AJEA (Actas De Jornadas Y Eventos Académicos De UTN)
DOI: https://doi.org/10.33414/ajea.1776.2024

Análisis de Riesgos de seguridad en Redes SDN

Security Risk Analysis in SDN Networks

Presentación: 23 y 24 de octubre de 2024

Juan Carlos CALLONI
Universidad Tecnológica Nacional, Facultad Regional San Francisco, Argentina
jccalloni@gmail.com

Antonela CALLONI
Universidad Tecnológica Nacional, Facultad Regional San Francisco, Argentina
antocalloni@gmail.com

Facundo MONDINO
Universidad Tecnológica Nacional, Facultad Regional San Francisco, Argentina
mondinofacundo254@gmail.com

Rebeca FILIPPA
Universidad Tecnológica Nacional, Facultad Regional San Francisco, Argentina
rebefilippa@gmail.com

Luciano VILLA
Universidad Tecnológica Nacional, Facultad Regional San Francisco, Argentina
lucianovilla00@gmail.com

Resumen

El presente trabajo está basado en un exhaustivo análisis de los riesgos de seguridad en las redes definidas por software (SDN), centrándose especialmente en la protección de los controladores SDN, que representan el núcleo de la arquitectura de estas redes. Se examinan las vulnerabilidades inherentes a los controladores SDN, tales como su susceptibilidad a diversos tipos de ataques, incluyendo los de denegación de servicio distribuido (DDoS). Además, se propone un método basado en el análisis para modelar y evaluar los riesgos de seguridad en estos entornos. Este método permite una representación estructurada mediante casos de uso y un análisis profundo de las amenazas a través de una matriz de riesgos, facilitando la identificación de puntos críticos de fallo y la formulación de estrategias de mitigación eficaces. Este estudio es de gran relevancia para profesionales y académicos interesados en mejorar la seguridad en redes SDN, ofreciendo un marco conceptual robusto para la gestión de riesgos en este entorno tecnológico emergente.

Palabras clave: Redes definidas por Software, Seguridad, Riesgos, Casos de uso.

Abstract

This work is based on an exhaustive analysis of security risks in software-defined networks (SDN), focusing especially on the protection of SDN controllers, which represent the core of the architecture of these networks. Vulnerabilities inherent to SDN controllers are examined, such as their susceptibility to various types of attacks, including distributed denial of service (DDoS). Furthermore, an analysis-based method is proposed to model and evaluate security risks in these environments. This method allows a structured representation through use cases and a deep analysis of threats through a risk matrix, facilitating the identification of critical points of failure and the formulation of effective mitigation strategies. This study is of great relevance for professionals and academics interested in improving security in SDN networks, offering a robust conceptual framework for risk management in this emerging technological environment.

Keywords: Software Defined Networks, Security, Risks, Use Cases.

Introducción

La Red Definida por Software (SDN) es un enfoque de red que permite a los administradores de red inicializar, controlar, cambiar y administrar el comportamiento de la red de manera dinámica mediante interfaces abiertas como el protocolo OpenFlow. SDN está cambiando la forma en que se controlan, gestionan y configuran las infraestructuras de redes de TI (Lawal, 2018).

AJEA (Actas De Jornadas Y Eventos Académicos De UTN)
DOI: https://doi.org/10.33414/ajea.1776.2024

Las redes definidas por software (SDN) han emergido como una arquitectura clave en la evolución de infraestructuras de red a gran escala, particularmente en el contexto de nuevas tendencias tecnológicas. SDN ha captado el interés de organizaciones y fabricantes, quienes han comenzado a implementar esta tecnología en centros de datos y están explorando su potencial en redes perimetrales, donde la seguridad definida por software presenta nuevos paradigmas. Además, SDN ofrece oportunidades significativas en la infraestructura de redes empresariales, destacándose por su capacidad de reducir costos operativos y de capital relacionados con la inversión en nueva infraestructura.

Sin embargo, la integración de SDN en el contexto de la seguridad de la información ha sido abordada de manera fragmentada, dejando fuera del Sistema de Gestión de la Seguridad de la Información (SGSI) aspectos cruciales del diseño e implementación de esta infraestructura. A diferencia de las redes convencionales, donde la seguridad es un aspecto integral del diseño, SDN aún enfrenta desafíos en su adopción segura, especialmente en entornos que también incluyen tecnologías emergentes como IoT, SDDC, IaaS, PaaS, SaaS, computación en la nube y virtualización (Fogelbach, 2015).

La gestión de la seguridad de la información en redes definidas por software (SDN) es muy importante dentro del contexto de un Sistema de Gestión de Seguridad de la Información (SGSI), alineado con las normas ISO/IEC 27001:2005 y 2013 (normaiso27001.es, 2024). La importancia de implementar una estrategia para planificar, ejecutar, monitorear y mejorar la seguridad de la información en una infraestructura SDN es destacada, y se identifican actividades clave para este proceso, como la evaluación de riesgos, identificación de activos, amenazas y vulnerabilidades, así como la implementación de controles. Este trabajo aportará la gestión de riesgo en el ámbito de una Universidad, en particular de la UTN Facultad Regional San Francisco.

La ISO 27001 establece la necesidad de seleccionar una metodología para la evaluación de riesgos. Métodos como Mehari, Magerit, NIST800-30 y la Guía de Gestión de Seguridad de Microsoft son opciones viables, siendo todos aplicables a infraestructuras SDN. Los principales pasos a seguir según esta Norma son: identificación de activos, valorizándolos según su función dentro de la red; identificación de amenazas y vulnerabilidades; y análisis y evaluación de los riesgos, donde se plantea el uso de una matriz de análisis de riesgos que correlacione amenazas con activos, considerando la probabilidad de materialización de riesgos.

Este enfoque asegura que solo las actividades y controles relevantes se apliquen a la infraestructura SDN dentro del SGSI, lo que garantiza una gestión de seguridad de la información eficiente y adaptada a este tipo de red.

Por último, es importante mencionar que el análisis de seguridad en controladores SDN desde una perspectiva del análisis de riesgos es un campo en constante evolución. A medida que surgen nuevas amenazas y vulnerabilidades, es necesario adaptar y mejorar continuamente las medidas de seguridad y los modelos ontológicos para garantizar una protección efectiva de la red.

El presente trabajo aportará una visión integral y actualizada sobre la importancia de la gestión de riesgos en infraestructuras de una red SDN en una Universidad, especialmente en el contexto de la seguridad de la información. Este análisis subraya la necesidad de adaptar y evolucionar las metodologías tradicionales de evaluación de riesgos, como ISO 27001, para enfrentar los desafíos únicos que presentan las redes SDN. Al abordar aspectos críticos como, la detección de amenazas y vulnerabilidades, y la implementación de controles específicos para SDN, este trabajo ofrece un marco sólido para gestionar de manera efectiva la seguridad en entornos tecnológicos emergentes.

Objetivo

Desarrollar un análisis de riesgos de seguridad en redes definidas por software (SDN) en un entorno universitario, específicamente para los controladores SDN en la red de la UTN FR San Francisco; a través del análisis de casos de uso de seguridad específicos para estos controladores, se busca definir una matriz de riesgos que permita identificar, evaluar y mitigar posibles vulnerabilidades, mejorando así la seguridad y resiliencia de la red universitaria.

Conceptos

Las redes definidas por software (SDN) son un conjunto de técnicas en el ámbito de las redes computacionales que permiten la implementación de servicios de red de manera determinista, dinámica y escalable, sin necesidad de que el administrador coordine estos servicios a nivel bajo. Esto se logra separando el plano de datos, que se encarga de enviar las tramas, del plano de control, que gestiona los dispositivos. Toda la inteligencia y lógica de control de la red se centraliza en un controlador basado en software (Cuesta, 2021) .

Una característica clave de las redes SDN es la programabilidad, que permite que todas las operaciones de red se describan como programas de software, integrando algoritmos y conceptos de programación propios del desarrollo de software. Esto facilita la implementación de medidas de seguridad, permitiendo resolver de manera eficaz y confiable muchos problemas de seguridad que afectan a las redes convencionales, mediante aplicaciones de software específicas para la seguridad de la red (Correa Chica Juan Camilo, 2020).

SDN está cambiando la forma en que se controlan, gestionan y configuran las infraestructuras de redes de TI (Lawal, 2018).

AJEA (Actas De Jornadas Y Eventos Académicos De UTN)
DOI: https://doi.org/10.33414/ajea.1776.2024

Aunque SDN ofrece beneficios en la administración centralizada y ágil de redes, también introduce riesgos de seguridad, especialmente en la capa de control, que es crucial para la interconexión del sistema. Si esta capa es vulnerada, puede causar fallos parciales o la interrupción total de los servicios. Dado el aumento en los delitos informáticos que amenazan la confidencialidad, integridad y disponibilidad (CIA) de la información en las organizaciones, es fundamental fortalecer la seguridad en las redes de datos (Alcívar Pedro, 2020).

Por ello, se propone desarrollar una guía teórico-práctica para Universidades que implementen SDN, con el objetivo de prevenir ataques como el DoS/DDoS en la capa de control. Esta guía incluirá un análisis de riesgos para identificar prácticas y herramientas efectivas para mitigar estos ataques y garantizar la autenticidad, confidencialidad y disponibilidad de la información en las redes SDN (Yibyth Tatiana Borda Ardila, 2023).

La ISO 27001 es un estándar de seguridad de la información que puede implementarse en cualquier organización para establecer buenas prácticas en la seguridad de la red. Este estándar es útil para gestionar, identificar y analizar los riesgos, lo que permite desarrollar estrategias de ciberseguridad y realizar auditorías que aseguren un control efectivo de la seguridad informática (Yibyth Tatiana Borda Ardila, 2023).

La ISO 27001 incluye un anexo (Anexo A) que contiene un listado de 114 controles distribuidos en 14 dominios. Al implementar un Sistema de Gestión de la Seguridad de la Información (SGSI), es posible seleccionar los dominios más relevantes para garantizar la seguridad en redes definidas por software (SDN). Esto ayuda a las organizaciones a proteger sus redes de manera más eficaz, siguiendo un marco reconocido internacionalmente para la seguridad de la información. Nuestro trabajo apunta en esta etapa a un análisis de riesgo de posibles tipos de ataques (ISO.ORG, 2013).

Análisis de Proyectos Similares

En el siguiente trabajo **“Propuesta De Diseño De Red De Datos Del Colegio Popular Bolivariano”.** El documento propone un diseño de red para el Colegio Popular Bolivariano, que incluye la identificación y tratamiento de riesgos mediante la metodología Magerit, siguiendo el ciclo PHVA (Planificar, Hacer, Verificar, Actuar). En la fase de planificación, se identifican los activos de la institución y se valoran según su importancia para la organización en términos de confidencialidad, integridad y disponibilidad, utilizando una escala cualitativa (Bajo, Medio, Alto). Luego, se evalúa el grado de criticidad de estos activos, clasificándolos en baja, moderada o alta criticidad (Fausto Camilo Vanegas Arévalo, 2023).

Una parte importante de este trabajo aporta a nuestro proyecto, pero no resuelve el problema que se plantea sobre tener un estudio de Análisis de Riesgos de seguridad en Redes SDN en una red híbrida universitaria mediante un conjunto de casos de uso específico.

En el siguiente trabajo **“Metodología de detección y mitigación de ataques ddos en entornos sdn basado en la norma iso/iec 27001 para mejorar la seguridad en el plano de control”** se menciona “El presente trabajo se realizó con el objetivo de desarrollar una Metodología para la implementación de una solución de seguridad relacionada a la detección y mitigación de ataques DDoS en el plano de control de SDN, capaz de ser utilizada como guía para los profesionales de la rama y demás interesados en la seguridad de la información. La metodología se desarrolló en base a la norma ISO 27001 y su alineación con el ciclo PDCA, de donde se tomaron las directrices generales para la realización de cada uno de los subprocesos de la metodología planteada: Identificación de riesgos, Planificación, Selección del mecanismo, Pruebas, Implementación, Monitoreo y Mejora” (Cheza, 2021).

Una parte importante de este trabajo servirá de aporte a nuestro proyecto, la parte de simulación y la metodología planteada pero no resuelve el problema que se plantea sobre tener un estudio de Análisis de Riesgos de seguridad en Redes SDN en una red híbrida universitaria.

Resultado y Método

El análisis de riesgos de la red de la facultad se inició tomando como referencia el diseño de la infraestructura de red existente. Con esta base, se procedió a desarrollar una serie de casos de uso que simulan los ataques más probables que podrían sufrir los sistemas. Cada caso de uso describe una secuencia de acciones que un atacante podría realizar para comprometer la seguridad de la red. A partir de estos casos de uso, se identificaron los riesgos específicos a los que está expuesta la red. Estos riesgos se clasificaron en función de su probabilidad de ocurrencia y su impacto potencial en la institución, documentándolos en una matriz de riesgos.

En la Figura 1 se muestra el diseño de una red para la UTN - Facultad Regional San Francisco, compuesta por tres conexiones WAN a Internet, cada una conectada a través de un router (Router A, B, y C). Estas conexiones están protegidas por dos firewalls (Firewall 1 y Firewall 2) que dividen la red en diferentes segmentos. El Firewall 1 conecta la red a un switch que maneja la LAN de Laboratorios y otro switch que maneja la red WiFi. El Firewall 2 está conectado a un switch que gestiona la LAN de Secretarías y a un switch adicional que se encarga de la zona desmilitarizada (DMZ), donde se encuentra un servidor o recurso crítico. Este diseño segmenta la red para proteger diferentes áreas, asegurar la gestión eficiente del tráfico, y brindar seguridad adecuada para cada segmento de la infraestructura de TI.

AJEA (Actas De Jornadas Y Eventos Académicos De UTN)
DOI: https://doi.org/10.33414/ajea.1776.2024

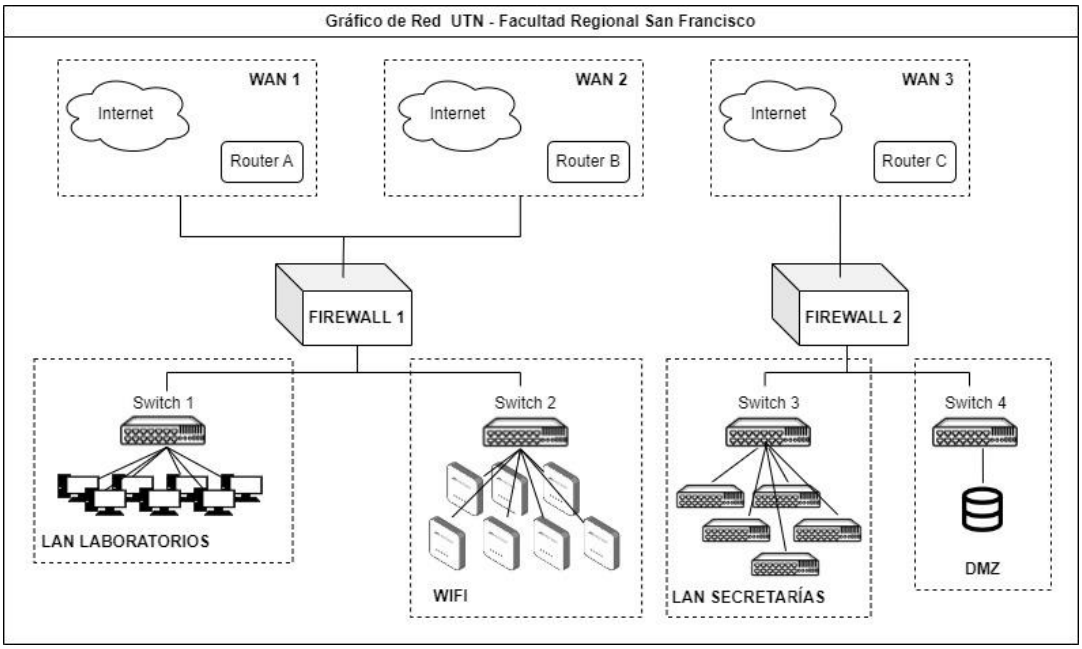

Figura 1. Gráfico de Red UTN San Francisco

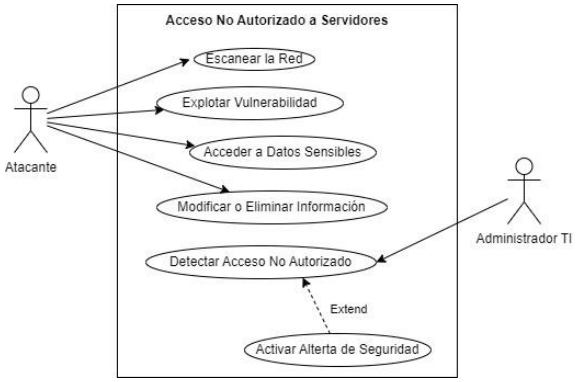

Figura 2. Acceso No Autorizado a Servicio

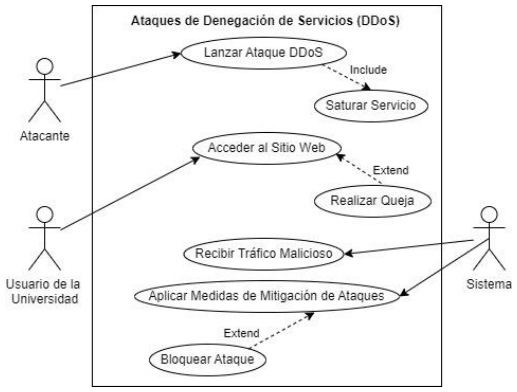

Figura 3. Ataques DDoS

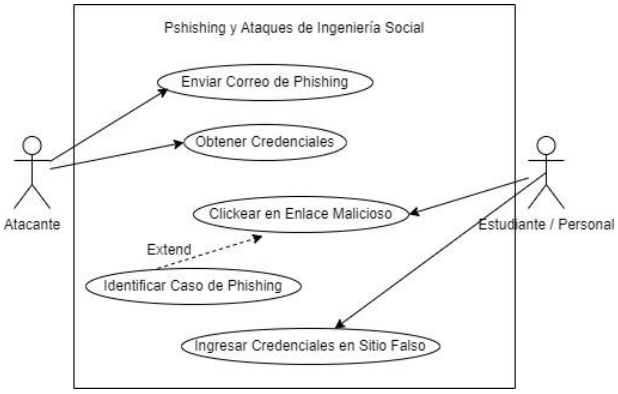

Figura 4. Pishing y ataques de Ingeniería Social

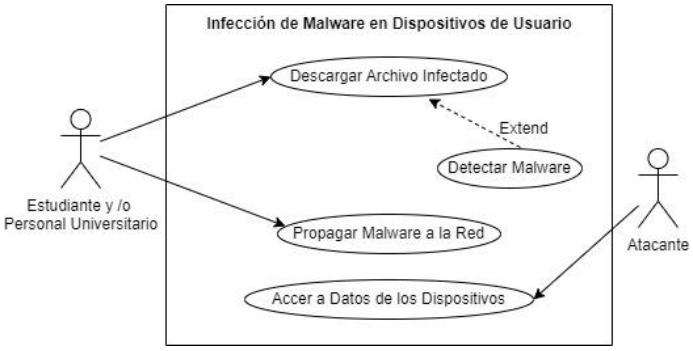

Figura 5. Infección de Malware

Los diagramas de casos de uso que se muestran en Figura 2 a Figura 9, ofrecen una visualización detallada de las secuencias de ataques más probables que podrían comprometer la seguridad de la red SDN de la institución. Cada caso de uso describe una serie de acciones que un atacante podría llevar a cabo, desde la fase de reconocimiento inicial hasta la obtención de acceso no autorizado a sistemas y datos sensibles. Los mismos se han utilizado para alimentar la matriz de riesgos.

AJEA (Actas De Jornadas Y Eventos Académicos De UTN)
DOI: https://doi.org/10.33414/ajea.1776.2024

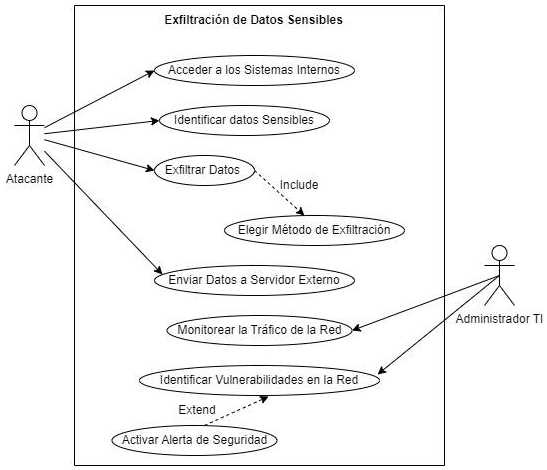

Figura 6. Exfiltración de datos sensibles

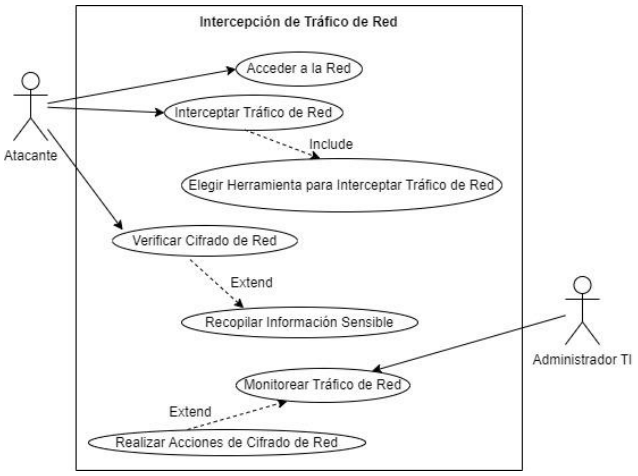

Figura 7. Intercepción de Tráfico de Red

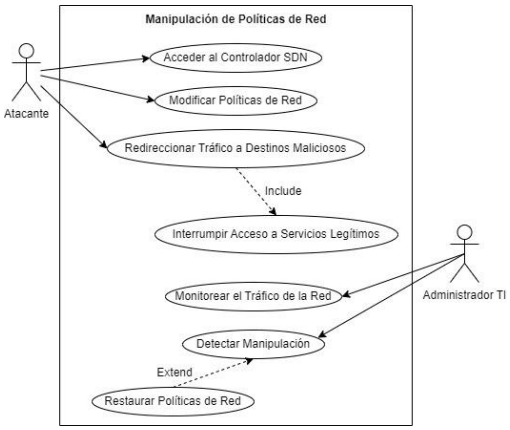

Figura 8. Manipulación de Política de Red

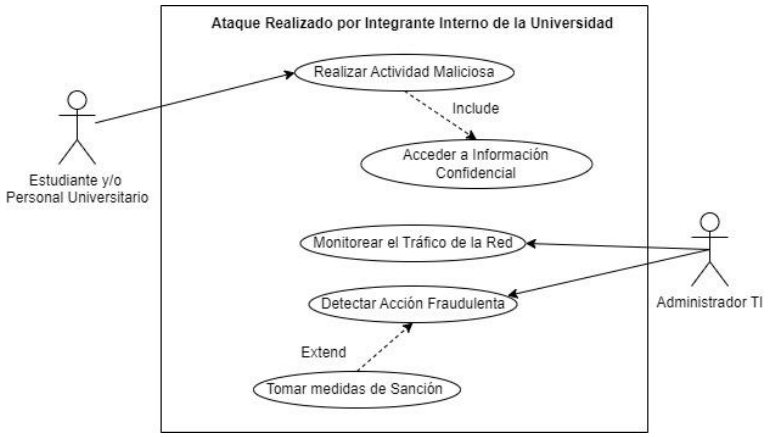

Figura 9. Ataque por integrante Interno

Tabla 1. Matriz de Riesgos de tipos de Ataques

N	Riesgo de tipo de Ataques	Probabilidad (1-5)	Impacto (1-5)	Nivel de Riesgo (P x I)	Comentarios
1	**Propagación de Malware Interno**	**4**	**5**	**20**	Puede comprometer toda la red universitaria.
2	**Ataques DDoS Externos**	**4**	**5**	**20**	Afecta gravemente la disponibilidad de servicios críticos.
3	**Falta de Capacitación en Seguridad**	**4**	**4**	**16**	Alta probabilidad de errores humanos que pueden ser explotados.
4	**Phishing Dirigido a la Comunidad Universitaria**	**4**	**4**	**16**	Alta probabilidad de que usuarios caigan en la trampa.
5	**Robo de Información por Personal Interno**	**3**	**5**	**15**	Riesgo significativo debido a la posibilidad de acceso a datos sensibles.
6	**Cambios en la Legislación de Protección de Datos**	**3**	**5**	**15**	Nuevas regulaciones pueden imponer sanciones significativas.
7	**Reputación Dañada por Incidentes de Seguridad**	**3**	**5**	**15**	Impacto a largo plazo en la confianza de la comunidad.
8	**Responsabilidad Legal y Multas**	**3**	**5**	**15**	Riesgo significativo debido a la normativa vigente en Argentina.
9	**Desactualización de Sistemas y Software**	**3**	**4**	**12**	Vulnerabilidades pueden ser explotadas si no se actualizan regularmente.
10	**Inadecuada Gestión de Contraseñas**	**3**	**4**	**12**	Contraseñas débiles pueden facilitar accesos no autorizados.
11	**Acceso No Controlado a Recursos**	**3**	**4**	**12**	Falta de políticas claras puede resultar en accesos no autorizados.
12	**Intercepción de Datos en Redes Públicas**	**3**	**4**	**12**	Uso de redes Wi-Fi públicas puede comprometer la seguridad.
13	**Fugas de Información por Errores Humanos**	**4**	**3**	**12**	Riesgo común que puede resultar en la exposición de datos sensibles.
14	**Pérdida de Productividad**	**4**	**3**	**12**	Afecta a estudiantes y personal, generando retrasos.
15	**Inexistencia de Protocolos de Respuesta a Incidentes**	**2**	**5**	**10**	Dificultad en la gestión de incidentes de seguridad.
16	**Desastres Naturales**	**2**	**5**	**10**	Riesgo moderado, pero con alto impacto potencial.
17	**Competencia Desleal y Robo de Propiedad Intelectual**	**2**	**4**	**8**	Riesgo moderado, pero puede afectar la reputación.

La matriz de riesgos presentada en este trabajo ofrece una visión detallada de las potenciales amenazas a la seguridad de las redes SDN de la institución educativa. Cada riesgo ha sido evaluado considerando dos dimensiones claves: probabilidad de ocurrencia y su impacto potencial. El factor de probabilidad se ha cuantificado en una escala del 1 al 5, donde 5 representa la mayor probabilidad de ocurrencia, mientras que el factor de impacto se ha evaluado en términos de las consecuencias que podría tener el riesgo sobre la institución, considerando aspectos como la disponibilidad de los servicios, la pérdida de información, daños a la reputación, y posibles sanciones legales. El

AJEA (Actas De Jornadas Y Eventos Académicos De UTN)
DOI: https://doi.org/10.33414/ajea.1776.2024

cálculo del producto de estos factores arroja el nivel de riesgo, proporcionando una medida cuantitativa de la gravedad de cada amenaza. La asignación de los valores se realizó a través de la lectura y clasificación de eventos de seguridad que ocurrieron en los últimos 15 años en la red de la UTN Facultad Regional San Francisco.

La relación entre la red, los casos de uso y la matriz de riesgos se centra en que la red proporciona el contexto para identificar los posibles puntos de ataque y vulnerabilidades, los casos de uso concretizan las amenazas y describen las secuencias de ataque más probables y la matriz de riesgos permite evaluar y priorizar los riesgos identificados en los casos de uso, facilitando la toma de decisiones en materia de seguridad. Al seguir este método, se logró obtener una visión clara y detallada de los riesgos a los que está expuesta la red de la facultad, lo que permitió diseñar e implementar medidas de seguridad efectivas para proteger los sistemas y datos de la institución.

Conclusión

El presente trabajo abordó de manera exhaustiva el análisis de riesgos en redes definidas por software (SDN) dentro de la infraestructura de la UTN - Facultad Regional San Francisco. A través de un método meticuloso que incluyó, la evaluación de amenazas y vulnerabilidades específicas, y el desarrollo de casos de uso detallados, se logró construir una matriz de riesgos que ofrece una visión cuantitativa y cualitativa de las amenazas a las que está expuesta la red SDN de la institución. El análisis ha destacado que, si bien SDN ofrece beneficios significativos en términos de flexibilidad, eficiencia y centralización en la gestión de redes, también introduce desafíos en materia de seguridad, particularmente en la capa de control. La centralización inherente de SDN, si no se protege adecuadamente, puede convertirse en un punto crítico de fallo que podría comprometer la totalidad de la red.

Asimismo, se ha evidenciado la importancia de adaptar y evolucionar las metodologías tradicionales de gestión de seguridad, como las propuestas por la norma ISO 27001, para enfrentar los retos específicos que presentan las redes SDN. La matriz de riesgos desarrollada no solo proporciona una herramienta valiosa para la toma de decisiones en materia de seguridad, sino que también subraya la necesidad de un monitoreo continuo y la actualización de las medidas de seguridad conforme emergen nuevas amenazas y vulnerabilidades.

Trabajos Futuros

Con la creciente adopción de SDN, también surge la necesidad de desarrollar métodos específicos de auditoría y cumplimiento normativo para estas redes. Un proyecto futuro podría centrarse en la creación de herramientas y metodologías para asegurar que las redes SDN cumplan con las normativas y estándares de seguridad internacionales.

Referencias

Alcívar Pedro, N. M. (2020). Comparativa entre red tradicional y red definida por software: Caso de estudio ESPAM MFL. Revista Iberica de Sistemas e Tecnologias de Informacao, 70-90.

Cheza, J. E. (2021). “Metodología de detección y mitigación de ataques ddos en entornos sdn basado en la norma iso/iec 27001 para mejorar la seguridad en el plano de control”. UNIVERSIDAD TÉCNICA DEL NORTE MAESTRÍA EN TELECOMUNICACIONES. Ibarra, Ecuador.

Correa Chica Juan Camilo, J. C. (2020). Seguridad en SDN: un estudio exhausti3vo. Revista de aplicaciones informáticas y de redes, 159, artículo 102595. https://doi.org/10.1016/j.jnca.2020.102595.

Cuesta, J. R. (2021). Seguridad en Redes definidas por software (SDN). Valencia: Escuela Técnica Superior de Ingeniería de Telecomunicación.

Fausto Camilo Vanegas Arévalo, R. D. (2023). PROPUESTA DE DISEÑO DE RED DE DATOS DEL COLEGIO POPULAR BOLIVARIANO. BOGOTÁ: UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS.

Fogelbach, R. -G.-G. (2015). Seguridad y Gestión del Riesgo en Redes Definidas por Software. Ciudadela Don Bosco, Soyapango: Universidad Don Bosco. Obtenido de https://rd.udb.edu.sv/items/cb1b7edc-0a48-4528-84aa-a5e292cb88d2

ISO.ORG. (2013). ISO.ORG. Obtenido de ISO.ORG: https://www.iso.org/obp/ui/?utm_source=google&utm_medium=ppc_paid_social&utm_campaign=am24-registration&gad_source=1&gclid=CjwKCAjw_ZC2BhAQEiwAXSgClhw1_c_nvMHNi4pfUtvneMbndFn9Aw8V-GFLhygBEmnuClHO7sePaBoCq80QAvD_BwE#iso:std:iso-iec:27001:ed-2:v1:en

Lawal, B. H. (2018). Real-Time Detection and Mitigation of Distributed Denial of Service (DDoS) Attacks in Software Defined Networking (SDN). 26 Signal Processing and Communications Applications Conference (SIU). 1–4.

Moreno, D. C. (2015). Atributos contextuales influyentes en el proceso de educción de requisitos: una exhaustiva revisión de literatura,. Ingeniare. Revista chilena de Ingeniería, 23(DOI 10.4067/S0718-33052015000200006), 208-218.

normaiso27001.es. (15 de 8 de 2024). ISO 27001. Obtenido de ISO 27001: https://www.normaiso27001.es/

Yibyth Tatiana Borda Ardila, W. G. (2023). Guía teórica-práctica sobre mejores prácticas de seguridad en los principales ataques DoS/DDoS en la capa de control de las redes definidas por Software (SDN) para medianas empresas. Bogotá: Universidad Distrital Francisco Jose De Caldas Facultad Tecnológica Ingeniería Telemática.