UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

POSGRADOS

MAESTRÍA EN
SEGURIDAD DE LA INFORMACIÓN

RPC-SO-28-NO.669-2021

OPCIÓN DE TITULACIÓN:
ARTÍCULOS PROFESIONALES DE ALTO NIVEL

TEMA:
PROPUESTA DE UNA POLÍTICA DE SEGURIDAD PARA EL DISEÑO DE UNA RED DE CAMPUS EMPRESARIAL CONSIDERANDO LA FUNCIONALIDAD Y LA CIBERSEGURIDAD ANTE INCIDENTES CONTRA LA CONFIDENCIALIDAD Y DISPONIBILIDAD.

AUTORES:
RICARDO FERNANDO VIÑANZACA TOLEDO
PAÚL ENRIQUE VILLAGÓMEZ BERMEO

DIRECTOR:
JOSÉ LUIS AGUAYO MORALES

CUENCA – ECUADOR
2023

Autores:

Ricardo Fernando Viñanzaca Toledo
Ingeniero de Sistemas.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
rvinanzaca@est.ups.edu.ec

Paúl Enrique Villagómez Bermeo
Ingeniero de Sistemas.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
pvillagomezb@est.ups.edu.ec

Dirigido por:

José Luis Aguayo Morales
Ingeniero en Electrónica y Telecomunicaciones.
Magister en Ciberseguridad.
Magister en Sistemas Informáticos educativos.
Magister en Redes de Comunicaciones.
jaguayo@ups.edu.ec

Propuesta de una política de seguridad para el diseño de una red de campus empresarial considerando la funcionalidad y la ciberseguridad ante incidentes contra la confidencialidad y disponibilidad.

DEDICATORIAS

A Dios y a la Virgen, por las innumerables bendiciones y oportunidades que han iluminado mi vida.

A mis queridos padres, Milton y Lety, les agradezco de todo corazón por seguir creyendo en mí, incluso a pesar de la distancia. Su cariño y apoyo incondicional son mi mayor fortaleza, siempre presentes en mis pensamientos y en lo más profundo de mi corazón.

A mi amada esposa Angie, gracias por acompañarme en la búsqueda de mis sueños, tú presencia, amor, confianza y paciencia es invaluable. Eres mi pilar fundamental para lograr cualquier objetivo en la vida.

A mis maravillosos Hijos Zuri y Marti, ustedes son mi inspiración y motivación en cada paso de este desafiante camino.

A mis queridos abuelitos, les agradezco por haber influido siempre en mi madurez y, sobre todo, por enseñarme a enfrentar y superar cualquier desafío en la vida.

A mi tía y primos, gracias por apoyarme siempre y por ser un soporte constante en mi anhelo de superación personal.

Ricardo Viñanzaca T.

Al Creador de todas las cosas, agradezco profundamente por darme la fortaleza para seguir cuando he estado al borde del abatimiento. Por los triunfos y las adversidades que me han ayudado a valorarlo cada día más. A mis padres, que me han proporcionado todo su amor incondicional, les expreso mi profunda gratitud por darme la vida y apoyarme siempre. Por haber creído en mí y regalarme una carrera para mi futuro, reconozco su inmensa generosidad. Todo esto lo hago con mucho cariño desde el fondo de mi corazón.

Hoy, en este día especial, quiero dedicar este proyecto a mi hijo, la persona más importante de mi vida. Desde el día en que naciste, has sido una constante fuente de inspiración para mí. Has crecido convirtiéndote en una persona amable, cariñosa y responsable. No hay palabras que puedan describir el profundo amor y orgullo que siento por ti. Estoy eternamente agradecido por tu amor, tu apoyo y por ser mi mejor amigo. Este proyecto es una muestra de mi amor hacia ti. Me siento honrado de ser tu padre y quiero que sepas que siempre estaré a tu lado para apoyarte y animarte.

¡A mi pareja, de verdad no hay palabras para expresar mi gratitud! Estos momentos juntos han resultado en la construcción de un gran vínculo entre nosotros. Hemos compartido risas, lágrimas y recuerdos inolvidables que me llenan el corazón de alegría. Estás conmigo en este día tan significativo, y por eso te agradezco de todo corazón

A mi compañero de tesis, quien me alentaba a seguir adelante cuando me sentía abrumado y pensaba que no podía continuar. Y, finalmente, a quienes no creyeron en mí, gracias a su actitud me motivaron a seguir adelante con más fuerza.

Paúl Villagómez B.

AGRADECIMIENTOS

- A Dios y la Virgen, eternamente agradecido por otorgarme salud y vida para alcanzar mis sueños.

  A mis padres, les agradezco por su amor, generosidad y confianza; representan mi mayor ejemplo de superación y valentía.

  A mi amada Angie, Gracias por ser mi compañera en este reto, por creer siempre en mí, incluso cuando yo mismo dudaba. Tú amor y apoyo incondicional han sido el motor que me ha impulsado a alcanzar esta meta.

  A mis pequeños ZUMA, ustedes son la razón de mi perseverancia, su amor y alegría es lo que me impulsa a seguir adelante.

  A mis abuelitos, tía y primos, les expreso mi sincera gratitud por su respaldo en los desafíos que me he planteado.

  A mi director de proyecto, Ing. José Luis, gracias por su guía y soporte a lo largo de este proceso.

  A mi compañero de proyecto Paúl, gracias por unirte a este desafío; ¡juntos lo logramos!

  Ricardo Viñanzaca T.

- A Dios, le agradezco infinitamente por acompañarme todos los días, y por el incondicional apoyo brindado por mi familia. Ellos han sido una fuerza vital para mi trayectoria, corrigiendo mis errores y celebrando mis logros.

  A mis amigos, estoy muy agradecido por su compañía, apoyo y motivación incondicional. Sus palabras y acciones han sido una inspiración para mí. A mis compañeros de estudio, les doy las gracias por su cooperación, amistad y generosidad. Sus contribuciones han sido de gran ayuda para que mi proyecto llegue a buen puerto. Estoy profundamente agradecido por todo el apoyo que me han brindado.

  Paúl Villagómez B.

Tabla de Contenido

Propuesta de una Política de Seguridad para el Diseño de una Red de Campus Empresarial Considerando la Funcionalidad y la Ciberseguridad ante Incidentes Contra la Confidencialidad y Disponibilidad.

Autores:

RICARDO FERNANDO VIÑANZACA TOLEDO.
PAUL ENRIQUE VILLAGÓMEZ BERMEO.

Resumen

En el diseño de una red, es indispensable identificar riesgos y amenazas que puedan impactar la confidencialidad y disponibilidad. Es importante prevenir y mitigar incidentes que afecten a las organizaciones e infraestructura, controlar el acceso, monitorear, detectar incidentes, respaldar y recuperar datos, actualizar y mantener sistemas, cumplir con leyes y regulaciones, implementar planes de respuesta a incidentes y revisarlos para lograr una mejora continua.

Siguiendo una metodología basada en la ISO/IEC 27000 y el modelo de diseño top down se adopta un enfoque claro sobre las normas que se deben cumplir, el rol que debe desempeñar y la definición de la seguridad de la organización, facilitando la implementación de medidas que ayudarán a proteger la infraestructura de red y la información empresarial, minimizando el riesgo de incidentes de ciberseguridad y garantizando la continuidad efectiva de las organizaciones.

El resultado es un modelo de política de seguridad que mitiga los riesgos desde el diseño, detallando sus partes constitutivas, cumpliendo el marco legal ecuatoriano vigente y tiene factibilidad financiera según el cálculo de retorno de inversión en seguridad de la información.

Palabras clave:

Red de Campus, Red Segura, Política de seguridad, Confidencialidad, Disponibilidad.

ABSTRACT

When designing a network, it is essential to identify risks and threats that may impact confidentiality and availability. It is important to prevent and mitigate incidents that affect organizations and infrastructure, control access, monitor, detect incidents, back up and recover data, update and maintain systems, comply with laws and regulations, implement incident response plans and review them for continuous improvement.

Following a methodology based on ISO/IEC 27000 and the top-down design model takes a clear approach to the standards to be met, the role to be played and the definition of the organization's security, facilitating the implementation of measures that will help protect the network infrastructure and business information, minimizing the risk of cybersecurity incidents and ensuring effective business continuity.

The result is a security policy that mitigates risks from the design, detailing its constituent parts, complying with the current Ecuadorian legal framework and has financial feasibility according to the calculation of return on investment in information security.

Keywords:
Campus Network, Secure Network, Security policy, Confidentiality, Availability

1. Introducción

El amplio desarrollo de las tecnologías informáticas, así como su utilidad dentro de las organizaciones y sociedad en general aumenta la demanda de elaborar planes efectivos, políticas sólidas y buenas prácticas en torno a la seguridad digital. Este aspecto es un pilar crucial en el diseño y operación de una red segura. La ausencia de un modelo de seguridad integral puede representar un alto riesgo, el cual debe ser analizado y mitigado. Este enfoque asegurará que tanto los usuarios como los servicios empresariales estén protegidos y no se encuentren vulnerables a posibles ataques cibernéticos [1].

Además, es esencial adoptar una tendencia que fomente una cultura de seguridad informática duradera, que no se limite a un único objetivo concreto, sino que actúe como un medio para alcanzar y preservar múltiples metas. Entre ellas se incluye el uso responsable de la información [2]. Esto basado en la implementación de modelos de seguridad robustos que utilicen las mejores prácticas en términos de arquitectura y configuración. Debe considerar que la información es un bien valioso, un componente esencial de nuestra identidad digital que debe ser celosamente protegido para prevenir su pérdida, alteración o acceso indebido. Por tanto, es indispensable tener en cuenta los principios de disponibilidad, integridad y confidencialidad. Sin embargo, este trabajo se centrará exclusivamente en la confidencialidad y disponibilidad como factores predominantes.

El establecimiento de normas de seguridad informática, tanto en la fase de diseño como en la implementación de la red de campus, es de suma importancia. Esta estrategia proporcionará las directrices necesarias para mitigar las vulnerabilidades y amenazas de seguridad. No obstante, estas normas deben estar firmemente establecidas en una política precisa y comprensible que defina los procedimientos y medidas necesarias para minimizar los riesgos dentro de la red de campus. Debido a que esta red no solo sirve como un canal crítico de comunicación, sino que también se entrelaza con varias facetas de la organización. Por lo tanto, su protección no es simplemente una cuestión de asegurar los datos, sino de preservar la integridad y la funcionalidad de la entidad en su totalidad.

El imperativo de proporcionar redes seguras pone de manifiesto la necesidad de emplear tecnología de vanguardia para la protección y el correcto funcionamiento de las redes. Este principio, junto con el desarrollo de planes y políticas de seguridad robustas para la red de campus, consolida una orientación unificada de protección. Esta visión debe sustentarse en varios pilares, incluyendo la detección y alerta temprana, una defensa activa y eficaz, así como medidas de prevención proactivas. Pero, por encima de todo, se requiere fortalecer la gestión de la información de la red y las medidas preventivas durante la transmisión, procesamiento y almacenamiento de datos [3].

La gestión eficaz de la red de campus, junto con las estrategias y las políticas de seguridad, deben operar en un estado de alerta y adaptabilidad continuas. En este entorno volátil y en constante cambio, nuevas tecnologías informáticas emergen y se integran en la sociedad a un ritmo vertiginoso. Esta realidad plantea la necesidad de estar siempre listos para enfrentar los desafíos y amenazas que emergen en esta confluencia de innovación. Esta preparación constante es fundamental para garantizar un funcionamiento controlado y una protección sólida de nuestras organizaciones. En el siempre fluctuante panorama de la ciberseguridad, nuestra obligación indiscutible es mantenernos siempre un paso por delante de las amenazas potenciales, asegurando la continuidad operativa y la seguridad de los activos de información. Nuestra responsabilidad no es solo reaccionar, sino también anticipar, prevenir y proteger, en un compromiso ininterrumpido con la vanguardia tecnológica.

2. Determinación del Problema

La tecnología ha generado una transformación significativa en nuestra sociedad, convirtiéndose en un aspecto de vital importancia. Su influencia es tan relevante que muchas personas y organizaciones dependen en gran medida de ella, debido al valor agregado que brinda, especialmente a las empresas. Por tanto, es indispensable contar con un diseño y gestión de redes robusto que se adapte a cualquier tipo de organización, garantizando la excelencia de los servicios prestados. Esta premisa se refleja en la disponibilidad, funcionalidad y confidencialidad de la información manejada. Teniendo como objetivo el proporcionar un servicio de alta calidad, acorde a las exigencias actuales de las organizaciones y usuarios. Sin embargo, para hacerlo de manera eficaz, es fundamental que este servicio esté asentado sobre una infraestructura que integre las tecnologías emergentes y, al mismo tiempo, ofrezca soluciones de seguridad garantizadas. Solo así podremos garantizar la integridad, confidencialidad y disponibilidad de la información, pilares fundamentales en la seguridad de la información

Las organizaciones deben enfocar sus esfuerzos no solo en diseñar una red funcional, sino también en desarrollar políticas robustas que aseguren la protección de su información. A menudo, estos puntos se pasan por alto, generalmente debido a una falta de conocimiento sobre los riesgos que un incidente de seguridad puede ocasionar. Es fundamental entender que prevenir una brecha de seguridad es mucho más eficiente y menos costoso que tener que corregir sus consecuencias.

Es importante tener en cuenta que un ataque informático exitoso a una entidad puede resultar en pérdidas económicas significativas. Más aún, puede causar una pérdida de credibilidad en la empresa, lo cual puede tener un impacto duradero y perjudicial para su reputación. Por tanto, la seguridad de la información no es un lujo, sino una necesidad crítica para cualquier organización.

Ante estos aspectos es prioritario definir los siguientes objetivos:

- **Objetivo Principal.**
    - Proponer una política de seguridad para el diseño de una red de campus empresarial considerando la funcionalidad y la

ciberseguridad ante incidentes contra la confidencialidad y disponibilidad (CyD).

- **Objetivos Específicos.**
    - Determinar los componentes para el diseño de una red de campus empresarial para que tenga una adecuada funcionalidad.
    - Analizar los diferentes estándares y herramientas para poder reducir las vulnerabilidades de confidencialidad y disponibilidad de la red de campus.
    - Proponer una política de seguridad para un adecuado acoplamiento de la red y sus mecanismos de protección.

El tema de investigación plantea ciertas incertidumbres entre las que se pueden mencionar:

- ¿En qué se basará la propuesta de políticas?
- ¿Cuáles son los componentes ideales para un adecuado diseño de red de campus?
- ¿Cuáles son los incidentes más comunes que afectan la confidencialidad y disponibilidad?
- ¿Cómo beneficiará a las organizaciones?

La elaboración de un conjunto de normas de seguridad informática, basadas en el análisis y diseño exhaustivo de la red, se convierte en un aspecto fundamental para cualquier organización. Esta estrategia garantizará no solo el conocimiento necesario, sino también la base sobre la cual se puede estructurar e integrar la infraestructura tecnológica. Todo con el propósito de ofrecer al usuario la mejor funcionalidad y la garantía de que su información y accesos están seguros, protegidos tanto de incidentes internos como de ataques externos.

Además, la implementación de estrategias de seguridad de la información contribuirá a mitigar riesgos y costos, con el objetivo de brindar un servicio de mayor calidad. Esto puede aumentar la productividad y proporcionar un servicio de excelencia, adaptando sus normas y regulaciones técnicas al nuevo contexto digital.

Esta investigación busca contribuir al diseño de las redes de datos con el propósito de que los servicios implementados sean ágiles y seguros favoreciendo principalmente a las organizaciones con un protocolo de diseño de seguridad establecido. La solución será económicamente factible cumpliendo con todos los atributos, requisitos técnicos y funcionales necesarios para garantizar la consecución de los objetivos y propósitos establecidos.

El estado de conocimiento en la presente investigación es muy variable, debido a esto es preciso determinar diferentes perspectivas de estudio que permitan concretar el objetivo del análisis, considerando el rápido desarrollo de la tecnología que facilita el poder abordar diversas temáticas de diseño y seguridad que puedan surgir durante el proceso de investigación.

3. Marco teórico referencial

La adopción e implementación de nuevas tecnologías ha generado un cambio significativo en nuestra sociedad y en las organizaciones, debido a su uso generalizado en todas las actividades cotidianas. Como resultado, el diseño de redes seguras y la implementación de medidas de regulación y prevención se han convertido en aspectos fundamentales. Estos cambios exigen garantizar la seguridad informática en todos los procesos tecnológicos, identificando los riesgos y estableciendo medidas preventivas básicas contra los ciberdelitos [4].

Diversos tipos de redes de información están presentes en nuestras vidas, pero establecer un diseño de red de campus es esencial para el funcionamiento seguro y eficiente de la infraestructura tecnológica en un entorno corporativo. Una red de área de campus (CAN) permite la comunicación entre los ordenadores de diferentes edificios e instalaciones en un entorno universitario, corporativo o industrial. No solo proporciona acceso a Internet y a recursos compartidos, sino también servicios de comunicación a todos los usuarios en el campus. Además, facilita la colaboración entre departamentos y equipos de la institución, permitiendo compartir información de manera eficiente [5].

La mayoría de las redes CAN están conectadas a la nube (Internet) mediante diversas formas de interconexión. Una red de campus es responsable de ofrecer servicios esenciales a los usuarios, con una estrategia centrada en el monitoreo constante de la seguridad y operación de la red [6]. Esto garantiza su funcionalidad y, además, brinda una topología modular que permite a la red evolucionar con facilidad.

Un diseño óptimo de redes de campus integra una variedad de componentes físicos (hardware) y aplicaciones (software). En la categoría de hardware encontramos routers, switches, firewalls, proxies, así como los cables y radio enlaces que los conectan. En cuanto al software, contamos con sistemas operativos de servidores, protocolos de comunicación, controladores de red, entre otros. Una integración adecuada de estos elementos permite desarrollar mecanismos de ciberseguridad que resguarden la información eficazmente, asegurando alta disponibilidad y confidencialidad para

satisfacer las necesidades de los usuarios. Sin embargo, este enfoque también implica el desafío de la configuración y administración, lo que representa una tarea crítica para el equipo de Tecnologías de la Información (TI).

Dentro del diseño de redes existen varias metodologías como la 'Metodología Top-Down Network Design'. Esta se basa en el Modelo OSI, que tiene 7 capas, cada una con un propósito y funcionalidades específicas, como se puede apreciar en la Tabla 1.

Capa	Nombre	Descripción
7	Aplicación	Se encarga de la interacción entre el software de aplicación y la red.
6	Presentación	Traduce los datos entre el formato que la red requiere y el formato que la aplicación requiere.
5	Sesión	Establece, administra y finaliza las conexiones entre las aplicaciones locales y remotas.
4	Transporte	Proporciona la transferencia de datos fiable de extremo a extremo y control de flujo.
3	Red	Maneja el enrutamiento de datos y la entrega de paquetes entre redes.
2	Enlace de Datos	Encapsula los paquetes en frames para transmitirlos a la red, también se encarga del acceso al medio y la detección de errores.
1	Física	Define las características físicas de la red, como las conexiones, los voltajes y la sincronización del reloj.

Tabla 1. Capas del modelo OSI [7].

Esta metodología de diseño empieza desde la capa 7 (aplicación) y va hacia abajo hasta llegar a la capa 1 (física), de ahí el nombre "Top-Down". Este enfoque ayuda a centrarse primero en las necesidades de los usuarios y las aplicaciones antes de considerar las tecnologías de red específicas a implementar tomando en cuenta las exigencias, restricciones y su organización lógica, factores primordiales al momento del desarrollo.

El diseño Top-Down Network Design divide el proceso de diseño de la red en varias fases. Estas fases tienen como objetivo identificar y definir las necesidades de la red desde la perspectiva de los usuarios y las aplicaciones, y luego diseñar e implementar la red para satisfacer esas necesidades. Las fases son las siguientes [8]:

1. **Identificación de las necesidades y objetivos de la red**: Esta fase implica la recopilación de información sobre la organización y los requisitos del sistema de la red. Esto puede incluir entrevistas con los usuarios finales, el análisis de las

aplicaciones actuales y futuras, y la identificación de cualquier problema con la red existente.

2. **Análisis de los requisitos de la red**: En esta fase, los diseñadores analizan los requisitos técnicos y operativos de la red. Esto puede incluir el análisis de los patrones de tráfico, los requisitos de ancho de banda, la necesidad de servicios de calidad de servicio (QoS) y los requisitos de seguridad.
3. **Diseño de la arquitectura de la red**: Esta fase implica la creación de un diseño de alto nivel de la arquitectura de la red. Esto incluye la selección de las tecnologías y dispositivos de red, el diseño de la topología de la red y la planificación de la implementación de la red.
4. **Diseño de la red detallado e implementación**: En esta fase, los diseñadores crean un diseño de red detallado, que incluye la configuración de los dispositivos de red y el diseño de la red física. Después de que el diseño está completo, la red se implementa.
5. **Pruebas y optimización**: Una vez que la red está implementada, se lleva a cabo una serie de pruebas para asegurarse de que la red está funcionando correctamente y satisfaciendo las necesidades identificadas en las primeras fases. Basándose en los resultados de estas pruebas, la red puede ser optimizada para mejorar su rendimiento y fiabilidad.
6. **Mantenimiento y actualización**: En la última fase, la red se mantiene y se actualiza según sea necesario. Esto puede incluir la resolución de problemas, la actualización de hardware y software y la monitorización continua del rendimiento de la red.

Estas fases se caracterizan por su atención a las necesidades del usuario y a las aplicaciones desde el principio, lo que ayuda a garantizar que la red final esté bien alineada con las necesidades de la organización.

Así también es necesario explorar conceptos como la convergencia, que juega un papel importante en las redes actuales. La convergencia se refiere al proceso mediante el cual diferentes tecnologías, medios y servicios se combinan en una única plataforma. Por otro lado, la hiperconvergencia es un enfoque en tecnologías de la información que combina todos los componentes de la infraestructura incluyendo almacenamiento,

procesamiento de información, red y virtualización en una única solución integrada. Esto se hace con el objetivo de garantizar que los usuarios del sistema disfruten de un funcionamiento adecuado, rendimiento optimizado y seguridad robusta.

Como resultado de esta convergencia e hiperconvergencia, las organizaciones obtienen beneficios significativos en sus entornos de trabajo, especialmente en el uso de redes. Estos beneficios incluyen una comunicación más fluida, un aumento en la competitividad, una reducción de los costos asociados al procesamiento de datos, y una mejora en los tiempos de respuesta de los usuarios [9].

Según Mohammed [10], mediante su investigación detalla que una arquitectura de red es muy importante para cualquier organización, pero siempre y cuando se establezca un nivel jerárquico y escalable. De igual manera, Shanmugam [11], determina que las redes hoy en día necesitan admitir más tráfico y que las redes de campus deben ser manejables para hacer frente a los desafíos.

En el ámbito de la ciberseguridad, las amenazas y vulnerabilidades constituyen factores críticos a tener en cuenta durante el diseño y operación de una red de campus. Las amenazas, que pueden surgir de acciones humanas, eventos naturales o incidentes tecnológicos, representan cualquier elemento o actividad que pueda poner en peligro la integridad de la información. Las vulnerabilidades, por otro lado, son debilidades intrínsecas presentes en un sistema, las cuales, si son explotadas por un ciberdelincuente, pueden poner en riesgo la seguridad de la información.

Existen distintos tipos de vulnerabilidades, que pueden encontrarse en hardware, software, redes o incluso en los propios usuarios. La falta de un control efectivo sobre estas vulnerabilidades puede provocar daños significativos en la red e información, comprometiendo la confidencialidad y disponibilidad (CYD) si no se gestionan de manera oportuna [12]. Por ello es fundamental establecer estrategias eficaces para prevenir y mitigar dichas vulnerabilidades, lo que a su vez dificulta la materialización de amenazas cibernéticas.

Las amenazas más comunes que afectan la CYD se pueden agrupar tal como se presentan en la tabla 2:

Tipo de Amenaza	Impacto en la Confidencialidad	Impacto en la Disponibilidad
Ataque de fuerza bruta	Puede comprometer la confidencialidad si logra descifrar contraseñas o claves de cifrado.	Puede provocar la indisponibilidad de servicios debido a la gran cantidad de solicitudes o intentos de acceso.
Malware	El software malicioso puede extraer información confidencial sin el consentimiento del usuario.	Algunos tipos de malware, como los ransomware, pueden bloquear el acceso a los datos o incluso a todo el sistema.
Ataque DDoS (Ataque Distribuido de Denegación de Servicio)	Generalmente no afecta directamente la confidencialidad, aunque puede ser utilizado como distracción para ataques que sí lo hagan.	Interrumpe la disponibilidad de los servicios al inundarlos con tráfico hasta que se vuelvan inaccesibles para los usuarios legítimos.
Phishing	Se utiliza para obtener información confidencial, como nombres de usuario y contraseñas, a través de tácticas de engaño.	No suele afectar la disponibilidad.
Ataque de interceptación (Man-in-the-Middle)	Un atacante puede interceptar y potencialmente modificar o robar datos confidenciales mientras se transmiten.	No suele afectar la disponibilidad a menos que el atacante decida bloquear o modificar el tráfico de manera que interrumpa el servicio.

Tabla 2. Amenazas contra la Confidencialidad e Integridad [13].

Esta tabla es una simplificación, pero la realidad puede ser mucho más compleja, con muchos tipos de amenazas y formas de ataque que pueden afectar la confidencialidad y la disponibilidad de maneras imprevistas

De igual manera se presenta en la tabla 3 algunas de las vulnerabilidades más comunes, pero se debe tener en cuenta que existen muchas otras que pueden afectar los sistemas. Es importante adoptar buenas prácticas de seguridad y realizar evaluaciones regulares para identificar y mitigar estas vulnerabilidades.

Tipo de Vulnerabilidad	Impacto en la Confidencialidad	Impacto en la Disponibilidad
Falta de autenticación	Puede permitir el acceso no autorizado a información confidencial.	Puede facilitar ataques de denegación de servicio o el uso indebido de recursos, afectando la disponibilidad.
Falta de cifrado	La información transmitida o almacenada puede ser interceptada y revelada.	No tiene un impacto directo en la disponibilidad, pero puede facilitar ataques de inyección de datos o manipulación de la integridad de los datos.
Vulnerabilidades de aplicaciones web	Pueden permitir el acceso no autorizado a datos confidenciales almacenados en aplicaciones.	Pueden ser explotadas para interrumpir o inutilizar aplicaciones, afectando la disponibilidad.
Falta de parches y actualizaciones	Permite la explotación de vulnerabilidades conocidas y puede resultar en la filtración de información confidencial.	Los sistemas no actualizados pueden ser más susceptibles a ataques que afecten la disponibilidad.
Vulnerabilidades de configuración incorrecta	Pueden exponer información confidencial o permitir accesos no autorizados.	La configuración incorrecta puede llevar a errores de configuración que afecten la disponibilidad del sistema.
Vulnerabilidades en contraseñas débiles	Las contraseñas débiles pueden ser fácilmente adivinadas o descifradas, lo que compromete la confidencialidad.	No tiene un impacto directo en la disponibilidad, pero puede facilitar el acceso no autorizado a recursos y servicios.

Tabla 3. Vulnerabilidades comunes [14].

Para prevenir incidentes de seguridad, es esencial establecer parámetros fundamentales como las políticas y procedimientos de ciberseguridad que se erigen como pilares esenciales en la construcción de un marco robusto de seguridad.

Las políticas de seguridad son un conjunto de objetivos que establecen las normas de comportamiento para usuarios, administradores y requisitos de sistemas. Su finalidad específica es garantizar la seguridad de la red, los datos y los sistemas informáticos.

Estas políticas están basadas en estándares internacionales para asegurar la uniformidad y coherencia en la operatividad de la red.

Además, se deben tener en cuenta directrices que sirven como sugerencias para definir y afinar estas políticas. Un ejemplo de esto es el 'ciberhigiene', que integra prácticas de seguridad cotidianas para ayudar a usuarios y organizaciones a mitigar incidentes de seguridad. El ciberhigiene fomenta hábitos como el uso de autenticación de dos factores, la actualización regular del software y la vigilancia constante de las actividades sospechosas. En resumen, para un enfoque efectivo de la ciberseguridad, es esencial desarrollar políticas claras, adoptar estándares uniformes y fomentar hábitos de ciberhigiene entre todos los usuarios del sistema [15].

Los estándares ISO, particularmente el conjunto de normas ISO/IEC 27000, son esenciales en el desarrollo de políticas de seguridad de la información. Estas normas estipulan requisitos para el establecimiento, implementación y mejora continua de los Sistemas de Gestión de la Seguridad de la Información (SGSI), proporcionando un marco de trabajo estandarizado.

De este conjunto, la norma ISO 27001 se destaca por su enfoque en estructurar los requisitos para la implementación de un SGSI. Esta norma es reconocida internacionalmente y su cumplimiento puede ser certificado, proporcionando una evidencia tangible de la robustez de la seguridad de la información en una organización.

Por otro lado, la norma ISO 27002 proporciona un conjunto de mejores prácticas que respaldan y asisten en la gestión de la seguridad de la información. Esta norma es ampliamente utilizada como referencia para definir controles y desarrollar directrices de políticas en las organizaciones [16].

La adopción de políticas basadas en estándares o normas reconocidas internacionalmente es un punto clave para identificar las necesidades corporativas y definir los requerimientos de las organizaciones. Al mejorar sus prácticas de seguridad de la información y ajustarse a estos estándares, las organizaciones pueden no solo incrementar la seguridad de su información, sino también optimizar sus operaciones de negocio. Todo esto se basa en parámetros esenciales como la Confidencialidad, Disponibilidad.

El despliegue de las redes CAN también presenta desafíos en la actualidad tales como [17]:

1. **Seguridad**: Aunque las redes CAN fueron diseñadas para uso en entornos cerrados, con el creciente uso de la conectividad en vehículos y sistemas industriales, las amenazas a la seguridad de las redes CAN han aumentado. Los ataques pueden variar desde escuchas no autorizadas hasta la inyección de mensajes falsos para alterar el funcionamiento de los dispositivos conectados.
2. **Interferencia y ruido**: Las redes CAN son susceptibles a la interferencia electromagnética y al ruido, que pueden causar errores de transmisión y problemas de comunicación.
3. **Rendimiento de la red**: Dado que la velocidad de transmisión en las redes CAN es relativamente baja comparada con otras tecnologías de red, puede haber retos relacionados con la latencia y la capacidad de transmisión de datos, especialmente en aplicaciones que requieren altos volúmenes de datos.
4. **Complejidad de la gestión**: Con el crecimiento y expansión de las redes CAN, la gestión y el mantenimiento de estas redes puede volverse cada vez más complejo, requiriendo más recursos y tiempo.
5. **Integración con otras tecnologías**: La integración de las redes CAN con otras tecnologías de red puede ser un desafío debido a las diferencias en los protocolos de comunicación y los estándares de transmisión.

Estos desafíos requieren atención y soluciones que sean específicas para cada aplicación de la red CAN, a fin de garantizar un funcionamiento seguro y eficiente.

En Ecuador, la implementación de un conjunto sólido de políticas de seguridad y un diseño de red de campus bien estructurado son fundamentales para cualquier tipo de negocio. Esta necesidad se ve intensificada por los actuales desafíos en ciberseguridad y seguridad informática que enfrenta el país, los cuales han dado lugar a estadísticas alarmantes. Los accesos no autorizados a sistemas informáticos se están volviendo cada vez más comunes.

Según el ECUCERT, el Centro de Respuesta a Incidentes Informáticos de Ecuador, en 2021 se identificaron 15,847 ataques, y tan solo en los primeros meses de 2022, se registraron 7,292 ataques. Un caso particularmente destacado ocurrió el 31 de mayo de

2022, cuando una institución financiera fue víctima de un ataque de Phishing que utilizó la técnica de SCAM.

Lo más preocupante es que se estima que el 80% de los delitos cibernéticos no se denuncian. Esto puede deberse a la falta de conocimiento de cómo proceder ante un incidente de este tipo, o a la falta de apoyo a nivel organizacional. Esto subraya la importancia de desarrollar una conciencia de ciberseguridad a nivel nacional, fomentar la formación en seguridad informática, y promover la denuncia y el manejo adecuado de estos incidentes [18]. Estos problemas se originan principalmente en el amplio desconocimiento de la sociedad ecuatoriana sobre seguridad informática, y en la falta de educación e inversión en esta área crítica, lo cual se refleja en el gran número de ataques no reportados.

En el ámbito corporativo, aunque las organizaciones están comenzando a invertir en protección, estrategia y respuesta a ciberseguridad, sólo el 3% de las empresas cuentan con las herramientas necesarias para proteger su información de manera efectiva. La mayoría se limita a implementar soluciones básicas como firewalls y antivirus en cada host. Esta falta de medidas de seguridad avanzadas, sumada a un interés financiero limitado en la seguridad y protección de los datos, justifica los altos porcentajes de ataques y crea una gran desventaja en la implementación de políticas o marcos de seguridad sólidos [18].

Por lo tanto, es esencial que las organizaciones adopten un enfoque proactivo en lugar de reactivo hacia la seguridad cibernética, creando políticas de prevención y control en lugar de limitarse a responder a incidentes una vez que ocurran. Es importante entender que las acciones en el mundo virtual tienen consecuencias tangibles en el mundo real. Los ciberataques y la manipulación de información en línea pueden alterar la percepción pública, perturbar la paz social, poner en riesgo la soberanía y desestabilizar las estructuras organizativas [19].

Es imperativo que las empresas presten solamente atención a los ciberataques, dado que lo que está en juego no se limita solo a la seguridad de sus datos. Ser víctima de un ataque cibernético puede llevar a una mala reputación, lo que a su vez puede resultar en la devaluación de la organización. Esto puede generar pérdida de confianza en la sociedad hacia los bienes o servicios que la empresa proporciona a sus usuarios. Por lo

tanto, invertir en medidas de seguridad sólidas y proactivas es esencial para mantener la integridad y la confianza en cualquier negocio.

4. MATERIALES Y METODOLOGÍA

El desarrollo de una política implica múltiples aspectos fundamentales, tales como la descripción de parámetros de funcionamiento y pautas generales que guíen el seguimiento y cumplimiento de estas políticas. En este estudio, la red de campus objeto de análisis debería adoptar un diseño jerárquico y modular. Este tipo de diseño ofrece flexibilidad, facilita su implementación y gestión, y considera aspectos vitales como la escalabilidad y la disponibilidad. Estos aspectos son particularmente importantes debido al crecimiento constante de las empresas y el aumento consecuente de sus requisitos de red. En este sentido, las organizaciones dependen cada vez más de su infraestructura tecnológica y de red para proporcionar sus diversos servicios de manera eficaz y eficiente [20].

El diseño jerárquico optimiza la distribución del ancho de banda, permitiendo que el tráfico de red se gestione a nivel local. Para garantizar un funcionamiento eficiente de este diseño, es esencial desarrollar al menos tres capas que estructuren la red de forma organizada y coherente [21] como se puede observar en la figura 1:

1. **Capa de Núcleo (o Backbone):** Esta es la capa de la red que proporciona conectividad rápida y fiable entre diferentes partes de la red, a menudo a través de múltiples edificios o sitios. La capa de núcleo debe ser capaz de operar con muy baja latencia y ser muy fiable, ya que maneja grandes volúmenes de tráfico de red.
2. **Capa de Distribución:** Esta capa actúa como un punto de agregación para la capa de acceso y proporciona conectividad hacia la capa de núcleo. Las funciones típicas de esta capa incluyen el enrutamiento entre subredes, la implementación de políticas de calidad de servicio (QoS), la segmentación de la red y la implementación de alta disponibilidad a través de redundancia.
3. **Capa de Acceso**: Esta es la capa que proporciona el punto de entrada a la red para los usuarios y los dispositivos finales. La capa de acceso puede incluir switches, puntos de acceso inalámbrico y otros dispositivos que proporcionan

conectividad a los dispositivos de los usuarios. Las políticas de seguridad y los controles de acceso a la red suelen implementarse en este nivel.

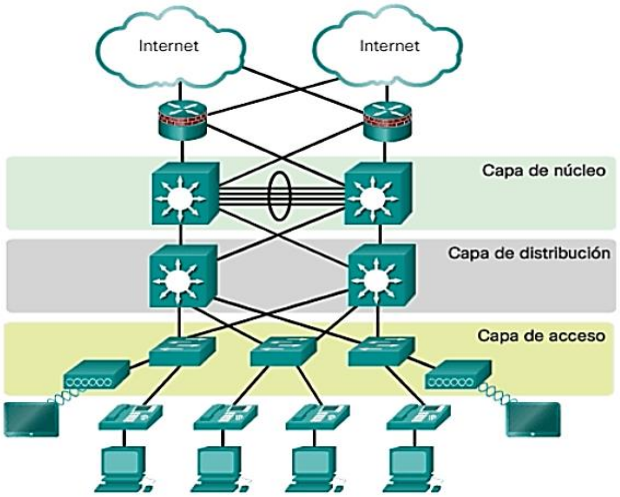

Figura 1. Modelo de Diseño Jerárquico [21].

Este diseño jerárquico ayuda a organizar y administrar una red de manera eficiente, proporcionando escalabilidad, redundancia y rendimiento.

El diseño de una red de campus se basa en el modelo jerárquico de red, y suele incluir varios módulos esenciales para ofrecer un rendimiento óptimo y una gestión eficiente. En la figura 2, se presentan algunos de los módulos básicos [20]:

- **Módulo de acceso a la red:** Este módulo se encarga de proporcionar conectividad a los dispositivos de los usuarios y a los nodos finales de la red. Normalmente incluye switches, routers y puntos de acceso inalámbrico.
- **Módulo de distribución de la red:** Este módulo se encarga de conectar los diferentes módulos de acceso entre sí y con el módulo del núcleo. Puede incluir switches y routers de capa 3 para realizar funciones de enrutamiento y filtrado.
- **Módulo de núcleo de la red (o backbone):** Este módulo proporciona una conectividad rápida y fiable entre los módulos de distribución, permitiendo la transmisión de datos a alta velocidad en toda la red del campus.

- **Módulo de servicios del campus:** Este módulo puede incluir servidores, almacenamiento y otros recursos compartidos que se utilizan en toda la red del campus.

- **Módulo de seguridad:** Este módulo es responsable de garantizar la seguridad de la red, implementando políticas de seguridad, sistemas de detección y prevención de intrusiones (IDS/IPS), firewalls y otras medidas de seguridad.

- **Módulo de gestión de la red:** Este módulo se encarga de la supervisión, la administración y la configuración de la red, lo que puede incluir software y hardware de gestión de la red.

- **Módulo de conectividad a Internet o WAN:** Este módulo proporciona la conectividad con Internet o con otras redes de área amplia (WAN), y puede incluir routers, módems y otros dispositivos de red.

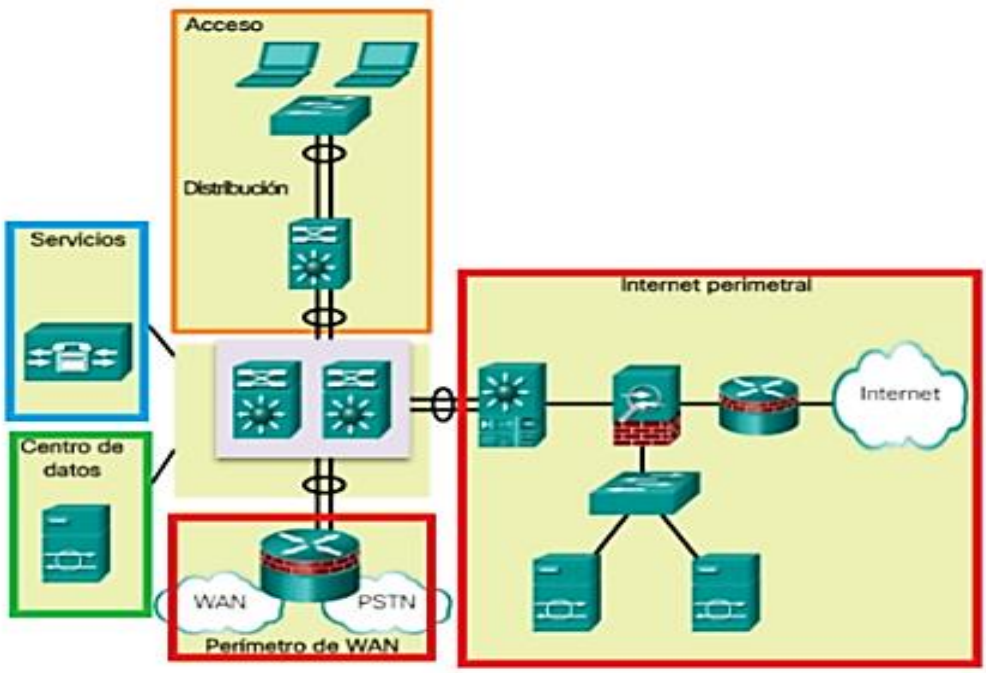

Figura 2. Módulos en la arquitectura empresarial [20].

Todos estos elementos deben fundamentarse en el desarrollo de un control de acceso efectivo a la información de las organizaciones, con el objetivo de garantizar la confidencialidad y la disponibilidad de los datos. Para construir una red de campus segura y robusta, es necesario adoptar tecnologías avanzadas como los cortafuegos

(firewalls), las Redes de Área Local Virtuales (VLANs), la tecnología de encriptación, las Redes Privadas Virtuales (VPNs), entre otros. Es importante destacar que la implementación de políticas de seguridad debe llevarse a cabo de tal manera que no afecte el rendimiento de la red ni cause interrupciones en ninguna de sus partes [22].

En este contexto, nos enfocamos en desarrollar un programa integral de seguridad para redes de campus, que se fundamenta en la implementación de controles de acceso efectivos a la información. Nuestro objetivo es garantizar la confidencialidad y disponibilidad de los datos, sin comprometer el rendimiento de la red.

4.1 Programa de seguridad.

Teniendo en cuenta que un programa de seguridad es un conjunto de políticas, procedimientos y tecnologías implementadas por una organización para proteger sus sistemas de información, redes y activos digitales contra amenazas y ataques cibernéticos. Este programa busca asegurar la confidencialidad y disponibilidad de la información, mitigando los riesgos de seguridad y garantizando el cumplimiento de las normativas y estándares de seguridad relevantes.

A continuación, se presenta breve ejemplo de un programa de seguridad de la información.

PROGRAMA DE SEGURIDAD DE LA INFORMACIÓN (PSI)

Descripción:

Comprendiendo la importancia de mantener una adecuada administración de la información, resulta esencial desarrollar un programa de seguridad de la información que genere entornos de adaptabilidad para los usuarios, cumpla con las leyes, regulaciones aplicables para alinearse con la misión y visión de la organización, independientemente de su sector o giro empresarial.

Objetivos Principales:

- Proteger la información confidencial.
- Minimizar el riesgo informático en la organización
- Cumplir con las normas y regulaciones acordes al giro del negocio
- Acatar los principios de seguridad de la información.

- Asegurar la confianza de los clientes y empleados.
- Salvaguardar la reputación y prestigio de la empresa.
- Proteger la infraestructura tecnológica.
- Optimizar el rendimiento y la eficacia
- Fomentar la cultura de seguridad.
- Establecer políticas, procedimientos o normas de seguridad

Una política siempre debe definir los siguientes factores claves en el desarrollo e implementación:

- **Identificación de los activos:** El paso inicial consiste en identificar los activos que se desean proteger, estos pueden ser datos, sistemas, redes, equipos, etc.
- **Análisis de riesgos:** Luego de identificar los activos, es necesario analizar los posibles riesgos a los que estos están expuestos. Este análisis debe incluir una evaluación de las amenazas internas y externas, así como de las vulnerabilidades existentes.
- **Definición de políticas y procedimientos:** Basados en el análisis de riesgos, se deben definir políticas y procedimientos de seguridad específicos para cada activo. Estos pueden incluir medidas de protección de datos, regulaciones de acceso a sistemas, etc.
- **Implementación de soluciones técnicas:** A continuación, se deben implementar soluciones técnicas para cumplir con las políticas y procedimientos definidos. Estas soluciones pueden incluir el uso de software de seguridad, firewalls, sistemas de autenticación, cifrado, entre otros.
- **Entrenamiento y concientización:** Es importante que todos los usuarios conozcan las políticas y normas de seguridad establecidas. Por lo tanto, es necesario realizar un entrenamiento y una campaña de concientización para asegurarse de que todos los usuarios comprendan su papel en la seguridad de los activos.
- **Monitoreo y evaluación continua:** Por último, es fundamental monitorear continuamente el programa de seguridad y evaluarlo periódicamente para asegurarse de que está cumpliendo con sus objetivos y para detectar y corregir cualquier posible brecha en la seguridad.

Hay q recordar que este es un programa modelo sencillo y su eficacia dependerá de las necesidades específicas de la organización y de su entorno operativo.

En este caso de estudio se identifica los siguientes activos como ejemplo:

1. **Información confidencial de los clientes:** Esto puede incluir nombres, direcciones, números de tarjetas de crédito y cualquier otra información personal identificable que la organización recopile.
2. **Propiedad intelectual:** Esto puede incluir patentes, marcas registradas, derechos de autor, secretos comerciales y cualquier otro tipo de conocimiento o ideas propietarias que la organización posea.
3. **Datos de los empleados:** Esto puede incluir información personal identificable, datos salariales, información sobre rendimiento laboral y otros datos relacionados con los empleados de la organización.
4. **Información financiera:** Esto puede incluir informes financieros, proyecciones, presupuestos, cuentas por cobrar y pagar y cualquier otra información relacionada con las finanzas de la organización.
5. **Información de proveedores:** Esto puede incluir datos de contacto, contratos, términos de pago y cualquier otra información relacionada con los proveedores de la organización.
6. **Sistemas de información y tecnología:** Esto puede incluir hardware, software, redes, bases de datos y otros sistemas de tecnología de la información que la organización utiliza para almacenar, procesar y transmitir su información.

La identificación de activos es un paso importante en el proceso de evaluación de riesgos, ya que te permite determinar qué activos necesitan protección y cómo podrían ser amenazados

4.2 Políticas de seguridad.

Una política de seguridad es importante pero cada organización puede requerir un enfoque diferente, dependiendo de sus necesidades específicas y de las amenazas a las que está expuesta, por lo tanto, a continuación, se desarrolla una corta propuesta de una política de seguridad, además de un conjunto de normas genéricas basadas en la ISO 27002, las mismas pueden ser usadas en cualquier giro organizacional.

Una política de seguridad basada en la norma ISO/IEC 27002:2013 debe ser exhaustiva y adaptarse a las necesidades específicas de la organización. Aquí se muestra un ejemplo simplificado de cómo podría estructurarse una política de seguridad siguiendo las directrices de la norma:

Propuesta de política de seguridad de la información [Fuente propia].

[Nombre de la Organización]

- **Introducción.**

  Propósito y alcance de la política de seguridad.

  Establecimiento de conceptos y términos fundamentales

- **Declaración de la política.**

  Declaración del respaldo de la gerencia en la protección de la información

  Objetivos de la política.

- **Organización de la seguridad de la información.**

  Estructura y responsabilidades del equipo de seguridad de la información

  Procedimientos para la autorización de acceso y la segregación de funciones

- **Gestión de riesgos de seguridad.**

  Proceso de evaluación y tratamiento de riesgos

  Metodología para identificar y evaluar riesgos

- **Seguridad interna.**

  Procedimientos de contratación y despido

  Programa de concientización y capacitación en seguridad

- **Gestión de activos.**

  Clasificación y etiquetado de activos de información

  Instrucciones de manejo y almacenamiento de los activos

- **Control de acceso.**

  Política para contraseñas y autenticación de múltiples factores

  Gestión de privilegios y autorizaciones

- **Seguridad en criptografía.**

  Empleo de encriptación y firma digital para resguardar datos en movimiento y almacenados.

Gestión de claves criptográficas

- **Seguridad física y del entorno.**

  Acceso controlado a instalaciones y áreas restringidas

  Medidas de protección contra incendios, inundaciones y otros desastres

- **Seguridad en las operaciones.**

  Métodos de supervisión de los registros de seguridad

  Gestión de parches y actualizaciones de software

- **Seguridad en las comunicaciones.**

  Seguridad en redes y transmisión de datos.

  Política de uso aceptable de dispositivos móviles y redes inalámbricas.

- **Gestión de incidentes de seguridad.**

  Procedimientos de notificación, respuesta y recuperación ante incidentes de seguridad

  Análisis y aprendizaje de incidentes

- **Gestión de la continuidad del negocio.**

  Plan de continuidad del negocio y recuperación ante desastres

  Pruebas y actualizaciones periódicas del plan

- **Cumplimiento normativo y legal.**

  Revisión de cumplimiento con leyes, regulaciones y estándares aplicables

  Procedimientos para la protección de datos personales y privacidad

  Esta propuesta es solo una base para la elaboración de una política de seguridad en una organización. Cada empresa debe adaptar y personalizar su política según sus necesidades específicas, riesgos y entorno regulatorio.

La política de seguridad es un documento redactado por los autores que brinda una estructura y directrices generales para que cualquier organización pueda utilizar como punto de partida para desarrollar su propia política de seguridad. Sin embargo, es importante tener en cuenta que esta política debe ser adaptada y personalizada para satisfacer los objetivos y requisitos específicos de cada organización.

Cada entidad tiene sus propias necesidades, recursos y riesgos particulares, por lo tanto, es fundamental realizar un análisis exhaustivo de las características y requerimientos de

la organización antes de implementar cualquier política de seguridad. Esto garantiza que la política resultante sea adecuada, relevante y efectiva en la protección de los activos de información y el cumplimiento de los objetivos establecidos.

Las normas genéricas que se desarrollan a continuación se apoyan en los controles de seguridad establecidos en la norma ISO 27002:2013 como referencia para aplicar medidas de seguridad de la información. La tabla 4 muestra una visión general de los 14 dominios de la norma ISO/IEC 27002:2013, con un total de 35 objetivos de control y 114 controles, se proporciona los títulos de los dominios y el número total de objetivos de control y controles por dominio [23]. Para un desglose completo de cada objetivo de control y control específico, se debe hacer referencia a la norma completa.

Dominio	Número de Objetivos de Control	Número de Controles
1. Política de seguridad	1	2
2. Organización de la seguridad de la información	2	7
3. Seguridad del personal	1	6
4. Gestión de activos	2	10
5. Control de acceso	7	14
6. Criptografía	1	2
7. Seguridad física y del entorno	2	15
8. Gestión de las operaciones y las comunicaciones	10	14
9. Seguridad de las comunicaciones	2	7
10. Adquisición, desarrollo y mantenimiento de sistemas de información	6	13
11. Gestión de las relaciones con los proveedores	2	5
12. Gestión de incidentes de seguridad de la información	2	7
13. Gestión de la continuidad del negocio	1	4
14. Cumplimiento	8	8
Total	35	114

Tabla 4. Resumen ISO 27002 [23].

4.3 Normas genéricas de una política de seguridad.

POLÍTICA DE RESPONSABILIDAD DE LOS USUARIOS
Descripción: Esta política establece las responsabilidades que tienen los usuarios de los sistemas informáticos y de información dentro de la organización, asegurando el uso correcto y seguro de los recursos de TI. A los usuarios al ingresar a la organización se les asigna un usuario y contraseña, las credenciales entregadas son de absoluta responsabilidad del usuario quienes tienen que proteger y no compartir las credenciales.
Alcance: Esta política es aplicable a todos los usuarios que hagan uso de una conexión a dispositivos o aplicaciones que soliciten contraseñas y validaciones para su ingreso dentro de la organización.
Objetivo: Garantizar que los usuarios comprendan sus responsabilidades en relación con el uso de los recursos de TI y las consecuencias de un uso incorrecto o irresponsable. Asegurar que los activos de información se utilicen de forma segura y eficaz, y que se respeten los derechos de los demás usuarios
Guía de Implementación (Criterios) • **Formación:** Todos los usuarios deben recibir formación adecuada en sus responsabilidades de seguridad. • **Acuerdos de usuario:** Todos los usuarios deben firmar un acuerdo de usuario en el que acepten cumplir con las políticas de seguridad de la organización. • **Cumplimiento:** Los usuarios deben ser conscientes de las posibles consecuencias, tanto disciplinarias como legales, del incumplimiento de las políticas de seguridad.
Responsables: • **Gerentes:** Asegurar que sus equipos cumplen con las políticas. • **Departamento de Seguridad de la Información:** Proporcionar formación y orientación sobre las políticas. • **Usuarios:** Cumplir con las políticas y reportar cualquier infracción.
Referencias de control según la ISO 27002:2013. • **7.2.2: Concientización, formación y capacitación en seguridad de la información.** • **9.1 Requisitos de negocio para el control de accesos** • **9.3 Responsabilidades del usuario.** • **9.4 Control de acceso a sistemas y aplicaciones.**

POLÍTICA GENERAL DE ACCESO A LA INFORMACIÓN
Descripción: Esta política define los principios y directrices para garantizar el acceso controlado a la información de la organización, protegiendo así la confidencialidad, y disponibilidad de los activos de información. La conexión a la información de la empresa deberá ser permitida sólo a usuarios habilitados, los datos se deben transmitir de manera codificada en la red, adicional debe manejar privilegios restringidos.
Alcance: Esta política aplica a todos los empleados, contratistas, socios y cualquier otra parte que tenga acceso y utilice los sistemas de información y las instalaciones de TI de la organización.
Objetivo: Regular y controlar el acceso a la información de la organización, asegurando que se conceda sólo a las partes autorizadas y sólo para los propósitos autorizados, y garantizando que la información se proteja de accesos no autorizados.
Guía de implementación: (criterios) 1. **Clasificación de la información:** Los activos de información deben ser clasificados de acuerdo con su nivel de sensibilidad y los controles de acceso se deben implementar en consecuencia. 2. **Autenticación:** Los usuarios deben ser autenticados antes de concederles el acceso a los sistemas de información. 3. **Gestión de derechos de acceso:** Los derechos de acceso deben ser otorgados en función de las necesidades de negocio y se deben revisar regularmente. 4. **Registros de acceso:** Se deben mantener registros de las actividades de acceso a la información.
Responsables: • **Gerentes:** Responsables de clasificar la información y determinar los derechos de acceso. • **Departamento de Seguridad de la Información:** Proporcionar formación y orientación sobre las políticas. • **Usuarios:** Responsables de cumplir con la política y utilizar las credenciales de acceso de manera segura.
Referencias de control según la ISO 27002:2013. • **8.2: Clasificación de la información.** • **9.2: Gestión de acceso de usuario.** • **9.3: Control de acceso a los sistemas y aplicaciones.** • **9.4: Seguridad en la gestión de los secretos de acceso.**

POLÍTICA DE MONITOREO DE SEGURIDAD DE LA INFORMACION
Descripción: Esta política establece las directrices para el monitoreo constante y la revisión de la seguridad de la información, para garantizar que los controles de seguridad son efectivos y que se detectan y manejan adecuadamente los incidentes de seguridad. Además de garantizar la supervisión por personal capacitado.
Alcance: Esta política aplica a todos los sistemas de información y redes de la organización, y a todos los empleados, contratistas, socios y cualquier otra parte que tenga acceso a estos sistemas. Así también a los responsables del análisis de incidentes de red y dispositivos dentro de la organización.
Objetivo: Proporcionar un marco para el monitoreo constante de la seguridad de la información, para detectar y manejar incidentes de seguridad, para garantizar el cumplimiento con las políticas y estándares de seguridad de la organización, y para mejorar continuamente la efectividad de los controles de seguridad.
Guía de Implementación (Criterios) 1. **Monitoreo de la seguridad:** Todos los sistemas y redes deben ser monitoreados continuamente para detectar y manejar incidentes de seguridad. 2. **Revisión de los controles de seguridad:** Los controles de seguridad deben ser revisados regularmente para garantizar su efectividad. 3. **Informes de seguridad:** Deben generarse informes de seguridad regularmente y ser revisados por la alta dirección. 4. **Mejora continua**: Los resultados del monitoreo y la revisión de la seguridad deben ser utilizados para mejorar continuamente los controles de seguridad. Revisar el incidente una vez ocurrido el daño no es suficiente, se requiere supervisión en tiempo real para la detección y respuesta inmediata. **5.** Incorporar responsabilidades y protocolos para manipular los eventos y debilidades de la seguridad de la información.
Responsables: 1. **Departamento de Seguridad de la Información:** responsable del monitoreo de la seguridad y de la generación de informes de seguridad. 2. **Gerentes:** Responsables de la revisión de los informes de seguridad y de garantizar el cumplimiento con las políticas de seguridad en sus equipos. **3. Usuarios:** Responsables de cumplir con las políticas de seguridad y de reportar cualquier incidente de seguridad.
Referencias de control según la ISO 27002:2013. • **12.4: Registro y monitoreo.** • **12.7: Gestión de la seguridad de la información en los proyectos.** • **16.1: Gestión de incidentes y mejoras de la seguridad de la información**.

POLÍTICA DE RESPALDO DE INFORMACION
Descripción: Esta política proporciona las directrices necesarias para realizar respaldos regulares de la información vital de la organización, con el fin de protegerla contra pérdidas, daños o corrupción.
Alcance: Esta política se aplica a todos los datos críticos almacenados en los sistemas de la organización, y a todas las personas que tienen acceso a estos datos.
Objetivo: Salvaguardar la integridad y disponibilidad de los datos de la organización mediante respaldos regulares y efectivos, y asegurarse de que estos respaldos se almacenen de forma segura y puedan ser recuperados de manera eficiente cuando sea necesario.
Guía de Implementación (Criterios) 1. **Identificación de datos críticos**: Identificar los datos que son críticos para el funcionamiento de la organización y que necesitan ser respaldados. 2. **Programación de respaldos:** Establecer un programa regular para respaldar los datos identificados, considerando el nivel de actividad y la importancia de los datos. 3. **Almacenamiento de respaldos:** Almacenar los respaldos en una ubicación segura y accesible, preferiblemente en un lugar diferente al de los datos originales. 4. **Prueba de recuperación:** Realizar pruebas periódicas para asegurarse de que los datos respaldados pueden ser recuperados eficientemente.
Responsables: • **Departamento de TI:** Responsable de la implementación de la política, realización de respaldos, almacenamiento seguro de respaldos y pruebas de recuperación. • **Gerentes:** Responsables de identificar los datos críticos dentro de sus respectivas áreas que necesitan ser respaldados. • **Usuarios:** Responsables de adherirse a las políticas y procedimientos de respaldo, y de reportar cualquier problema o incidente relacionado con los respaldos.
Referencias de control según la ISO 27002:2013. • **12.3: Protección contra malware.** • **12.5: Copia de seguridad.** • **13.2: Transferencia de información.**

POLÍTICA DE PROTECCION CONTRA ATAQUES INTERNOS O EXTERNOS
Descripción: Esta política define las medidas necesarias para identificar, prevenir y responder a ataques cibernéticos internos o externos, asegurando así la integridad, confidencialidad y disponibilidad de la información de la organización.
Alcance: Esta política se aplica a todos los sistemas, redes y datos de la organización, así como a todos los empleados, contratistas y terceros que tienen acceso a los mismos.
Objetivo: Proteger la información de la organización contra amenazas internas y externas mediante la implementación de controles apropiados de seguridad de la información y de respuesta a incidentes.
Guía de Implementación (Criterios). 1. **Identificación de amenazas:** Utilizar técnicas de análisis de riesgos para identificar las amenazas potenciales a los sistemas y datos de la organización. 2. **Prevención de ataques:** Implementar controles preventivos, como firewalls, sistemas de detección de intrusos y formación en seguridad para los usuarios. 3. **Detección de ataques:** Monitorizar regularmente los sistemas y redes para detectar signos de un ataque. 4. **Respuesta a ataques:** Establecer procedimientos claros para responder a un ataque, que pueden incluir la contención del incidente, la erradicación de la amenaza y la recuperación de los sistemas y datos.
Responsables: • **Departamento de Seguridad de la Información/TI:** Responsable de la implementación de la política y de las medidas de prevención, detección y respuesta. • **Empleados, contratistas y terceros:** Responsables de cumplir con la política y de informar de cualquier actividad sospechosa o incidente de seguridad.
Referencias de control según la ISO 27002:2013 • **12.4: Redes de comunicación y operaciones de gestión.** • **12.6: Gestión de vulnerabilidades técnicas.** • **13.1: Seguridad de la información en la gestión de incidentes.**

POLÍTICA DE CONFIDENCIALIDAD DE LA INFORMACION
Descripción: Esta política establece las directrices para garantizar que la información sensible o confidencial de la organización se maneje adecuadamente para prevenir su acceso, divulgación o alteración no autorizada.
Alcance: Esta política es aplicable a toda la información confidencial de la organización, independientemente de su formato o medio de almacenamiento. Abarca a todos los empleados, contratistas, socios y terceros que manejan información confidencial en nombre de la organización.
Objetivo: El objetivo principal de esta política es proteger la información confidencial de la organización manteniendo su privacidad e integridad, y garantizar el cumplimiento de las leyes y regulaciones de privacidad y protección de datos aplicables.
Guía de Implementación (Criterios) 1. **Clasificación de la Información:** Clasificar todos los datos de la organización según su nivel de sensibilidad y confidencialidad**.** 2. **Acceso a la Información:** Restringir el acceso a la información confidencial sólo a las personas autorizadas. 3. **Protección de Datos:** Implementar medidas de seguridad físicas y digitales para proteger la información confidencial de la divulgación no autorizada, como el cifrado de datos y el bloqueo físico de los archivos. 4. **Capacitación:** Proporcionar formación regular a los empleados y contratistas sobre la importancia de la confidencialidad de la información y las mejores prácticas para su manejo seguro.
Responsables: • **Departamento de Seguridad de la Información/TI:** Encargado de implementar y supervisar el cumplimiento de la política. • **Todos los empleados, contratistas y terceros:** Responsables de adherirse a la política y de manejar la información confidencial de manera segura y apropiada.
Referencias de control según la ISO 27002:2013. • **8.2: Clasificación de la Información.** • **9.2: Acceso a la Información y Privilegios de Acceso.** • **9.4: Control de Acceso a la Información y a las Funciones de Aplicación**

5. Resultados y discusión

El desarrollo de políticas de seguridad informática tiene un impacto significativo en las organizaciones, obteniendo diversos beneficios y ventajas que refuerzan su estructura operativa y su posición en el mercado. Aquí están algunas de las principales ventajas:

1. **Protección de activos:** Las políticas de seguridad ayudan a proteger los activos de la organización, incluyendo datos, sistemas, redes y equipos, contra posibles amenazas y vulnerabilidades.
2. **Mejora de la confianza:** Al implementar políticas de seguridad efectivas, la organización puede mejorar la confianza de sus clientes, proveedores y otros interesados en la seguridad de sus activos y datos.
3. **Prevención de incidentes:** Las políticas de seguridad contribuyen a evitar sucesos de seguridad, como el robo de información o la entrada no permitida a sistemas o redes, lo que puede dañar la imagen de la empresa.
4. **Cumplimiento normativo:** En muchos casos, existen regulaciones y leyes que exigen la implementación de políticas de seguridad en determinadas organizaciones, como la banca, la salud y el sector público. Al cumplir con estas regulaciones, la organización puede evitar multas y sanciones.

   Para ilustrar, en Ecuador es imperativo adherirse a la Ley de Protección de Datos Personales (**LOPDP**). Esta legislación, repleta de elementos cruciales para la seguridad de la información, contiene diversos artículos de vital importancia. Algunos de estos artículos fundamentales, como ejemplos representativos de la ley, se mencionarán a continuación:

   *"**Articulo 5 LOPDP.** Integrantes del sistema de protección de datos personales. Son parte del sistema de protección de datos personales, los siguientes:*

   1. *Titular*

   2. *Responsable del tratamiento*

   3. *Encargado del tratamiento*

   4. *Destinatario*

   5. *Autoridad de Protección de Datos personales; y,*

6. *Delegado de protección de datos personales* [24].*"*

*"**Articulo 45 LOPDP.** Garantía del secreto de las comunicaciones y seguridad de datos personales. - Para la correcta prestación de los servicios de telecomunicaciones y la apropiada operación de redes de telecomunicaciones, los prestadores de servicios de telecomunicaciones deben garantizar el secreto de las comunicaciones y seguridad de datos personales. Únicamente por orden judicial, los prestadores de servicios de telecomunicaciones podrán utilizar equipos, infraestructuras e instalaciones que permitan grabar los contenidos de las comunicaciones específicas dispuestas por los jueces competentes. Si se evidencia un tratamiento de grabación o interceptación de las comunicaciones no autorizadas por orden judicial se aplicarán lo dispuesto en la presente Ley* [24].""

Así también tenemos el **COIP (CODIGO ORGANICO INTEGRAL PENAL**) que como ejemplo presenta los siguientes artículos:

***"Artículo 178 del COIP. Violación a la intimidad**. La persona que, sin contar con el consentimiento o la autorización legal, accede intercepta, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de voz, audio y video, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio será sancionada con pena privativa de libertad de uno a tres años* [25].**"**

*"**Artículo 180 COIP. Difusión de información de circulación restringida.** La persona que difunda información de circulación restringida será sancionada con pena privativa de libertad de uno a tres años. Es información de circulación restringida:*

a) La información que está protegida expresamente con una cláusula de reserva previamente prevista en la ley.
b) La información producida por la Fiscalía en el marco de una investigación previa.
c) La información acerca de las niñas, niños y adolescentes que viole sus derechos según lo previsto en el Código Orgánico de la Niñez y Adolescencia.

5. **Mejora de la eficiencia:** Al implementar políticas de seguridad adecuadas, la empresa puede optimizar la eficacia de sus operaciones, reduciendo las interrupciones o demoras causadas por incidentes de seguridad.

6. **Concientización y educación en seguridad**: Las políticas de seguridad fomentan la concienciación y educación en seguridad entre los empleados y colaboradores, lo que ayuda a prevenir errores humanos y reduce la probabilidad de que los usuarios caigan en ataques de ingeniería social, como el phishing.
7. **Reducción de costos a largo plazo:** Aunque la implementación de políticas de seguridad puede requerir una inversión inicial, la protección que brindan puede reducir los costos a largo plazo asociados con la recuperación de incidentes de seguridad.
8. **Establecimiento de roles y responsabilidades**: Una política de seguridad claramente definida asigna responsabilidades específicas a los empleados y equipos de seguridad y TI, garantizando que todos entiendan sus roles en la protección de los activos y la información de la organización

Esta investigación diseñó su propuesta de política de seguridad basándose en la normativa ISO 27000, enfocándose particularmente en la ISO 27002:2013. Esta norma permite una gestión eficaz de riesgos y desarrollo de planes de acción, proveyendo orientaciones para la implementación de controles de seguridad.

Es así que, para determinar una red de campus eficaz y segura, es esencial tener en cuenta una variedad de componentes y tecnologías, entre los cuales destacan los siguientes en la tabla 5:

Componente	Descripción
Firewall	Este componente es esencial para bloquear el tráfico no deseado y controlar el flujo de datos dentro y fuera de la red.
Red Privada Virtual (VPN)	Una VPN permite a los usuarios acceder a la red de forma segura desde ubicaciones remotas.
Sistema de detección de intrusos (IDS)	Los sistemas IDS monitorean la red en busca de patrones de comportamiento sospechoso o inusual que podrían indicar un ataque.

Sistema de Prevención de Intrusiones (IPS)	Un IPS es similar a un IDS pero tiene la capacidad de bloquear o prevenir la actividad sospechosa identificada.
Autenticación de doble factor (2FA)	Este componente agrega una capa adicional de seguridad al requerir que los usuarios proporcionen dos formas de identificación antes de conceder acceso a la red.
Software antivirus	Este software es esencial para proteger la red contra malware, virus y otras amenazas de seguridad.
Control de acceso a la red (NAC)	Los controles de acceso a la red verifican la identidad de los dispositivos y usuarios antes de permitirles acceder a la red.
Enrutadores y switches seguros	Estos dispositivos controlan el tráfico de red y, cuando están habilitados con funciones de seguridad, pueden ayudar a proteger contra amenazas.
Gestión de parches y actualizaciones	Un sistema para gestionar parches y actualizaciones de software y hardware para garantizar que todos los componentes de la red estén actualizados y protegidos contra las últimas amenazas.
Copias de seguridad y recuperación de desastres	Este componente es crucial para garantizar que los datos puedan ser recuperados en caso de pérdida o daño.

Tabla 5. Componentes de red y Seguridad.

Cabe recordar que la implementación de estos componentes debe ser adecuada al contexto y las necesidades de cada organización, y debe formar parte de una estrategia de seguridad integral que incluya también políticas de seguridad, formación de los usuarios, monitoreo y actualización constantes.

Los incidentes que afectan la confidencialidad y disponibilidad de información pueden comprometer seriamente una organización. Prevenir y responder a estos incidentes

implica fortalecer las defensas de red, implementar autenticación fuerte, capacitar al personal y prepararse para la recuperación de desastres, manteniendo una vigilancia constante y adaptándose a nuevas amenazas de seguridad.

La seguridad de la red es una preocupación fundamental en el panorama actual del ciberespacio. Es esencial que las organizaciones tomen las medidas apropiadas para proteger su información y activos digitales, fortaleciendo la resiliencia de sus sistemas y preparándose para responder eficazmente a incidentes. El continuo desarrollo e implementación de políticas y tecnologías de seguridad eficaces, alineadas con las normas y prácticas recomendadas, son importantes para mantener la confidencialidad y disponibilidad de los datos. El compromiso con la seguridad de la red es un paso vital para garantizar el futuro digital de cualquier organización. Para garantizar el cumplimiento de la política de seguridad, los equipos de seguridad y TI deben comprender claramente los requerimientos de seguridad e implementar procesos adecuados para asegurar el acceso seguro a datos y servicios.

Un factor también a tomar en cuenta en el desarrollo de políticas es el ROSI (Return on Security Investment) debido a que evalúa los beneficios versus los costos de inversión en seguridad. Incluye aspectos como contratación, licencias y entrenamiento, contrastándolos con beneficios como confianza del cliente y eficiencia de red. El ROSI se calcula como el porcentaje de beneficios en comparación con el costo total [26].

En un escenario hipotético tras un análisis de riesgo en una red de campus, identificamos tres amenazas críticas: ataques DDoS, accesos no autorizados y pérdida de datos. Estimamos la frecuencia de ocurrencia y el impacto financiero de cada riesgo con valores supuestos para cuantificar su magnitud como se observa en la tabla 6.

Tipo Ataque	Probabilidad	Impacto Financiero
Ataque DDoS	30%	$50.000
Acceso no autorizado	20%	$100.000
Pérdida de datos	10%	$200.000

Tabla 6. Riesgos valores supuestos.

Calcular el riesgo anual sin medidas de seguridad: Multiplicamos la probabilidad de cada riesgo por su impacto financiero y sumamos los resultados.

Riesgo anual sin medidas de seguridad = (0.3 * $50,000) + (0.2 * $100,000) + (0.1 * $200,000) = $15,000 + $20,000 + $20,000 = $55,000

Al implementar medidas de seguridad, como un firewall, un sistema de prevención de intrusiones (IPS) y una solución de copias de seguridad y recuperación. Estas medidas reducen las probabilidades de ocurrencia de los riesgos como se observa en la tabla 7.

Tipo Ataque	Probabilidad	Medida Seguridad
Ataque DDoS	5%	Firewall e IPS
Acceso no autorizado	8%	Firewall e IPS
Pérdida de datos:	2%	Copias de Seguridad

Tabla 7. Medidas de seguridad aplicadas.

Se calcula el riesgo anual con medidas de seguridad:

Riesgo anual con medidas de seguridad = (0.05 * $50,000) + (0.08 * $100,000) + (0.02 * $200,000) = $2,500 + $8,000 + $4,000 = $14,500

Se estima el costo anual de las medidas de seguridad: Supongamos que el costo anual de las medidas de seguridad es de $30,000, incluidos los gastos de hardware, software, mantenimiento y capacitación del personal.

Calculo el ROSI:

ROSI = ($55,000 - $14,500) - $30,000 = $40,500 - $30,000 = $10,500.

En este ejemplo, el ROSI es de $10,500, lo que indica que la inversión en medidas de seguridad proporciona un retorno económico positivo al reducir el riesgo en la red de campus.

La aplicación del modelo ROSI aporta un enfoque cuantitativo y tangible para evaluar la eficiencia de las inversiones en seguridad de la información. Al balancear los costos de las medidas de seguridad con el valor económico de los riesgos mitigados, las organizaciones pueden tomar decisiones de inversión más informadas y justificadas, promoviendo una ciberseguridad efectiva y económicamente viable.

Para culminar, en una red de campus diseñada con un esquema de Backbone colapsado, es fundamental que se seleccionen y adquieran equipos adecuados para cada una de las

tres capas de la arquitectura de red: acceso, distribución y núcleo. En la tabla 8 se muestra algunos ejemplos de equipos que satisfacen estas necesidades:

Componente	Dispositivo	Precio	Observación
Capa de acceso	Switch CISCO Designed Business CBS350-24FP-4G | 24 puertos GE | PoE completo	1035	https://goo.su/bwwmU
Capa de distribución	Cisco Ingram Catalyst 9300 C9300-24T 24 puertos gestionados 10/100/1000Base-T Gigabit	3070	https://goo.su/nLJbX
Capa de núcleo	Catalyst 9500 40-port 10Gig switch, Network Essentials.	18285	https://goo.su/N2kC
Cableado	Rollo Cable Nexxt Utp Cat 6 100m Interior Certificado Gigabit	125	https://shre.ink/lCuM
Fibra Óptica	Cable Fibra Óptica Drop 4h | G657a2 | 2km	300	https://shre.ink/lCb2
Implementación	Configuración Inicial de red.	2800	

Tabla 8. Equipos red de campus

Una vez analizados los diferentes parámetros dentro de este estudio se puede definir el siguiente modelo corto de propuesta de política de seguridad tomando en cuenta

considerando la Funcionalidad y la Ciberseguridad ante Incidentes contra la Confidencialidad y Disponibilidad.

Política de Seguridad para el Diseño de una Red de Campus Empresarial

Descripción: Esta política tiene como objetivo establecer los lineamientos para el diseño de una red de campus empresarial que garantice la funcionalidad y la seguridad de la información contra incidentes que amenacen la confidencialidad y la disponibilidad de la información.

Alcance: Esta política aplica a todas las áreas de la empresa que estén involucradas en el diseño, implementación, mantenimiento y uso de la red de campus empresarial.

Objetivo: Asegurar que la red de campus empresarial esté diseñada de manera que garantice la continuidad del negocio, minimice los riesgos de seguridad y cumpla con las leyes y regulaciones pertinentes.

Guía de Implementación:

1. **Diseño Modular:** Implementar un diseño de red jerárquico y modular que mejore la eficiencia y facilite la administración de la red.
2. **Protección de Datos:** Incluir soluciones avanzadas de seguridad como firewalls, VLANs y VPNs, y tecnologías de encriptación para proteger la información.
3. **Control de Acceso:** Implementar controles de acceso sólidos que limiten el acceso a la información solo a los usuarios autorizados.
4. **Monitoreo y Respuesta**: Establecer un sistema de monitoreo de la red que permita detectar y responder rápidamente a incidentes de seguridad.
5. **Continuidad del Negocio:** Implementar soluciones de respaldo y recuperación de desastres para garantizar la disponibilidad de la información.

Responsables: La Dirección de Tecnología será la responsable de la implementación de esta política, con el apoyo de todas las áreas de la empresa.

Referencias de Control: Esta política se basa en las mejores prácticas de seguridad y está alineada con los estándares ISO 27002:2013.

Evaluación: La efectividad de esta política se evaluará a través del análisis de ROSI (Return on Security Investment), para asegurar un equilibrio entre la inversión en seguridad y los beneficios obtenidos.

6. Conclusiones

- El diseño de una red de campus empresarial es una tarea importante que requiere un enfoque metódico y meticuloso para garantizar que los componentes seleccionados sean adecuados para su funcionalidad. Un diseño de red de campus empresarial debe tener en cuenta factores como seguridad, conectividad, escalabilidad, disponibilidad y rendimiento. Además, debe estar diseñado para satisfacer las necesidades de la empresa y proporcionar una solución sostenible a largo plazo.
- Es fundamental que las organizaciones adopten diferentes estándares y herramientas para abordar y reducir las vulnerabilidades que afectan la confidencialidad y disponibilidad de sus redes. Estas estrategias incluyen el uso de protocolos de seguridad actualizados, la implementación de soluciones de seguridad perimetral como firewalls y sistemas de prevención de intrusiones, así como la adopción de políticas de seguridad rigurosas que fomenten una cultura de concienciación en seguridad.
- Una política de seguridad de la información siempre debe definirse como una responsabilidad que debe usarse de manera consistente y efectiva que nazca desde los usuarios, ya que el buen cumplimiento permitirá mantener una cultura de seguridad en la organización y proteger el activo más importante que es la información, además el desarrollo de una política adaptable que mantenga un proceso constante de actualización permitirá acoplarse a los cambios del entorno organizativo y por ende soportar las nuevas amenazas, regulaciones y normas que unido a una evaluación del retorno de la inversión en seguridad asegurará que los beneficios obtenidos justifiquen los costos de la inversión en los sistemas de información
- Para garantizar una seguridad adecuada, los equipos deben contar con características mínimas que les permitan proteger eficazmente los recursos y la información de la organización como: Protección antivirus, actualizaciones y parches de seguridad, políticas de contraseñas, cifrado de datos, control de

acceso, políticas de respaldo, etc., adicional los equipos de red deben manejar características específicas acorde al diseño propuesto.

- Esta propuesta de estrategia de seguridad cumple con las normativas actuales, tomando en cuenta leyes como la Ley de Protección de Datos Personales, COIP y otras similares, con el propósito de adecuarse a los requerimientos contemporáneos de distintos ámbitos comerciales y gestionar la información de forma apropiada para prevenir riesgos cibernéticos.

Referencias

[1] Atlas, “8 pasos para implementar un plan de ciberseguridad”, [En línea]. Disponible: https://www.atlas.com.co/8-pasos-para-implementar-un-plan-de-ciberseguridad/

[2] W. R. Marchand-Niño and B. P. Guzman Fonseca, "Social Engineering for Diagnostic the Information Security Culture," 2019 IEEE 39th Central America and Panama Convention (CONCAPAN XXXIX), 2019, pp. 1-6, doi: 10.1109/CONCAPANXXXIX47272.2019.8977071.

[3] J. Zhang, "Design of Campus Network Security System Based on Network Information Security," 2022 IEEE Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC), 2022, pp. 1194-1197, doi: 10.1109/IPEC54454.2022.9777499.

[4] J. A. Armas, “Ciberseguridad: como adoptar medidas para proteger sus activos de información”, review, vol. 4, n.º 2, pp. 20-21, feb. 2020.

[5] “¿Qué es una red de área de campus (CAN)?”, Cloudfare, [En línea]. Disponible: https://www.cloudflare.com/es-es/learning/network-layer/what-is-a-campus-area-network/

[6] J. Lu, "Research and Implementation of Security Technology in Campus Network Construction," 2019 International Conference on Computer Network, Electronic and Automation (ICCNEA), 2019, pp. 219-224, doi: 10.1109/ICCNEA.2019.00050.

[7] G. Tolosa, G, “Protocolos y modelo OSI.”, (2014). [En línea]. Disponible: http://www. tyr. unlu. edu. ar/pub/02-ProtocolosOSI. pdf.

[8] J. Guevara, D. Quizhpe, “Diseño de la Red de Campus de la empresa “Equipos y Suministros de Telecomunicaciones EQUYSUM” de la ciudad de Quito. Tesis Pregrado. Ingeniería Electrónica, Universidad Politécnica Salesiana, Quito, 2017.

[9] G. Chávez, L. Tuárez, “Propuesta de red de datos para la gestión de los servicios de red en el CAMPUS POLITÉCNICO DE LA ESPAM MFL”, Tesis Pregrado, Carrera de Informática, Escuela superior politécnica agropecuaria de Manabí Manuel Félix López, Calceta, Manabí, 2016.

[10] A. Mohammed, M. Emran Hossain, M. Parvez. "Design and implementation of a secure campus network." International Journal of Emerging Technology and Advanced Engineering 5, no. 7 (2015): 370-374.

[11] T. Shanmugam and B. Malarkodi, "Analysis of Campus Network Management Challenges and Solutions," 2019 TEQIP III Sponsored International Conference on Microwave Integrated Circuits, Photonics and Wireless Networks (IMICPW), 2019, pp. 312-316, doi: 10.1109/IMICPW.2019.8933236.

[12] F. N. Solarte, E. R. Enríquez Rosero, y M. del C. Benavides, “Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001”, rte, vol. 28, n.º 5, dic. 2015.

[13] J. Figueroa, R. Rodríguez, C. Bone, J. Saltos. (2018). La seguridad informática y la seguridad de la información. Polo del Conocimiento, 2(12), 145-155. [En línea]. Disponible en: http://dx.doi.org/10.23857/pc.v2i12.420

[14] P. Gracia, “Top 10 vulnerabilidades web de 2021”, INCIBE, [En línea]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/top-10-vulnerabilidades-web-2021

[15] “Buenos hábitos de ciberhigiene que te ayudarán a mantener la seguridad online”, Kaspersky [En línea]. Disponible en: https://www.kaspersky.es/resource-center/preemptive-safety/cyber-hygiene-habits

[16] R. Gonzales, J. Rodríguez, “Gestión de la seguridad de la información, basado en las Normas ISO/IEC 27000 y la metodología MAGERIT, para mitigar los riesgos de TI en la empresa ITNOVATE LAB S.R.L. Chiclayo 2020”, Tesis, Facultad de ciencias físicas y matemáticas, Universidad Nacional Pedro Ruiz Gallo, Lambayeque- Perú, 2022.

[17] J. Oliva, “Aplicación de metodología para el diseño e implementación de redes de Campus Universitario”. Tesis Maestría, Departamento de Ingeniería eléctrica, Universidad de Chile, 2019.

[18] Primicias, “Ecuador registra un bajo índice de ciberseguridad”, [En línea]. Disponible en: https://www.primicias.ec/noticias/sociedad/ecuador-registra-bajo-indice-ciberseguridad/

[19] R. Borbúa, L. Herrera, R. Reyes, “Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa.” URVIO, Revista latinoamericana de Estudios de Seguridad, 2017. (20), 31-45. DOI: http://dx.doi.org/10.17141/urvio.20.2017.2571

[20] “Arquitectura de red Empresarial Cisco”, CCNA4, [En línea]. Disponible: https://ccnadesdecero.es/arquitectura-red-empresarial-cisco/
[21] “Implementación de un Diseño de Red”, CCNA3, [En línea]. Disponible: https://ccnadesdecero.es/implementacion-diseno-de-red/
[22] L. Kumari, S, Debbarma, R, Shyam, “Security Problems in Campus Network and Its Solutions”, International Journal of Advanced Engineering & Applications (IJAEA). Volume-1. pp 98-101. (2011).
[23] “Controles de ISO 27002”, Disponible: https://studylib.es/doc/1319647/resumen-de-los-controles-definidos-en-iso-27002
[24] Ley de Protección de Datos Personales Ecuador, Suplemento del Registro Oficial No. 884 de 20 de mayo del 2016.
[25] Código Orgánico Integral Penal (COIP), Registro Oficial Suplemento 180 de 10 de febrero del 2014.
[26] McGraw-Hill Education. (2014). ROSI (Return on Security Investment). In Information Security Management Handbook (pp. 1-15). McGraw-Hill Education.