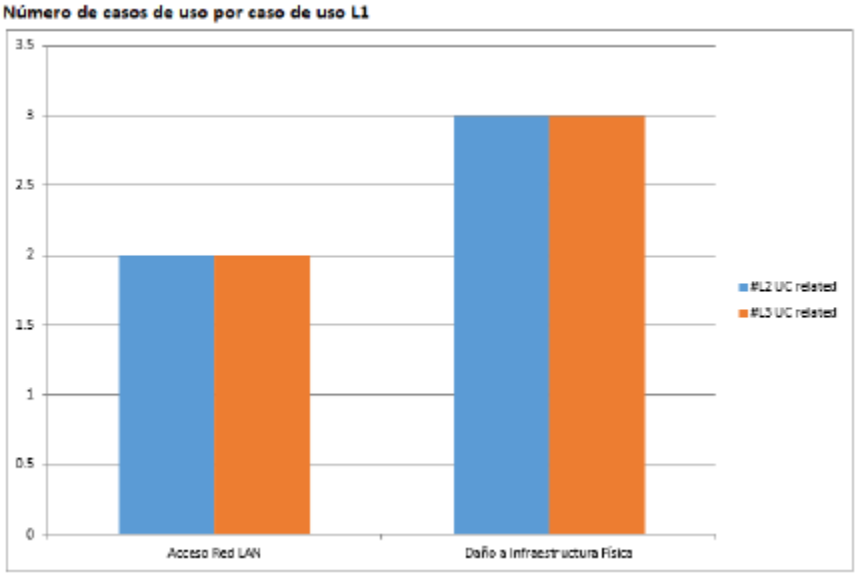


**Figura 11.** Cantidad de casos de uso L2 y L3 para cada caso de uso L1.

Además, la figura 12, presenta el rendimiento global en uso de herramientas y políticas de acceso a la red LAN de la Universidad de Cuenca.

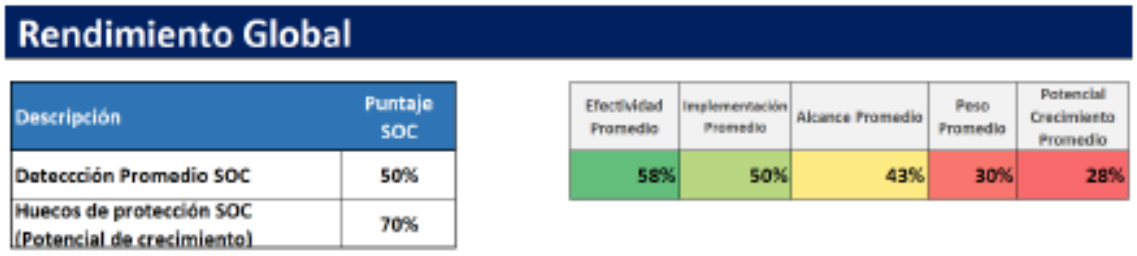


**Figura 12.** Rendimiento global.

**Establecimiento de política para acceso a red LAN**

Como propuesta se define una política de acceso a la red LAN que permita resguardar la información que trafica y se genera día a día por sus usuarios internos (funcionarios, docentes, estudiantes) y por sus usuarios externos (proveedores, contratistas, socios estratégicos, instituciones de regulación del Estado). La misma se define en base al estudio realizado en el presente documento, aplicando la herramienta MaGMa, y a los conceptos definidos por la norma ISO/IEC 27001:2013 ((ISO/IEC,

2013)). La norma ISO/IEC 27001 define que las políticas de seguridad deben estar basados en las necesidades de la organización, como consecuencia de un análisis de los objetivos de la misma, con el fin de respaldar su consecución. Dentro de los principios claves de la norma se cuentan la confidencialidad, la integridad y la disponibilidad. En cuanto a la confidencialidad, la política de seguridad debe garantizar que la información se mantiene en entornos que preservan la privacidad de los usuarios contra intrusos que puedan generar consecuencias negativas. Es así que la Universidad se plantea como objetivo el monitoreo constante y el análisis de los registros en busca de comportamientos sospechosos que puedan generar incidentes que dañen a la universidad como entidad, y a sus usuarios internos y externos. Definición de la política de acceso a la red LAN La Universidad de Cuenca cuenta con un documento de políticas generales de seguridad de la información, la cual al momento de la elaboración del presente estudio se encuentra en fase de elaboración. Éste se comprende en un documento extenso donde se menciona mucha información particular relacionada a la Universidad, como son los antecedentes, el contexto organizacional, los cuales están fuera del alcance del presente estudio. En el mencionado documento, se describe políticas para la gestión de activos de la información, para licenciamiento de software, para continuidad de los servicios informáticos, y también políticas del control de acceso. Dentro de este apartado, y luego de los resultados obtenidos, se añaden los siguientes puntos a la política:

- Los usuarios de la Universidad de Cuenca deberán acceder únicamente a los sistemas de información para los cuales han sido formalmente admitidos.
- Se prohíbe intentos de acceso ilegítimos.
- La Universidad de Cuenca se reserva el derecho del registro de información por tiempo limitado, con la finalidad de realizar auditoria en caso de incidentes, entre los que se cuentan:
    - Dirección IP desde donde se conecta.
    - Última fecha de inicio de sesión.
    - Acciones que correspondan al: ingreso, actualización o eliminación de datos.
    - A toda persona a la que se haya entregado un identificador de usuario, es responsable de la actividad asociada al mismo en los sistemas de información, dispositivos, aplicativos y otros a los que tenga acceso de acuerdo a su perfil de usuario.

Así, el estudio y cuantificación de los mecanismos y procedimientos del equipo de seguridad de la información en la Universidad de Cuenca, con la herramienta MaGMa, nos da como resultado nuevas perspectivas para aplicar a las políticas universitarias.

## Conclusiones

Este artículo planteó como objetivo principal el estudio para la definición de una política de seguridad para el acceso a la red LAN en la Universidad de Cuenca. Para lo cual se hizo uso de la herramienta y el marco de referencia MaGMa para cuantificar la efectividad, implementación y alcance que una organización posee en temas de seguridad de la información, mediante la aplicación de casos de uso. La herramienta de gestión MaGMa permite ver en sus resultados, el valor del potencial que tiene una organización para un determinado caso de uso, entendiéndose como potencial el crecimiento que la misma obtiene realizando inversiones en el área del caso de uso.

En el escenario de la Universidad de Cuenca, el valor resultante de potencial fue alto para los casos de uso relacionados con el acceso a la red LAN. Esto sugiere que la Universidad gestionará de mejor manera la seguridad de la información, asignando valores a dicha área, evitando así potenciales daños provocados por ataques maliciosos de intrusos en la red.

La Universidad de Cuenca necesita destinar recursos para que el equipo encargado de la seguridad de la información pueda monitorear activamente los logs de tráfico generados por sus herramientas de firewall, así como también debe implementar un sistema de control de acceso a la red (NAC por sus siglas en inglés), los cuales le permitan monitorear, analizar y auditar comportamientos sospechosos en la red y/o las causas de un incidente relacionado con ataques y vulneraciones a la información de los usuarios de la red universitaria.

A partir de definir las necesidades de la Universidad de Cuenca frente al control del acceso a la red LAN, se establece una política de seguridad basada en la normativa ISO/IEC 27001, que garantiza que el tráfico generado por los usuarios y su información estén dentro de un entorno privado y protegido.

## Referencias

1. Doig Díaz, D. F.; Mendoza Blanco, J. C.; Mendoza Pasco, J. L.; Yañez Herrera, D. A. Escenarios de aprendizaje competitivo a través de uso de elementos lúdicos para estrenamiento en ciberseguridad. 2019.
2. Alonso Ricardo, C. A.; Gutiérrez Beltrán, D. P., et al. Elaboración de un instrumento basado en la unificación de los estándares PCI DSS 3.2, framework de ciberseguridad versión 1.1 y NTC-ISO-IEC 27001: 2013 estableciendo el estado actual y proponiendo medidas para el fortalecimiento de la seguridad de la información en una empresa de gas natural. Ph.D. thesis, 2019.
3. Estupiñan, A. d. C. A.; Pulido, J. A.; Jaime, J. A. B. Análisis de Riesgos en Seguridad de la Información. Ciencia, innovación y tecnología 2013, 1, 40–53.
4. Hutchins, E. M., Cloppert, M. J., Amin, R. M. y col. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Leading Issues in Information Warfare & Security Research, 1 (1), 80.
5. ISO/IEC. (2013). Information technology — Security techniques — Information security management systems — Requirements (ISO/IEC 27001:2013). International Organization for Standardization. https://www.iso.org/standard/54534.html
6. Kokulu, F. B., Soneji, A., Bao, T., Shoshitaishvili, Y., Zhao, Z., Doupé, A. & Ahn, G.-J. (2019). Matched and mismatched socs: A qualitative study on security operations center issues. Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, 1955-1970.
7. Maroto, J. P. (2009). El ciberespionaje y la ciberseguridad. La violencia del siglo XXI. Nuevas dimensiones de la guerra, 45-76.
8. Muñoz, J. & Ponce, D. (2017). Metodologıa para seleccionar polıticas de seguridad informática en un establecimiento de educación superior. Maskana, 8, 1-8.
9. Sánchez-Torres, B., Rodrıguez-Rodrıguez, J. A., Rico-Bautista, D. W. & Guerrero, C. D. (2018). Campus inteligente: Tendencias en ciberseguridad y desarrollo futuro. Revista Facultad de Ingenieria, 27 (47), 91-100.
10. Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G. & Thomas, C. B. (2018). Mitre att&ck: Design and philosophy. Technical report.

11. van Os, R. (2020 [Online]). MaGMa. https://www.betaalvereniging.nl/veiligheid/publiek-private-samenwerking/magma/
12. Yupanqui, J. R. A. & Oré, S. B. (2017). Polıticas de Seguridad de la Información: Revisión sistemática de las teorıas que explican su cumplimiento. Revista Ibérica de Sistemas e Tecnologias de Informação, (25), 112-134.