



UNIVERSIDAD POLITÉCNICA DE VICTORIA
INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

Estancia II

Empresa: Fiscalía General de Justicia del Estado de Tamaulipas

Proyecto: Proyecto de implementación de firewall

Asesor Empresarial: Lic. Víctor Luis Águila Morales

Asesor Institucional: M. S. I. José Fidencio López Luna

Alumno: Hermayonick Catalina hernandez Gonzalez

Enero, 2024

1 Resumen

Este documento detalla las acciones llevadas a cabo a lo largo de un período de cuatro semanas, desde el lunes 8 de enero hasta el viernes 2 de febrero de 2024, Durante el desarrollo del proyecto "Implementación de Firewall" en la Fiscalía General de Justicia del Estado de Tamaulipas, se llevaron a cabo diversas actividades con el propósito de fortalecer la seguridad en los equipos informáticos de la institución. Entre las acciones emprendidas, se destaca la formulación de políticas de restricción de aplicaciones, las cuales se aplicaron de manera diferenciada según los distintos niveles de acceso, con el objetivo de regular el uso específico de Internet. Se diseñaron políticas que limitan el acceso a ciertas páginas web.

Estas medidas fueron implementadas con el fin de salvaguardar la integridad y confidencialidad de la información, así como para asegurar un uso responsable y eficiente de los recursos informáticos dentro de la institución.

2 Abstract

This document details the actions taken over a four-week period, from Monday, January 8 to Friday, February 2, 2024, during the development of the "Firewall Implementation" project at the Attorney General's Office of the State of Tamaulipas, various activities were carried out with the purpose of strengthening the security of the institution's computer equipment. Among the actions undertaken, the formulation of application restriction policies stands out, which are applied in a differentiated manner according to the different levels of access, with the aim of regulating the specific use of the Internet. Policies are designed that limit access to certain web pages.

These were implemented in order to save the integrity and confidentiality of the information, as well as to ensure responsible and efficient use of computer resources within the institution. **Palabras claves:** Firewall, páginas web, Internet

Contents

| | | |
|----------|---|-----------|
| 1 | Resumen | 1 |
| 2 | Abstract | 1 |
| 3 | Introducción | 3 |
| 3.1 | Descripción de la empresa | 3 |
| 4 | Marco teórico | 4 |
| 4.1 | Fundamentos básico de redes | 4 |
| 4.1.1 | Cortafuegos o firewall | 4 |
| 4.1.2 | Protocolos de red | 4 |
| 4.1.3 | Modelo OSI | 5 |
| 4.1.4 | Modelo TCP/IP | 5 |
| 4.1.5 | Certificados SSL | 6 |
| 4.2 | Herramientas de Check Point (Check Point Software Technologies) | 6 |
| 4.2.1 | ¿Qué es GAIA? | 6 |
| 4.2.2 | Características de GAIA. | 7 |
| 4.2.3 | ¿Qué es SmartConsole? | 7 |
| 4.2.4 | Características de smartconsole | 7 |
| 5 | Justificación | 8 |
| 6 | Objetivos | 8 |
| 7 | Desarrollo del proyecto | 9 |
| 7.1 | Semana 1 | 9 |
| 7.2 | Semana 2 | 9 |
| 7.3 | Semana 3 | 11 |
| 7.4 | Semana 4 | 12 |
| 8 | Resultados | 14 |
| 9 | Conclusiones | 14 |

3 Introducción

Este proyecto se erige como un pilar estratégico destinado a preservar la integridad y confidencialidad de la información en el ámbito digital de la Fiscalía General de Justicia del Estado de Tamaulipas. Más allá de su enfoque primordial en la seguridad cibernética, la iniciativa también busca asegurar un empleo responsable y eficiente de los recursos informáticos dentro de la institución, destacando una atención particular hacia la gestión y restricción del acceso a Internet. La implementación de medidas concretas, como la formulación de políticas de bloqueo de aplicaciones y la estratificación de niveles diferenciados de acceso, se concibe con la finalidad de prevenir el uso indebido de los equipos y fomentar la ejecución exitosa de las actividades en consonancia con los rigurosos lineamientos establecidos. Este enfoque proactivo no sólo abona a la alineación con las normativas vigentes en materia de seguridad informática, sino que también propicia el establecimiento de un orden más eficaz en la administración de los recursos tecnológicos de la institución. La cuidadosa limitación del acceso a Internet, regida por criterios específicos para invitados, personal administrativo y líderes, evidencia la preocupación subyacente por maximizar la productividad, al mismo tiempo que se resguarda con celo la seguridad de la información sensible. En última instancia, este proyecto no solo se erige como un escudo protector ante potenciales amenazas cibernéticas, sino también como un impulsor de la eficiencia y la integridad en el entorno digital de la Fiscalía General de Justicia del Estado de Tamaulipas.

3.1 Descripción de la empresa

Nombre de la empresa: Fiscalía General de Justicia del Estado de Tamaulipas.

Tipo de empresa: Organismo público.

Misión: Somos una Fiscalía autónoma que garantiza el acceso a la justicia, el debido proceso, la verdad y la reparación del daño a las personas víctimas de delito, el respeto y protección a los derechos humanos mediante el profesionalismo y efectividad en la investigación criminal para fomentar confianza y seguridad en la ciudadanía.

Visión: Ser una institución reconocida por su profesionalismo, eficiencia en la procuración de justicia a través de personal comprometido, confiable, con sentido humano y de pertenencia, así como vocación de servicio a la ciudadanía mediante tecnología de vanguardia y recursos humanos especializados.

Objetivo: Las y los servidores públicos de la Fiscalía General tienen la obligación de velar, garantizar y promover el cumplimiento de los derechos humanos de las y los ciudadanos con perspectiva de género, independientemente de la calidad que tengan las personas intervinientes en el proceso penal [1].

Av. José Sulaimán Chagnón #641, entronque con Libramiento Naciones Unidas C.P. 87039, Ciudad Victoria, Tamaulipas, México Teléfono: 834 318 5118

4 Marco teórico

4.1 Fundamentos básico de redes

El constante avance de la tecnología ha impulsado la expansión y mejora de las infraestructuras de red, con el fin de satisfacer las necesidades de conexión cada vez más sofisticadas. El aumento en la cantidad de dispositivos conectados ha impulsado un desarrollo proporcional en la velocidad, alcance y capacidad de las redes, lo que ha permitido la creación de entornos de comunicación más eficientes y versátiles.

4.1.1 Cortafuegos o firewall

El cortafuego o firewall mejor conocido decide qué tipo de información puede entrar o salir. Permite que la información segura pase, como correos electrónicos legítimos, pero bloquea la información peligrosa, como virus o intentos de pirateo. En resumen, su objetivo principal es dejar pasar lo bueno y mantener fuera lo malo para mantener la red segura [2].

4.1.2 Protocolos de red

Es un estándar de comunicaciones. Contiene las reglas necesarias y la información sobre cómo las computadoras intercambian datos entre sí. Se requiere una interacción de diferentes tipos para diversas tareas, como, por ejemplo, el simple intercambio de mensajes.

Para lograr mantener esas conexiones con éxito deben especificarse una serie de propiedades:

- Detección de la conexión física y existencia de puntos finales o nodos.
- Negociación de varias características de la conexión.
- Inicialización y finalización de mensajes.
- Formateo de mensajes.
- Corrección de errores.
- Detección y tratamiento de posibles pérdidas de conexiones.
- Terminación de conexiones.

Existen una gran variedad de protocolos y estándares, como podrían ser los siguientes:

- **Modelo OSI:** modelo estándar y marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones.
- **Modelo TCP/IP:** el modelo más utilizado a nivel mundial, tanto en la comunicaciones a nivel global como local.
- **Certificados SSL:** es un certificado digital que autentica la identidad de un sitio web y habilita una conexión cifrada.
- **Segmento de red (subred):** Un segmento de red suele ser definido por el "hardware" o una dirección de red específica. Por ejemplo, en el entorno "Novell NetWare", en un segmento de red se incluyen todas las estaciones de trabajo conectadas a una tarjeta de interfaz de red de un servidor y cada segmento tiene su propia dirección de red.
- **Red de área locales (LAN):** Una LAN es un segmento de red que tiene conectadas estaciones de trabajo y servidores o un conjunto de segmentos de red interconectados, generalmente dentro de la misma zona. Por ejemplo un edificio.
- **Red de área extensa (WAN y redes globales):** Las WAN y redes globales se extienden sobrepasando las fronteras de las ciudades, pueblos o naciones. Los enlaces se realizan con instalaciones de telecomunicaciones públicas y privadas, además por microondas y satélites.

4.1.3 Modelo OSI

El modelo OSI, creado por la Organización Internacional para la Estandarización, es un marco conceptual que permite la conexión de diferentes sistemas de comunicación mediante el uso de protocolos estándar. En resumen, el OSI establece un estándar para que diversos sistemas de equipos puedan comunicarse entre sí [3].

Este modelo puede considerarse como un lenguaje universal para la conexión de redes de equipos. Se fundamenta en la idea de dividir un sistema de comunicación en siete capas abstractas, apiladas una sobre la otra, como se ilustra en la figura 1.

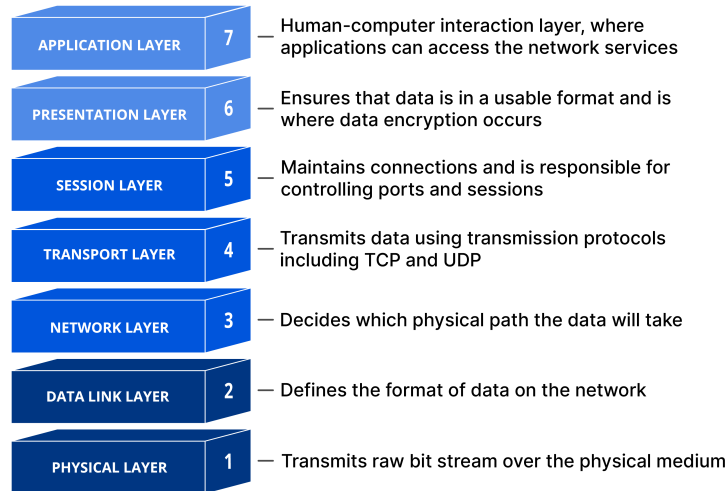


Figure 1: El modelo OSI y sus 7 capas.

Cada capa del modelo OSI cumple una función específica y se comunica con las capas superiores e inferiores. Los ataques DDoS están dirigidos a capas específicas de una conexión de red; los ataques a la capa de aplicación se enfocan en la capa 7, mientras que los ataques a la capa de protocolo se dirigen a las capas 3 y 4.

4.1.4 Modelo TCP/IP

Los protocolos son reglas que permiten a las máquinas y programas intercambiar información. Cada máquina debe seguir estas reglas para que el sistema receptor pueda entender el mensaje. El conjunto de protocolos TCP/IP se puede entender en términos de capas o niveles. [4].

La figura 2 representa las capas del protocolo TCP/IP, las cuales son: capa de aplicación, capa de transporte, capa de red, capa de interfaz de red y hardware, en ese orden de arriba hacia abajo.

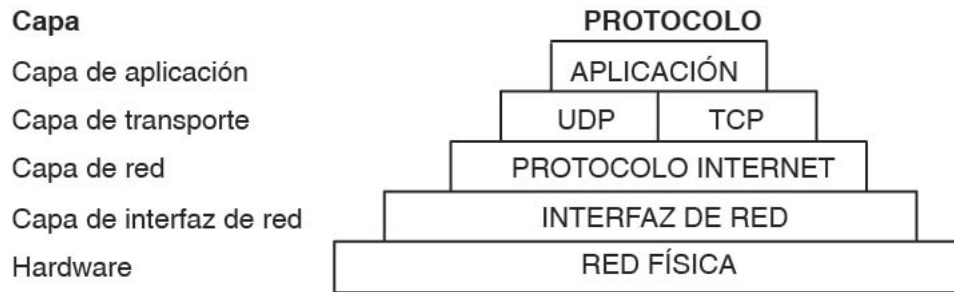


Figure 2: Protocolos TCP/IP.

4.1.5 Certificados SSL

Un certificado digital autentica la identidad de un sitio web y permite una conexión cifrada. SSL significa Secure Sockets Layer, un protocolo de seguridad que crea un enlace cifrado entre un servidor web y un navegador web. Estos certificados garantizan que los datos transferidos entre usuarios y sitios web sean imposibles de leer. Utilizan algoritmos de cifrado para proteger la información confidencial, como nombres, direcciones y números de tarjetas de crédito [5].

4.2 Herramientas de Check Point (Check Point Software Technologies)

Es un líder proveedor de soluciones en el ámbito de seguridad cibernética para empresas y para grandes empresas a nivel mundial. Las soluciones que ofrecen para proteger a sus clientes de ciberataques de 5ª generación como puede ser el malware, ransomware entre otros ataques peligrosos. Check Point ofrece una gran arquitectura de seguridad multinivel, "Infinity Total Protection" con prevención avanzada de amenazas de 5ª generación, que defiende la información de los usuarios en la nube, la red y los dispositivos móviles de las empresas. Check Point proporciona el sistema de gestión de seguridad de un punto de control más completo e intuitivo. [6].

4.2.1 ¿Qué es GAIA?

Es un sistema operativo de la próxima generación de Check Point para aplicaciones de seguridad, Gaia en griego significa *la madre de todos* que representa partes estrechamente integradas para formar un sistema eficiente. El sistema operativo Gaia es compatible con la cartera completa de productos Blades, Gateway y Security Management de Check Point Software [7].

Gaia es un sistema operativo de seguridad unificado que combina lo mejor de los sistemas operativos originales de Check Point e IPSO, el sistema operativo de los productos de seguridad de dispositivos. Gaia está disponible para todos los dispositivos de seguridad y servidores abiertos de Check Point.

Diseñado desde cero para implementaciones modernas de alto nivel, Gaia incluye soporte para:

- IPv4 e IPv6 .
- Alta capacidad de conexión y sistemas virtuales.
- Carga compartida.
- Alta disponibilidad.
- Enrutamiento dinámico y de multidifusión.
- Interfaz de línea de comandos fácil de usar.
- Administración basada en roles.

4.2.2 Características de GAIA.

- Obtenga actualizaciones de Check Point con licencia directamente a través del sistema operativo .
- Descargue e instale las actualizaciones más rápidamente. Descargue de forma automática, manual o periódica. Instalaciones manuales o periódicamente.
- Reciba notificaciones por correo electrónico sobre actualizaciones recientemente disponibles y sobre descargas e instalaciones.
- Fácil reversión desde una nueva actualización.

4.2.3 ¿Qué es SmartConsole?

SmartConsole es una GUI para la gestión y administración de las políticas de seguridad, gestión de dispositivos, gestión de registros y eventos. SmartConsole facilita la administración de redes complejas y tiene una amplia selección de protocolos y aplicaciones para las políticas de seguridad que integre el usuario.

Estos objetos se utilizan en SmartConsole para muchas tareas, incluida la creación de Políticas de seguridad. También se usa para monitorizar el tráfico a través de registros y administrar Software Blades, licencias y actualizaciones [8].

4.2.4 Características de smartconsole

- Detección de amenazas de manera inmediata.
- Operaciones eficientes de seguridad.
- Administración escalable según la demanda.

5 Justificación

En la actualidad, los avances tecnológicos suceden a un ritmo vertiginoso, transformando la forma en que llevamos a cabo nuestras tareas diarias en el ámbito laboral. En este contexto, se vuelve esencial abordar la cuestión de la seguridad informática, no solo como una medida preventiva ante posibles amenazas cibernéticas, sino también como un componente crucial para asegurar la privacidad y la concentración de los empleados en sus responsabilidades laborales.

La implementación de medidas de seguridad, particularmente en el acceso a Internet, se justifica por la necesidad de salvaguardar la integridad de la información sensible de la empresa y protegerla contra posibles vulnerabilidades. Además, el control y restricción del acceso a ciertas páginas web se convierte en una herramienta estratégica para garantizar que los empleados se concentren en sus tareas laborales, evitando distracciones innecesarias.

Cuando no se establecen políticas de seguridad en el acceso a Internet, es común observar que los empleados tienden a acceder a diversas redes sociales y otras plataformas no relacionadas con su trabajo, lo que puede resultar en una disminución de la productividad y en una desviación de los objetivos laborales establecidos.

En este sentido, la implementación de un sistema de seguridad informática efectivo no solo protege la empresa contra amenazas externas, sino que también contribuye a fomentar un entorno laboral enfocado, donde los empleados pueden desempeñar sus funciones con mayor eficiencia y concentración. Así, la inversión en seguridad no solo se traduce en la protección de la información sensible, sino también en la promoción de un ambiente laboral más productivo y centrado en los objetivos institucionales.

6 Objetivos

El objetivo primordial de este proyecto radica en el fortalecimiento de la seguridad para la administración y control de la navegación por Internet destinada tanto a los empleados como a los visitantes en la Fiscalía General de Justicia del Estado de Tamaulipas. La implementación de un sistema de seguridad informática efectivo no solo se orienta a resguardar a la institución contra posibles amenazas externas, sino que también busca proactivamente fomentar un entorno laboral más enfocado y eficiente. Al restringir el acceso no autorizado a ciertos contenidos en línea, se pretende mitigar distracciones innecesarias que podrían afectar la productividad y concentración de los empleados durante sus labores diarias. Como por ejemplo:

- Páginas de dudosa procedencia.
- Páginas que no cumplan con los certificados de seguridad.
- Páginas de entretenimiento y/o redes sociales, etc.

7 Desarrollo del proyecto

La ejecución de este proyecto se extendió a lo largo de un periodo de cuatro semanas, durante el cual nos embarcamos en una serie de actividades estratégicas diseñadas para alcanzar con éxito nuestros objetivos predefinidos. A lo largo de este lapso temporal, hicimos uso de una variedad de recursos, siendo destacados entre ellos el sistema operativo GAIA y la plataforma SmartConsole. Es fundamental resaltar que estas actividades abarcaron desde la fase inicial de familiarización con el sistema hasta la etapa avanzada de creación e implementación de políticas de seguridad.

Las tareas emprendidas durante este periodo demostraron ser sumamente eficaces, generando beneficios tangibles tanto para la empresa como para nuestro propio crecimiento en el ámbito de la ciberseguridad. Esta fase intensiva de actividad no solo permitió una comprensión profunda del sistema operativo GAIA y las herramientas asociadas, sino que también facilitó la formulación y aplicación de políticas de seguridad que se alinean con las mejores prácticas en el campo de la seguridad informática.

A través de un enfoque meticuloso y una dedicación constante, pudimos explorar a fondo las capacidades y funcionalidades del sistema operativo GAIA, lo que se tradujo en un dominio más completo de sus características. La plataforma SmartConsole, por su parte, se convirtió en una herramienta integral para la gestión y monitorización, ampliando nuestras capacidades en la implementación de políticas de seguridad de manera efectiva.

Este periodo de actividad intensiva no solo se tradujo en logros prácticos y soluciones concretas para la empresa, sino que también contribuyó significativamente a nuestro bagaje de conocimientos en el campo de la ciberseguridad. La combinación de la teoría y la aplicación práctica durante estas cuatro semanas enriqueció nuestra comprensión global y nos proporcionó una base sólida para abordar futuros desafíos en el ámbito de la seguridad informática.

7.1 Semana 1

El desarrollo del proyecto se inició a través de una exhaustiva serie de investigaciones en colaboración con mi compañero, Alan Isai Torres Desilos, con el propósito fundamental de comprender de manera adecuada el uso de los sistemas proporcionados. En las etapas iniciales, nos encontrábamos ante la falta de conocimiento sustancial sobre dichos sistemas, lo que motivó la necesidad de realizar un análisis detallado.

La primera fase de nuestra investigación se centró en un examen minucioso de las aplicaciones disponibles, abordando aspectos cruciales como su definición, utilidad, funcionamiento y su aplicabilidad en la implementación de políticas de firewall. Esta fase inicial resultó esencial para establecer una base sólida y comprender el contexto en el cual íbamos a trabajar.

Posteriormente, se facilitaron equipos de cómputo y procedimos a la descarga de los sistemas operativos pertinentes. Esta acción nos brindó la oportunidad de llevar a cabo una exploración más profunda de los sistemas, permitiéndonos familiarizarnos con sus características intrínsecas. La combinación de la investigación teórica, que nos proporcionó un marco conceptual sólido, y la exploración práctica de los sistemas, que nos sumergió directamente en su funcionamiento, contribuyó de manera integral a nuestro conocimiento.

La sinergia entre la investigación teórica y la experiencia práctica no solo fortaleció nuestra comprensión de las tecnologías específicas involucradas en el proyecto de seguridad informática, sino que también nos permitió adquirir una perspectiva más holística y contextualizada. Este enfoque integral resultó esencial para abordar los desafíos que surgieron durante la implementación del proyecto y asegurar que nuestras decisiones estuvieran fundamentadas en un conocimiento profundo y diversificado. En última instancia, la combinación de estos enfoques enriqueció significativamente nuestra capacidad para diseñar e implementar soluciones efectivas en el ámbito de la seguridad informática.

7.2 Semana 2

Una vez que nos familiarizamos a fondo con las herramientas disponibles, nos embarcamos en la fase de aplicación de políticas de prueba, marcando un hito significativo en el desarrollo del proyecto. En esta etapa, nos centramos en la restricción de acceso a determinadas páginas web prominentes, incluyendo pero no

limitándonos a youtube.com, facebook.com e instagram.com. El propósito subyacente de estas restricciones fue evaluar la efectividad de nuestras políticas de seguridad y verificar su capacidad para mitigar el acceso no autorizado a sitios web específicos.

Sin embargo, para llevar a cabo una evaluación exhaustiva de la operatividad de nuestras políticas, adoptamos un enfoque práctico al conectar directamente uno de nuestros dispositivos al firewall. Esta acción se llevó a cabo con la intención de demostrar de manera tangible que las políticas implementadas estaban operando de acuerdo con nuestras expectativas previas. La conexión directa al firewall proporcionó una visión detallada de cómo las restricciones afectaban el acceso a los sitios web designados, permitiéndonos validar la eficacia de nuestras configuraciones de seguridad.

Antes de implementar las políticas en sí, realizamos una fase crítica de preparación. Esto implicó habilitar el acceso a Internet y configurar el firewall en la computadora designada para nuestras pruebas. Este paso inicial fue esencial para establecer las condiciones necesarias que nos permitieron llevar a cabo las pruebas que validaron la funcionalidad efectiva de las políticas de seguridad que estábamos a punto de implementar.

La cuidadosa planificación y ejecución de estas fases aseguraron no solo la implementación adecuada de las políticas de seguridad, sino también la capacidad de realizar pruebas rigurosas que respaldaran la eficacia de las medidas adoptadas. Este enfoque metódico y detallado refleja nuestro compromiso con la calidad y la precisión en la implementación de soluciones de seguridad informática 3.

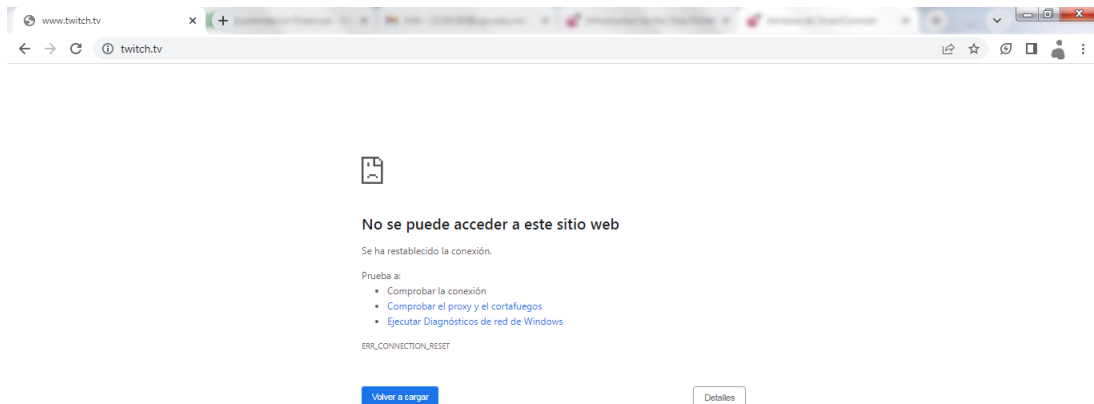


Figure 3: Pagina de twitch.tv bloquea por politicas.

Con las políticas de prueba en pleno funcionamiento, nos embarcamos en la tarea de confeccionar un diagrama de red que ilustrara la configuración de la infraestructura en la empresa. Para llevar a cabo esta tarea, recurrimos a la información proporcionada por la plataforma GAIA, que detalla el uso de puertos y su asociación con redes específicas. Esta información crítica nos permitió elaborar un esbozo preliminar del diagrama de red, reflejando con precisión la disposición y las interconexiones de los diferentes componentes en la red empresarial. Como se muestra en la figura 4

Este esfuerzo no solo contribuyó a nuestra comprensión visual de la red, sino que también sirvió como herramienta de comunicación efectiva. El diagrama de red se convirtió en un recurso fundamental para compartir información sobre la estructura de la red con otros miembros del equipo y partes interesadas en el proyecto. Facilitó la explicación de la configuración de seguridad implementada y proporcionó una visión clara de cómo las políticas de prueba afectaban la dinámica general de la red.

Además, el proceso de elaboración del diagrama de red nos permitió identificar posibles áreas de mejora en la

configuración de la red, lo que resultó valioso para la optimización continua de la seguridad y el rendimiento. Este enfoque holístico en la visualización y comprensión de la infraestructura de red resalta nuestra dedicación no solo a la implementación efectiva de políticas de seguridad, sino también a la mejora constante y a la alineación con las mejores prácticas en la gestión de redes empresariales.

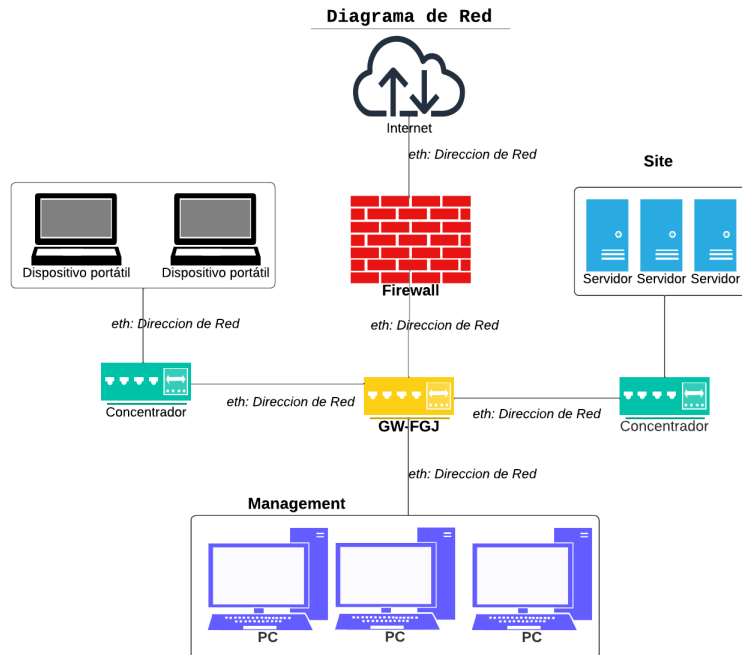


Figure 4: Borrador de diagrama de red de la empresa.

7.3 Semana 3

EDurante esta semana, profundizamos en el conocimiento de la infraestructura de red existente, dando paso a la identificación y activación de redes locales y externas presentes en la empresa, las cuales brindaban servicios fundamentales. Esta fase de descubrimiento permitió obtener una visión más completa y detallada del entorno de red. Con la información recién adquirida, pudimos actualizar de manera exhaustiva y finalizar nuestro diagrama de red. Este proceso incluyó una revisión y ajuste de los elementos previamente identificados, así como la incorporación de las nuevas redes identificadas durante esta fase de exploración. Esta semana de exploración y actualización del diagrama de red no sólo proporcionó una representación más precisa de la topología de la red, sino que también facilitó una comprensión más profunda de cómo las diversas redes interactúan entre sí, contribuyendo así a una implementación más eficaz y segura de las políticas de seguridad. Se muestra en la figura como quedó el diagrama final de la red. Como se ver la figura [5](#)

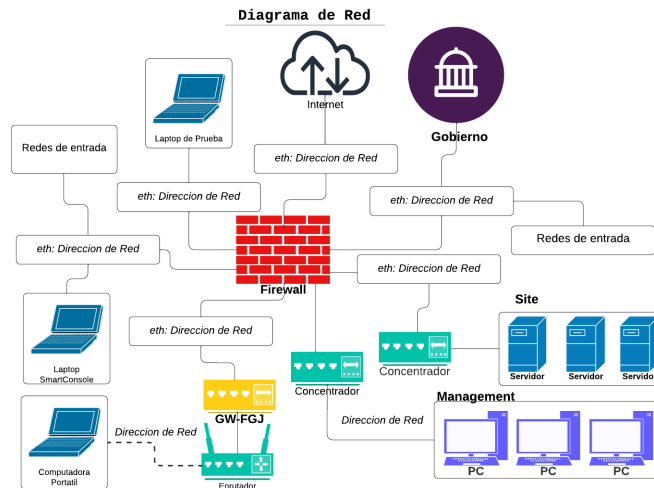


Figure 5: Diagrama de red de la empresa actualizado.

SDe manera adicional, llevamos a cabo la creación de grupos de redes sociales y páginas web específicas que se tenían la intención de bloquear. Este proceso tenía como propósito facilitar la identificación y reconocimiento visual de las páginas que serían restringidas mediante la implementación de las políticas de seguridad. La creación de estos grupos permitió una mejor organización y categorización de las páginas que se buscaba bloquear, proporcionando una visión clara y estructurada de las restricciones planificadas.

| No. | IPto | Nombre | Source | Destination | VPN | Services & Applications | Action | Tools |
|-----|--------------|-----------------------------|--------------------|-------------|-----|-------------------------|--------|--------------|
| 1 | 24 (Low) | Entertainment | ↔ Dirección de red | ↔ Internet | Any | Streaming | Drop | Log, Account |
| 2 | 111 (Low) | Redes sociales | ↔ Dirección de red | ↔ Internet | Any | Redes sociales | Drop | Log, Account |
| 3 | 136 (Medium) | Net | ↔ Dirección de red | ↔ Internet | Any | File Services | Accept | Log, Account |
| 4 | 88 (Low) | Gubernamental & Noticias | ↔ Dirección de red | ↔ Internet | Any | Gobierno & Noticias | Accept | Log, Account |
| 5 | 1136 (High) | Cleanup rule internetAccess | Any | Any | Any | Any | Accept | Log, Account |

Figure 6: Políticas aplicadas en SmartConsole.

La detección de los grupos a los cuales se asignaron las restricciones de acceso a páginas web o páginas especiales fue un aspecto fundamental, ya que estábamos en proceso de crear grupos según las necesidades específicas de cada segmento de usuarios. Se establecieron diferentes grupos con políticas de acceso diferenciadas en función de las responsabilidades y roles dentro de la organización. La importancia de la creación de estos grupos radica en la necesidad de adaptar las políticas de seguridad a los requisitos particulares de cada tipo de usuario. Posteriormente, llevamos a cabo pruebas exhaustivas para verificar la efectividad de las restricciones implementadas.

7.4 Semana 4

Durante el transcurso de esta semana, nos sumergimos en la fase crítica de implementación de las políticas que previamente habíamos definido, así como en la configuración de los grupos ya establecidos. Este proceso

no solo implicó la aplicación teórica de restricciones de acceso, sino también la personalización de estas restricciones según las especificaciones detalladas para cada grupo de usuarios. Nuestra meta principal era asegurar una implementación coherente de las políticas de seguridad, alineada de manera precisa con las necesidades y responsabilidades específicas asignadas a cada grupo dentro de la organización.

Durante estas pruebas, adoptamos un enfoque riguroso al enfrentar diferentes situaciones simuladas, evaluando la capacidad de las aplicaciones para superar los filtros establecidos. Si una aplicación lograba superar estos filtros, procedíamos a su denegación, asegurando así que incluso en situaciones desafiantes, las políticas de seguridad se mantuvieran efectivas y en pleno funcionamiento. Por otro lado, si una aplicación no lograba superar los filtros, confirmábamos la eficacia de las políticas vigentes y su capacidad para cumplir con los objetivos de seguridad establecidos.

Este proceso minucioso y las pruebas exhaustivas nos permitieron implementar con éxito el bloqueo de aplicaciones, garantizando un cierre efectivo y reforzando la seguridad del entorno informático de la empresa. Estos esfuerzos no solo se traducen en la mitigación de riesgos potenciales, sino que también reflejan nuestro compromiso continuo con la adaptabilidad y la mejora constante en el ámbito de la seguridad informática.

| Action | Source | Destination | Service | Application Name | Primary Category |
|--------|------------------|-------------|------------|------------------|------------------|
| Accept | Dirección de red | Internet | HTTP/HTTPS | | |
| Accept | Dirección de red | Internet | HTTP/HTTPS | | |
| Accept | Dirección de red | Internet | HTTP/HTTPS | | |
| Accept | Dirección de red | Internet | HTTP/HTTPS | | |
| Accept | Dirección de red | Internet | HTTP/HTTPS | | |
| Reject | Dirección de red | Internet | HTTP/HTTPS | Twitch.tv | Media Streams |
| Accept | Dirección de red | Internet | HTTP/HTTPS | | |
| Accept | Dirección de red | Internet | HTTP/HTTPS | | |
| Accept | Dirección de red | Internet | HTTP/HTTPS | | |
| Accept | Dirección de red | Internet | HTTP/HTTPS | | |
| Accept | Dirección de red | Internet | HTTP/HTTPS | | |
| Accept | Dirección de red | Internet | HTTP/HTTPS | | |

Figure 7: Archivo log del trafico.

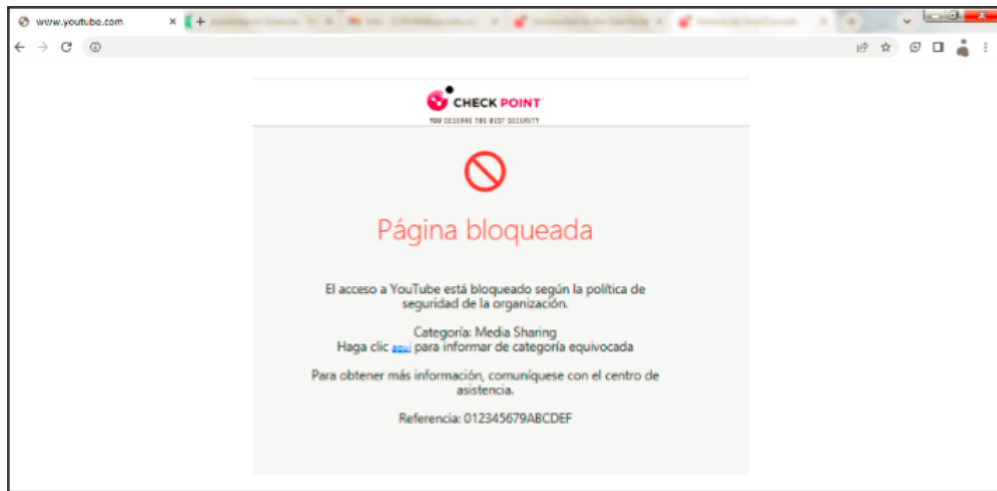
| B. | Action | Source | Destination | Service | Application Name | Primary Category |
|----|--------|------------------|-------------|------------|------------------|------------------|
| | Accept | Dirección de red | Internet | HTTP/HTTPS | | |
| | Accept | Dirección de red | Internet | HTTP/HTTPS | | |
| | Accept | Dirección de red | Internet | HTTP/HTTPS | | |
| | Accept | Dirección de red | Internet | HTTP/HTTPS | | |
| | Accept | Dirección de red | Internet | HTTP/HTTPS | | |
| | Reject | Dirección de red | Internet | HTTP/HTTPS | YouTube | Media Streams |
| | Reject | Dirección de red | Internet | HTTP/HTTPS | | |
| | Accept | Dirección de red | Internet | HTTP/HTTPS | | |
| | Accept | Dirección de red | Internet | HTTP/HTTPS | | |
| | Accept | Dirección de red | Internet | HTTP/HTTPS | | |
| | Accept | Dirección de red | Internet | HTTP/HTTPS | | |
| | Accept | Dirección de red | Internet | HTTP/HTTPS | | |
| | Accept | Dirección de red | Internet | HTTP/HTTPS | | |

Figure 8: Archivo log del trafico.

8 Resultados

A lo largo de este periodo de desarrollo, es con gran satisfacción que informo que los resultados obtenidos en cada actividad han sido consistentemente positivos, generando impactos beneficiosos tanto para la empresa como para mí misma. Dentro del marco de los resultados del proyecto, hemos alcanzado un éxito significativo al lograr el bloqueo efectivo de diversas páginas web. Este logro se ha concretado mediante la implementación de estrategias cuidadosamente diseñadas, las cuales se centran en la identificación y restricción de grupos específicos de páginas o aplicaciones previamente identificadas como bloqueadas.

El bloqueo efectivo de estas páginas no solo representa un hito importante en términos de cumplimiento de objetivos, sino que también subraya la eficacia de las políticas de seguridad implementadas. Estas estrategias han demostrado ser fundamentales para la protección de la infraestructura digital de la empresa, contribuyendo de manera activa a la mitigación de riesgos asociados con el acceso no autorizado a contenido no deseado.



9 Conclusiones

La ejecución de este proyecto representó una experiencia novedosa para mí, dado que nos embarcamos en la realización del mismo utilizando aplicaciones para las cuales no contábamos con conocimiento previo. A lo largo de este proceso, fuimos adquiriendo conocimientos de manera progresiva, aprendiendo de manera continua durante la utilización y la investigación.

Este enfoque de aprendizaje activo resultó fundamental para comprender las complejidades inherentes a las aplicaciones en cuestión y nos permitió adaptarnos de manera efectiva a los desafíos que surgieron durante el desarrollo del proyecto. La disposición para explorar nuevas tecnologías y adquirir habilidades sobre la marcha ha sido una parte integral de nuestra metodología de trabajo, y los conocimientos adquiridos durante esta experiencia sin duda enriquecerán nuestras capacidades profesionales a medida que avanzamos en futuros proyectos.

Los conocimientos adquiridos durante esta experiencia no solo han sido valiosos para el proyecto en cuestión, sino que también han enriquecido nuestras capacidades profesionales de cara a futuros desafíos. Esta experiencia nos ha permitido desarrollar una mentalidad de crecimiento, fortaleciendo nuestra capacidad de enfrentar nuevas situaciones con confianza y adaptabilidad. Estoy seguro de que los aprendizajes obtenidos durante este proyecto seguirán siendo de gran utilidad a medida que avancemos en futuros proyectos y desafíos profesionales.

Bibliografía

- [1] *Fiscalía General de Justicia del Estado de Tamaulipas — Fiscalía General de Justicia del Estado de Tamaulipas*. <https://www.fgjtam.gob.mx/conocenos/>. Consultado el 29 01 2024.
- [2] *¿Qué es un firewall? Los diferentes tipos de firewall - Check Point Software*. <https://www.checkpoint.com/es/cyber-hub/network-security/what-is-firewall/>. Consultado el 30 01 2024.
- [3] *¿Qué es el modelo OSI?— Ejemplos de modelos OSI — Cloudflare*. <https://www.cloudflare.com/es-es/learning/ddos/glossary/open-systems-interconnection-model-osi/>. Consultado el 30 01 2024.
- [4] *Protocolos TCP/IP - Documentación de IBM*. <https://www.ibm.com/docs/es/aix/7.2?topic=protocol-tcpip-protocols>. Consultado el 30 01 2024.
- [5] *¿Qué es un certificado SSL y por qué es importante?* <https://latam.kaspersky.com/resource-center/definitions/what-is-a-ssl-certificate>. Consultado el 30 01 2024.
- [6] *Descripción general de la empresa Check Point - Check Point Software*. <https://www-app.checkpoint.com/es/about-us/company-overview/>. Consultado el 29 01 2024.
- [7] *Descripción general de Gaia*. https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Gaia_AdminGuide/Topics-GAG/Gaia-Overview.htm. Consultado el 29 01 2024.
- [8] 28046 Madrid P^o de la Castellana 109. “Guía de Seguridad de las TIC CCN-STIC 653 - Seguridad en Check Point”. In: *Catálogo de Publicaciones de la Administración General del Estado* <https://cpage.mpr.gob.es> (2023).



Ciudad Victoria,
Tamaulipas, a
**20 de
Diciembre de
2023**

FISCALÍA GENERAL DE JUSTICIA DEL ESTADO DE TAMAULIPAS
LIC. VÍCTOR LUIS AGUILAR MORALES
PRESENTE



La Universidad Politécnica de Victoria tiene a bien presentar a **HERNANDEZ GONZALEZ HERMAYONICK CATALINA** estudiante del programa académico de **INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN**, con número de matrícula **2130036** y seguro facultativo IMSS número **44180365841**; quién deberá realizar su práctica profesional de **ESTANCIA II**, a partir del **08 de Enero de 2024** al **02 de Febrero de 2024**, con duración de **200 horas** desarrollando el proyecto "**Proyecto de implementación firewall**" que le fué asignado.

Al concluir se le extenderá la carta de liberación al evaluarlo satisfactoriamente.

El practicante deberá cumplir con el Reglamento Interno aplicable al personal en su centro de trabajo.

Sin otro particular.

ATENTAMENTE

M. A. OTHÓN CANO GARZA
DIRECTOR DE VINCULACIÓN

C.C.P. ----
ASESOR EMPRESARIAL



UNIVERSIDAD POLITÉCNICA DE VICTORIA

Av. Nuevas Tecnologías 5902
Parque Científico y Tecnológico de Tamaulipas
Carretera Victoria Soto La Marina Km. 5.5
Cd. Victoria, Tamaulipas. C.P. 87138

Tel: (834) 1711100 al 10
www.upvictoria.edu.mx



Tamaulipas
1901-2000



FGJ
FISCALÍA GENERAL DE
JUSTICIA DEL ESTADO
DE TAMAULIPAS

"2024, Año de Felipe Carrillo Puerto, Benemérito del
Proletariado, Revolucionario y Defensor del Mayab"

Ciudad Victoria, Tamaulipas; a 08 de enero de 2024

Asunto: Carta de Aceptación

M. A. OTHÓN CANO GARZA
Director de Vinculación
P R E S E N T E . -

Por medio del presente, me permito informar que la C. HERNÁNDEZ GONZÁLEZ HERMAYONICK CATALINA alumna del séptimo semestre de la Ingeniería en Tecnologías de la Información, con número de matrícula 2130036, es Aceptada para realizar sus Prácticas Profesionales de Estancia II en la Dirección General de Tecnología, Información y Telecomunicaciones de esta Fiscalía General de Justicia del Estado.

Las cuales deberá cubrir en un plazo no menor de un mes, cubriendo un total de 200 horas de lunes a viernes de 09:00 a 15:00 horas, activándose a partir de la fecha aceptada en base al Registro del Control de Asistencia.

Sin más por el momento, aprovecho la ocasión para enviarle un cordial saludo.

Atentamente
LA DIRECTORA DE RECURSOS HUMANOS



C.P. MAYRA ELIZABETH MORA MARTÍNEZ

Toda persona que por algún motivo tenga conocimiento del contenido del presente y en su caso de sus anexos, deberá abstenerse de difundirlo por cualquier medio y adoptar las medidas necesarias para evitar su publicidad.
Fundamento: artículo 9 fracción VII de la Ley Orgánica de la Fiscalía General de Justicia del Estado de Tamaulipas, 2 fracción XIII de su Reglamento, 117 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tamaulipas, y demás relativos y aplicables.

C.C.P.- Lic. Leobardo Catalán Torres.- Director General de Administración de la Fiscalía General de Justicia del Estado de Tamaulipas.
C.C.P.- Lic. Asis Alejandra Sifuentes Fuentes.- Directora de Vinculación y Enlace
C.C.P.- Archivo
C.C.P.- Expediente

SRF/LEGC



FGJ

FISCALÍA GENERAL DE
JUSTICIA DEL ESTADO
DE TAMAULIPAS

Ciudad Victoria, Tamaulipas; a 06 de febrero de 2024

Asunto: Carta de Liberación

M. A. OTHÓN CANO GARZA

Director de Vinculación

PRESENTE. -

Por medio del presente, me permito informar que la C. HERNÁNDEZ GONZÁLEZ HERMAYONICK CATALINA alumna de la Carrera de la Ingeniería en Tecnologías de la Información, con número de matrícula 2130036, ha concluido SATISFACTORIAMENTE sus Prácticas Profesionales de Estancia II en la Dirección General de Tecnología, Información y Telecomunicaciones, de esta Fiscalía General de Justicia del Estado.

Las cuales cubrieron un total de 200 horas en un tiempo no menor de un mes, asistiendo de lunes a viernes con horario de 09:00 a 15:00 horas, comprendido en el período del 08 de enero del 2024 al 02 de febrero del 2024.

Sin más por el momento, me es grato enviarle un cordial saludo.

Atentamente

LA DIRECTORA DE RECURSOS HUMANOS



FISCALÍA GENERAL DE
JUSTICIA DEL ESTADO
DE TAMAULIPAS

C.P. MAYRA ELIZABETH MORA MARTÍNEZ

Toda persona que por algún motivo tenga conocimiento del contenido del presente y en su caso de sus anexos, deberá abstenerse de difundirlo por cualquier medio y adoptar las medidas necesarias para evitar su publicidad.

Fundamento: artículo 9 fracción VII de la Ley Orgánica de la Fiscalía General de Justicia del Estado de Tamaulipas, 2 fracción XIII de su Reglamento, 117 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tamaulipas, y demás relativos y aplicables.

C.C.P.- Lic. Leobardo Catalán Torres.-Director General de Administración de la Fiscalía General de Justicia del Estado de Tamaulipas.

C.C.P.- Lic. Asís Alejandra Sifuentes Fuentes.- Directora de Vinculación y Enlace

C.C.P.- Archivo

C.C.P.- Expediente

SBR/LEG



EVALUACIÓN POR EL ASESOR EMPRESARIAL

LISTA DE COTEJO

DATOS GENERALES DEL PROCESO DE EVALUACIÓN

| | | | | | | | |
|-------------------|---|-----|-----|-----|---|----------------------------------|--|
| NOMBRE ALUMNO: | Hermayonick Catalina Hernandez Gonzalez | | | | NOMBRE DEL ASESOR EMPRESARIAL: | LIC. Victor Luis Aguilar Morales | |
| MATRICULA: | PROGRAMA ACADÉMICO | | | | NOMBRE DE LA EMPRESA: | | |
| 2130036 | ITI | MEC | ISA | ITM | Fiscalia General De Justicia Del Estado De Tamaulipas | | |
| FIRMA DEL ALUMNO: | | | | | FIRMA DEL ASESOR EMPRESARIAL: | | |

INSTRUCCIONES

En la columna de valor se encuentran sombreados los reactivos esenciales de su calificación. Revisar las actividades que se solicitan y marque en los apartados el porcentaje y la ponderación (en relación al porcentaje del valor) de cada reactivo. En la columna "OBSERVACIONES" mencione indicaciones que puedan ayudar al alumno a saber cuales son las condiciones no cumplidas, si fuese necesario.

| VALOR | Característica a cumplir (Reactivo) | Porcentaje | Ponderación | OBSERVACIONES |
|---------------------------------------|--|------------|-------------|---------------|
| 10 | Conocimiento de su área | 10% | 10 | |
| 10 | Iniciativa | 10% | 10 | |
| 10 | Uso adecuado de instalaciones | 10% | 10 | |
| 10 | Respeto a los lineamientos de seguridad e higiene | 10% | 10 | |
| 10 | Puntualidad y asistencia | 10% | 10 | |
| 10 | Responsabilidad durante el desarrollo de las actividades | 10% | 10 | |
| 10 | Participación y cooperación | 10% | 10 | |
| 10 | Trabajo en equipo | 10% | 10 | |
| 10 | Disposición al trabajo | 10% | 10 | |
| 10 | Expresión oral y escrita | 10% | 10 | |
| CALIFICACIÓN: | | 100% | 100 | |
| Recomendaciones o aspectos a mejorar: | | | | |
| | | | | |
| | | | | |
| | | | | |

BITACORA DE LA ESTANCIA

08-12 Enero 2024

ACTIVIDADES REALIZADAS:

Conociendo el programa asignado (CheckPoint SmartConsole)

Investigación y conocimiento de la pagina (Gaia)

Investigación de como implementar politicas al firewall

Investigación de como implementar politicas para el internet

Investigación de certificado SSL y como se implementa

Investigación de como optimizar procesos en las politicas

Explicación y conocimiento de trabajo a realizar

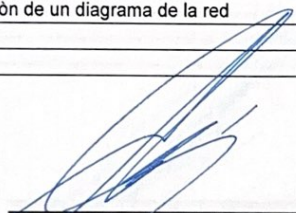
ACTIVIDADES PENDIENTES:

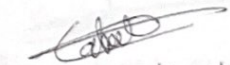
Implementación de politicas en el firewall

Pruebas del funcionamiento de politicas

Conocimiento de la red (LAN)

Realización de un diagrama de la red


FIRMA DEL ASESOR EMPRESARIAL


FIRMA DEL ALUMNO



BITACORA DE LA ESTANCIA


15-19 Enero 2024

ACTIVIDADES REALIZADAS:

Implementacion de politicas de firewall
Pruebas del funcionamiento de politicas
Borrador de un diagrama de la red
Pruebas en un equipo informático
Dar acceso a internet a un equipo informatico para pruebas

ACTIVIDADES PENDIENTES:

Conocimiento de la red (LAN)
Realización de un diagrama de la red


FIRMA DEL ASESOR EMPRESARIAL


Hermayrick Caballero Hdez Cde
FIRMA DEL ALUMNO



BITACORA DE LA ESTANCIA

22-26 Enero 2024

ACTIVIDADES REALIZADAS:

Conocimiento de la red (LAN)

Realización de un diagrama de la red

Activación de nuevas redes locales al sistema (Gaia)

Servicios conjuntos diseñados para implementarse en las políticas.

Implementación de nuevas políticas de firewall


Pruebas del funcionamiento de políticas

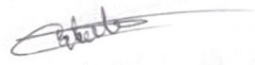
ACTIVIDADES PENDIENTES:

Pruebas del funcionamiento de políticas

Aplicación de políticas en la redes locales y externas

Creación de paquete personalizados para diferentes segmentos de red


FIRMA DEL ASESOR EMPRESARIAL


Hernandez Celine Hdc C12
FIRMA DEL ALUMNO



BITACORA DE LA ESTANCIA

29 Enero - 02 Febrero 2024

ACTIVIDADES REALIZADAS:

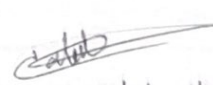
Creación de paquete personalizados para diferentes segmentos de red

Aplicación de políticas en la redes locales y externas

Ambiente simulado

ACTIVIDADES PENDIENTES:


FIRMA DEL ASESOR EMPRESARIAL


Hermanick Catalina Hdez Cár
FIRMA DEL ALUMNO



PLAN DE TRABAJO DE LA ESTANCIA

ALUMNO(S): Hermayonick Catalina Hernandez Gonzalez

ASESOR INSTITUCIONAL: MSI José Fidencio López Luna

NOMBRE DE LA EMPRESA: Fiscalía General De Justicia Del Estado De Tamaulipas

ASESOR EMPRESARIAL: LIC. Víctor Luis Aguilar Morales

| No. | ACTIVIDAD Ejemplo | FECHA INICIO | FECHA TÉRMINO | TIEMPO (HRS) | AVANCE | ENERO-FEBRERO | | | |
|-----|--|-----------------|------------------|-----------------|--------|---------------|----|----|----|
| | | | | | | S1 | S2 | S3 | S4 |
| 1 | Investigaciones generales | 8/01/24 | 12/01/24 | 40HRS | P | | | | |
| | | | | | R | | | | |
| 2 | Conocimiento de la red(LAN) | 15/01/24 | 18/01/24 | 24HRS | | | | | |
| | | | | | | | | | |
| 3 | Realización de Diagrama de la red | 19/01/24 | 23/01/24 | 18HRS | P | | | | |
| | | | | | R | | | | |
| 4 | Dar acceso a internet a un equipo informático | 19/01/24 | 19/01/24 | 8HRS | P | | | | |
| | | | | | R | | | | |
| 5 | Implementación de políticas de firewall | 22/01/24 | 26/01/24 | 30HRS | P | | | | |
| | | | | | R | | | | |
| 6 | Pruebas del funcionamiento de políticas | 22/01/24 | 26/01/24 | 40HRS | P | | | | |
| | | | | | R | | | | |
| 7 | Activación de nuevas redes locales al sistema | 26/01/24 | 29/01/24 | 8HRS | P | | | | |
| | | | | | R | | | | |
| 8 | Creación paquete personalizados para diferentes segmentos de red | 30/01/24 | 31/01/24 | 16HRS | P | | | | |
| | | | | | R | | | | |
| 9 | Aplicación final de políticas | 1/02/24 | 2/02/24 | 16HRS | P | | | | |
| | | | | | R | | | | |


OBSERVACIONES:

| |
|--|
| |
| |

EVALUACIÓN DEL REPORTE DE ESTANCIA

LISTA DE COTEJO

DATOS GENERALES DEL PROCESO DE EVALUACIÓN

| | | | |
|--|---|---|--|
| NOMBRE ALUMNO: Hermayonick Catalina Hernandez Gonzalez | | NOMBRE DEL ASESOR INSTITUCIONAL: MSI José Fidencio López Luna | |
| MATRICULA: 2130036 | PROGRAMA ACADÉMICO | FIRMA DEL ASESOR INSTITUCIONAL: | |
| | ITI MEC ISA ITM | | |
| FIRMA DEL ALUMNO: |  | | |

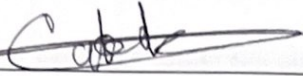
INSTRUCCIONES

En la columna de valor se encuentran sombreados los reactivos esenciales de su calificación. Revisar las actividades que se solicitan y marque en los apartados el porcentaje y la ponderación (en relación al porcentaje del valor) de cada reactivo. En la columna "OBSERVACIONES" * mencione indicaciones que puedan ayudar al alumno a saber cuales son las condiciones no cumplidas, si fuese necesario.

| VALOR | Característica a cumplir (Reactivo) | Porcentaje | Ponderación | OBSERVACIONES |
|---------------|--|------------|-------------|---------------|
| 10 | Presentación El reporte cumple con los requisitos de: a. Buena presentación b. No tiene faltas de ortografía c. Maneja el lenguaje apropiado. | | | |
| 5 | Resumen ejecutivo y abstract. Indica qué se realizó, cómo se realizó y qué se obtuvo. (una cuartilla en español e inglés). | | | |
| 5 | Marco teórico. Presentan una descripción teórica de la tecnología y recursos utilizados. | | | |
| 5 | Justificación. Deficiencia del problema, justifica el proyecto (¿Por qué razón realiza el proyecto?, por ejemplo, puede ser parte de los planes de la mejora de la empresa, de un problema de producción o se trata de una parte de un proyecto mayor). | | | |
| 5 | Objetivos. Describen cual será el motivo del proyecto o actividades a realizar. | | | |
| 30 | Desarrollo. Sigue una metodología de trabajo y sustenta lo que se realizó. | | | |
| 20 | Resultados. Interpreta y analiza los resultados obtenidos durante su estancia. | | | |
| 10 | Conclusiones. Las conclusiones son claras y acordes con el objetivo esperado. | | | |
| 10 | Responsabilidad. Entregó el reporte en la fecha y hora señalada, así como asistió al menos al 80% de sus días de estancia. | | | |
| CALIFICACIÓN: | | | | |

CONCENTRADO DE LAS EVALUACIONES

DATOS GENERALES DEL PROCESO DE EVALUACIÓN

| | | | | |
|----------------------|---|--------------------|---------------------|--------------|
| NOMBRE ALUMNO: | Hermayonick Catlina Hernandez Gonzalez | PROGRAMA ACADÉMICO | | |
| MATRICULA: | 2130036 | MEC | ITI | ITM |
| FIRMA ALUMNO: |  | FECHA: | | |
| FIRMA DEL EVALUADOR: | | | | |
| | Criterios de evaluación | Ponderación | Calificación | Total |
| 1 | Estancia (Asesor Empresarial) | 35% | | |
| 2 | Exposición (Asesor Institucional) | 20% | | |
| 3 | Reporte (Asesor Institucional) | 25% | | |
| 4 | Exposición en inglés(Asesor Institucional) | 20% | | |
| CALIFICACIÓN | | | | |