UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

OCTUBRE 2023 - MARZO 2024

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

ANALISIS DE VULNERABILIDAD Y PROPUESTA DE ASEGURAMIENTO DE LA SEGURIDAD DE LA INFORMACION EN LA INFRAESTRUCTURA TECNOLOGICA DE LA EMPRESA “INTERNET LOS RIOS”

ESTUDIANTE:

SOLORZANO PALMA VALENTIN GREGORIO

TUTOR:

ING. MONTECE MORENO OMAR

AÑO 2024

RESUMEN

En la actualidad la información es la base fundamental para cualquier organización, empresa o entidad, en un mundo tan interconectado, en donde los datos de las personas son cada vez mayores y la necesidad de proteger los mismos es un requisito importante dentro de los organismos para asegurar la integridad de los usuarios que se registran dentro de un sistema. El tratamiento de la información recoge muchos aspectos para la recolección de datos, que van desde documentos físicos hasta documentos virtuales almacenados en bases de datos. Para un ISP la protección de la información es de suma importancia, dado a que, cualquier intrusión a estos provocaría una violación grave a los equipos y datos informáticos de los clientes, vulnerando así la seguridad y dándole a los atacantes acceso y control a estos. Por esto el presente proyecto busca hacer un análisis de la seguridad de la información en la infraestructura tecnológica de la empresa "Internet Los Ríos" buscando las posibles vulnerabilidades y amenazas que puedan comprometer gravemente la integridad de la empresa. Durante el desarrollo del caso de estudio se conocerán bases teóricas sobre los temas relacionados a la seguridad informática y de la información, así mismo veremos los tipos de ataques que se pueden suscitar y formas de cómo evitarlos, a su vez buscar técnicas de prevención para asegurar la información e impedir el secuestro de la misma. Una seguridad fuertemente fundamentada y aplicada será una barrera que alejara cualquier tipo a ataque que busque atentar contra el bienestar de los activos de la entidad, el aprender conceptos, términos y métodos que utilizan los distintos tipos de delitos en el ciberespacio dará un enfoque claro y dotara de mejores estrategias para la prevención de estos.

PALABRAS CLAVES

Seguridad Informática, Vulnerabilidades, ISP, Router, Hacker, Cracker, Exploit, Payload, Pentesting, Backdoor, Nessus, Nmap, Virus, Spyware, Gusano.

SUMMARY

Currently, information is the fundamental basis for any organization, company or entity, in such an interconnected world, where people's data is increasing and the need to protect it is an important requirement within organizations to Ensure the integrity of users who register within a system. Information processing includes many aspects for data collection, ranging from physical documents to virtual documents stored in databases. For an ISP, the protection of information is of utmost importance, given that any intrusion into these would cause a serious violation of the clients' computer equipment and data, thus violating security and giving attackers access and control over them. For this reason, this project seeks to carry out an analysis of the information security in the technological infrastructure of the company “Internet Los Ríos” looking for possible vulnerabilities and threats that could seriously compromise the integrity of the company. During the development of the case study, theoretical bases will be known about the topics related to computer and information security. Likewise, we will see the types of attacks that can arise and ways of how to avoid them, in turn looking for prevention techniques to ensure . information and prevent its kidnapping. Strongly founded and applied security will be a barrier that will keep away any type of attack that seeks to attack the well-being of the entity's assets. Learning concepts, terms and methods used by different types of crimes in cyberspace will give a clear and will provide better strategies for the prevention of these.

KEYWORDS

Computer Security, Vulnerabilities, ISP, Router, Hacker, Cracker, Exploit, Payload, Pentesting, Backdoor, Nessus, Nmap, Virus, Spyware, Worm.

CONTENIDO

PLANTEAMIENTO DEL PROBLEMA

Las ISP son empresas que brindan conexión de internet a todos sus clientes, por eso mismo tienen un contacto cercano hacia ellos, por ende en “Internet Los Ríos” el procurar salvaguardar la información de cada uno de ellos debe ser un requisito primordial para el cumplimiento de sus funciones, para ello se debe mantener dentro de la empresa un conocimiento extenso y certero sobre los peligros a los que están expuesto por el desconocimiento y pocos testeos sobre la seguridad de sus máquinas y sistemas informáticos, siendo este una de las problemáticas a las cuales se enfoca el siguiente estudio.

En tal situación, el hacer un análisis sobre la infraestructura tecnológica y el conocer todos los riegos de vulnerabilidad que esta presenta, permitirá tomar acción sobre los distintos métodos de ataque que utilizan los ciberdelincuentes para el robo de la información. El tener un sistema seguro y confiable evitará cualquier intrusión a los datos guardados de la empresa, evitando robos y extorciones de datos.

El problema no solo radica en las vulnerabilidades que tenga en la infraestructura tecnológica, sino también en las prácticas que se dan dentro de ella. Por eso el instruir a los empleados sobre el buen manejo de estas, brindarán una mayor confiabilidad y asegurarse de no ser no comprometer los datos de los usuarios.

No integrar dentro de su sistema buenas prácticas, controles de prevención, sistemas de seguridad, capacitaciones de seguridad informáticas y otros protocolos de prevención de riegos informáticos, sufrirán ataques y ser víctimas de delitos informáticos.

JUSTIFICACION

La empresa “Internet Los Ríos” es uno de los ISP más cotizados en las zonas rurales de la provincia de Los Ríos dado a que desde sus inicios fue su principal enfoque. La empresa cuenta con una infraestructura que busca estar en constante evolución, de esta depende el correcto funcionamiento de los diferentes procesos administrativos dentro de la institución hacia sus usuarios, lo cual implica un gran compromiso con los mismos, en una era donde todo está interconectado y la información es la principal arma, el acceder a esta de forma no autorizada significa que todos los datos están comprometidos.

Debido a esto es esencial para que la empresa cuente con un base sólida de seguridad robusta la cual mantenga a salvo toda la información, dado a que toda esta se encuentra en equipos informáticos de la empresa, lo cual el más mínimo acceso no deseado puede ser fuertemente perjudicial, obteniendo datos privilegiados, lo cual a su vez también podría fácilmente tener acceso a equipos de clientes y poder vulnerar toda una red doméstica teniendo el control de ello, por lo cual el prevenir todas estas problemáticas a tiempo evitarían estos sucesos los cuales afectarían gravemente la integridad y reputación, presentando pérdidas de tiempo y dinero.

En la actualidad toda empresa y organización busca brindar el mejor servicio posible, por lo cual el aseguramiento de la información es un punto clave dentro de cualquier infraestructura, el prevenir riesgos de la información aplicando técnicas de seguridad informática hará que la empresa mejore significativamente este aspecto. La seguridad es esencial en cualquier infraestructura tecnológica, todo daño que esta reciba afectará duramente en los procesos internos, dejando muy mal parada la confiabilidad del ISP, para ello el usar medidas de prevención con antelación es la mejor opción para evitar estos problemas.

OBJETIVOS

Objetivo General

- Analizar los posibles ataques cibernéticos a los sistemas informáticos de la empresa “Internet Los Ríos” evaluando vulnerabilidades desde un punto de vista técnico de toda la infraestructura tecnológica y de tal modo plantear una propuesta que asegure toda la información, mitigando todo tipo de riesgos y protegiendo los activos importantes de la empresa.

Objetivos Específicos

- Identificar y analizar vulnerabilidades mediante técnicas y herramientas que permitan evaluar de manera práctica la infraestructura tecnológica de la empresa "Internet Los Ríos".
- Determinar mediante diversas técnicas y pruebas de pentesting posibles fallos críticos en la seguridad de la información de la empresa.
- Establecer de manera clara políticas y procedimientos que permitan mitigar cualquier riesgo de seguridad informática y a su vez responder a incidentes de seguridad.

LINEA DE INVESTIGACIÓN

- Sistemas de información y comunicación, emprendimiento e innovación.

SUBLINEA DE INVESTIGACIÓN

- Redes y tecnologías inteligentes de software y hardware.

Este caso de estudio tiene una amplia relación con la línea de investigación dado a que el tema contiene aspectos de seguridad de la información dentro de una infraestructura tecnológica, lo cual está relacionada con los sistemas de información y comunicación, así como la manipulación de equipos computacionales para la mejora continua de la seguridad.

La sublinea de investigación redes y tecnologías inteligentes de software y hardware se relaciona dado a que con el uso de las redes se efectúan la mayoría de los ciberataques, infectando sistemas informáticos mediante el uso de aplicaciones malignas comprometiendo de esta forma datos críticos de la empresa y perjudicando gravemente la integridad de sus clientes, para la prevención de esto, se hacen uso de herramientas software y hardware para la efectuación de pruebas de pentesting para el desarrollo de protocolos de aseguramiento de la información.

El seguimiento de esta sublinea permite dirigir a la elaboración de nuevas medidas de seguridad, algunas de estas como la obtención sistemas que permitan detectar invasiones y otros que ayudan a prevenir intrusiones, con ello poder salvaguardar la infraestructura tecnológica de todo tipo peligros cibernéticos. Con un buen aprovechamiento de las características de las redes y recursos tecnológicos pueden aumentar el rendimiento, mejorando la disponibilidad de los servicios.

MARCO CONCEPTUAL

En el presente marco conceptual se ha buscado una variedad de conceptos claves para la profundización de este caso de estudio, para ello analizaremos una variedad de temas basados en los sistemas de información, ciberseguridad, prevención de riesgos e infraestructura tecnológica.

Seguridad informática

La seguridad informática es un término referente a la protección de toda la información y como esta es procesada y almacenada con la intención de evitar la manipulación de los datos y evitar ser modificada por una persona no autorizada.

Hay muchos conceptos para definir la seguridad informática, una de esta se la interpreta como: “El proceso de anticipación e identificación de accesos maliciosos a sistemas informáticos y sus recursos por parte de agentes externos, anónimos e incluso a veces personas que pertenecen a la misma institución.” (Valencia Martínez et al., 2023)

Este concepto nos dice qué los sistemas informáticos deben estar libres del acceso por personas sin autorización y libre de cualquier intrusión no deseada, por la cual se realizan procesos de prevención y detención de todos estos.

Característica de la seguridad informática

La seguridad informática tiene características esenciales para poder ser fuerte y eficaz, de tal forma poder brindar una seguridad robusta a todo su sistema, en el mundo de la tecnología todo sistema puede ser vulnerado, para ello es necesario contar con bases y principios a los cuales apoyarse para otorgar las mejores prácticas de protección y no dejar fugas de las cuales se aprovechen los ciberdelincuentes.

Según Pinilla (2022) la seguridad de la información tiene ciertas características que se centran en garantizar y mantener dentro de cualquier organización:

A. **Autenticidad:** Es una comprobación de identidad, en esta se garantiza de que un mensaje, transacción o intercambio de información pertenece de la fuente que dice ser.

B. **Confidencialidad:** Hace referencia a comprender que toda la información que se adquiera y se almacene deber ser protegida, así mismo saber a quién autorizar y como dar accesos.

C. **Integridad:** Significa que la información no se debe modificar durante su almacenamiento o transmisión.

D. **No Repudio:** Se refiere a la seguridad de que alguien o una entidad no podrán negar algo. Es la capacidad para asegurar que las partes en un contrato o comunicación no podrán negar la autenticidad de su firma o envío de un mensaje.

Estas características se reflejan como los pilares de la seguridad, son puntos claves dentro de cualquier infraestructura actual dado a que la ausencia de una de ellas provocaría una brecha grande en la guarda de los datos, la autenticidad permite la identificación dentro de un intercambio de mensaje, permite saber quién, cómo y desde dónde se la envía. La confidencialidad es el proteger la información, saber quién puede tener acceso a ella y quién no, la integridad que se basa en el principio de la honestidad, que la información no debe ser modificada en su envio y el no repudio que es la característica en la cual ambas partes no podrán negar el mensaje enviado y recibido dentro de una comunicación.

Importancia de la seguridad informática dentro de una empresa

La seguridad informática dentro de una empresa es de suma importancia, es la barrera que separa los datos privilegiados de los atacantes de sombrero negro, cada empresa debe contar con un sistema seguro que acoja fuertemente los datos críticos de la entidad, pero para lograr dicha finalidad no solo se basa en tener equipos y softwares de calidad, sino también un personal capacitado para el correcto uso de estas herramientas.

Matías Armándola (2021) señala que "La formación constante brinda una gran ayuda a prevenir quebrantamientos y ataques, ayuda a fortificar las protecciones tecnológicas, dado que a como se sabe, necesitan de la contribución constante de las personas. Las organizaciones que resaltan la capacitación también son más rápidos y eficaces en la detección de ataques y más efectivos en aislarlos."

Una empresa comprometida con el servicio y disponibilidad, debe tener en cuenta todo aspecto relacionado con la protección, cada causa tiene su efecto y el tener un sistema deficiente no es más que una bomba de tiempo esperando a ser detonada. Por eso es tan importante la seguridad de la información.

Tipos de seguridad informática

En la informática hay una variedad de tipos de seguridad la cual una empresa tiene que tener en cuenta para el aseguramiento y protección de los datos. Para Jorge Che Centurión (2019) los tipos de la seguridad informática son:

- **Seguridad de Hardware:**

Se puede asociar con un dispositivo que se aplicar para escanear un sistema o vigilar el tráfico de red. Los ejemplos más comunes incluyen firewalls o cortafuegos de hardware y servidores proxy.

- **Seguridad de Software:**

Se emplea para preservar el software contra ataques malintencionados de hackers y otros riesgos, de forma que nuestro software siga operando correctamente con este tipo de potenciales peligros. Esta seguridad de software es indispensable para proporcionar integridad, autenticación y disponibilidad.

- **Seguridad de Red:**

Se refiere a diversas actividades elaboradas para proteger la red. En concreto, estas actividades aseguran la facilidad de uso, confianza, integridad y seguridad de su red y datos. La seguridad de red eficaz se dirige a una diversidad de amenazas y la manera de prevenir que entren o se esparzan en una red de dispositivos.

¿Qué son las vulnerabilidades?

Las vulnerabilidades son un punto flácido en cualquier sistema, son el punto de inflexión por donde los hackers acceden de manera ilícita a la propiedad informática de una entidad, dando lugar a usurpaciones de información y privación de la misma, cada fallo que haya puede tomarse como una oportunidad para el atacante, el ingreso de estos desemboca una pérdida sustancial, dejando mal parada la credibilidad del negocio.

Como otro concepto se puede decir que la vulnerabilidad “Es cualquier flaqueza de un activo que pueda impactar de alguna forma sobre el correcto funcionamiento del sistema

informático. Estas debilidades, también conocidas como “huecos de seguridad”, pueden estar asociadas a fallos en la implementación de los softwares o en la configuración del sistema operativo.”(Samaniego et al., 2021)

Dentro de las vulnerabilidades podemos encontrarnos con dos tipos:

- Vulnerabilidades Físicas.
- Vulnerabilidades Lógicas.
- **Vulnerabilidades Físicas**

Para Romero (2018) Las vulnerabilidades físicas son aquellas vulnerabilidades que van a afectar personalmente a la infraestructura de la organización de manera material y de las cuales se pueden señalar a los desastres naturales en este tipo de clasificación, un ejemplo de este se podría identificar una vulnerabilidad de este tipo sí se vive en una zona con un porcentaje alto en riesgo de sismos, ya que puede surgir una negación en el servicio, una vulneración en la disposición y a partir de ahí podría iniciarse con problemas. Si la organización está en una zona que generalmente se inunda, se tiene también otro tipo de vulnerabilidad.

Estas vulnerabilidades se centran en los equipos tangibles de la organización, es decir, son tienen que ver con todo componente electrónico físico que puede ser manipulado directamente con el tacto humano y en este tipo de vulnerabilidades dependen también de la zona en donde se encuentre ubicada.

- **Vulnerabilidades Lógicas**

Estas tendrán un gran efecto en la infraestructura lógica y en cada uno de los procesos que se realicen dentro de ella. Romero (2018) también nos dice que estas operaciones pueden ser:

- Configuración
- Actualización
- Desarrollo

En este apartado podemos decir que, las vulnerabilidades de configuración en el sistema operativo, se puede referir a todas aquellas configuraciones predeterminadas del sistema o incluso en aquellas aplicaciones del servidor que se tengan susceptibles, puede ser también la composición de algunos firewalls que no está administrado de una manera correcta y también de infraestructura perimetral.

Las vulnerabilidades de actualización, estas están más referenciadas en las cuales las empresas no actualizan sus sistemas, debido a esto van surgiendo más vulnerabilidades y es uno de los puntos principales en los cuales se debe tomar en cuenta para el aseguramiento.

Las vulnerabilidades de desarrollo, aquí se puede mencionar las inyecciones de código en SQL, Cross Site Scripting, esto puede variar dependiendo del tipo de aplicación, la validación de los datos.

Terminología de las diferentes variables:

- **Hacker:**

Un hacker es una persona con amplios conocimientos informáticos que con ello incursiona dentro de todos los ámbitos de la informática, estos tienen el objetivo de demostrar saber en estos temas, buscando siempre fallos y vulnerabilidades en cualquier sistema.

Los hackers son personas hábiles que llevan consigo amplios conocimientos informáticos desarrollados para acceder a un concreto sistema o dispositivo y realizar modificaciones desde

adentro, fundamentalmente destinadas a la seguridad informática y a la evolución de técnicas para su mejora. (Redacción Banco Pichincha, 2022)

- **Cracker:**

Un cracker es una persona con amplios conocimientos informáticos pero que a diferencia de los hackers su finalidad es la de hacer actividades plenamente ilícitas, buscando vulnerabilidades en softwares o sistemas informáticos con el único fin de violar la integridad de los usuarios.

El cracker invade los sistemas para hurtar archivos y cualquier tipo de información digital, que le sirva para poder pedir un rescate por su devolución. Estos se ven favorecidos de la más mínima oportunidad sin ningún tipo de compunción moral, estos buscan lucrarse económicamente de estas fragilidades dentro de los sistemas, haciendo intrusiones no autorizadas, cometiendo actos ilegales fuera de la ley. (Ortega, 2023)

- **Ethical Hacking:**

El hacking ético conlleva la realización de testeos de seguridad de la información para identificar para identificar exposiciones amenazas y vulnerabilidades en redes y sistemas de información. El fin es evaluar el comportamiento actual de la organización, con la finalidad de implementar los protocolos necesarios para avalar la protección y seguridad de los activos y datos de la empresa. (Andreina Vivar, 2023)

- **Exploit:**

Este es un lenguaje de programación el cual se centra en buscar y hallar vulnerabilidades dentro de un sistema operativo, inyectando código malicioso para explotar un fallo. Un script

utilizado para explotar un error o vulnerabilidad en un sistema para provocar un comportamiento no deseado o inesperado.(Una guía de aproximación para el empresario, 2020)

- **Payload:**

El payload son instrucciones ejecutadas en el servidor de destino aprovechándose de la vulnerabilidad para establecer y administrar una conexión con el sistema de destino. Con ello abrir una sesión y poder así indagar en los documentos internos de la maquina atacada. El payload es la carga maliciosa que ejecuta un hacker en el ordenador de una víctima durante un ciberataque. Si bien, por medio de la explotación de vulnerabilidades, el atacante consigue infiltrarse en un sistema, el payload es aquel set de instrucciones que ejecutará el daño deseado en el ordenador.

Un payload es una carga útil maliciosa que un pirata informático ejecuta en la computadora de una víctima durante un ataque cibernético. Incluso si un atacante logra ingresar al sistema aprovechando los agujeros de seguridad, la carga útil es un conjunto de instrucciones que causan el daño deseado a la computadora. (Redacción KeepCoding, 2023)

- **Kali Linux:**

Kali Linux (basado en Debian GNU/Linux) es uno de los sistemas operativos de código más utilizados para el pentesting, Su fama se debe a que este colecciona una gran variedad de instrumentos para el monitoreo y testeo de todas las debilidades de un sistema informático. Es el sistema con mayor utilización para comprobar la seguridad de los sistemas empleados en un solo sistema.

El sistema operativo Kali Linux está diseñado concretamente en Linux, enfocándose en el análisis de la seguridad informática. Esta distribución basada en Debian está dirigida a una gran variedad de trabajos de seguridad, en las cuales están las pruebas anticipadas, indagación de

seguridad, investigación de crímenes cibernéticos e ingeniería inversa. Kali trae consigo cientos de herramientas centradas en la seguridad, varias se usan para diagnosticar redes, desciframiento de contraseñas, prospección de vulnerabilidades, vulnerabilidades inalámbricas, piratería de bases de datos, ataque a dispositivos móviles y una gran variedad más. (Ordoñez, 2023)

- **Ingeniería Social:**

La ingeniería social es la práctica ilegítima en donde los atacantes utilizan manipulaciones para la obtención de información de un usuario y de esta manera poder acceder a datos privilegiados gracias al fallo humano.

También se puede definir a la ingeniería social como el conjunto de técnicas utilizadas por delincuentes para embaucar a los usuarios de sistemas y servicios TIC, para que estos les proporcionen información de valor añadido como credenciales, información sobre sistemas, servicios instalados, etc. (Una guía de aproximación para el empresario, 2020)

- **Backdoor:**

Un backdoor o puerta trasera es un acceso remoto secreto que permite que los atacantes puedan ingresar a un dispositivo de manera remota, este se define como un virus que permite al usuario poder controlar los dispositivos a distancia, con esto poder extraer información, enviar archivos, ejecutarlos, eliminarlos, reiniciar el equipo, etc.

Los backdoors no necesariamente suelen ser maliciosos, esto pueden utilizarse por usuarios legítimos para operaciones de mantenimiento o hacer updates de dispositivos. Sin embargo, su utilización puede convertirse en arriesgada, dado que, a través de un software previamente existente en el sistema, puede ayudar a que un usuario ilegítimo tome el control de manera remota y persistente. (Gómez, 2023)

- **Router:**

Un router es un dispositivo que sirve para realizar conexiones entre una red local e internet, estos equipos son muy importantes dado a que otorgan direcciones ip y enrutan los dispositivos a internet. La principal misión del router es capturar la conexión a internet que nos brinda el módem y compartirlas en varias líneas de servicio, ya sean alámbricas, tanto por cable o por conexiones inalámbricas, estas serían a través de ondas por wifi. Finalmente, estas líneas de servicio cumplen la función para que todos los dispositivos se conectan a internet. (Bermúdez, 2022)

- **Access Point:**

Un access point funciona como un emisor de señal para la conexión de diferentes dispositivos inalámbricos, esto permite que puedan conectarse a internet sin ningún tipo de conexión cableada, haciendo más extenso su área de registro, aumentando de tal forma el número de equipos que puedan conectarse a la red.

En teoría, los Access Point (AP) o Wireless Access Point (WAP) son famosos por establecer una conexión inalámbrica entre aparatos y pueden montar una red inalámbrica externa (local o internet) para vincular dispositivos móviles o tarjetas de red inalámbricas. (Pachón, 2023)

- **Ciberseguridad ofensiva:**

La ciberseguridad ofensiva es cuando se aplican métodos y técnicas que usan los atacantes para vulnerar los sistemas de una organización, pero estas no van dirigidas para provocar daño, más bien va dirigida para mejorar los sistemas de seguridad de la empresa.

La seguridad ofensiva de tiene un deber fundamental, que es el de asistir a las organizaciones a consolidar su postura de seguridad precisando y corrigiendo extenuantemente las vulnerabilidades antes de que sean aprovechadas fuertemente por los atacantes maliciosos. Esto se logra por medio de la ejecución de pruebas de penetración, valoración de vulnerabilidades, ingeniería inversa, averiguación sobre las amenazas y otras técnicas avanzadas para identificar posibles puntos frágiles en los sistemas. (Ruiz, 2023)

- **Pentesting:**

El pentesting es una técnica de penetración en la cual se le realizan varias pruebas a un sistema para saber el nivel de seguridad que esta tiene, aquí se realizan múltiples ataques informáticos y se va evaluando cada uno de ellos, así mismo se analiza como el sistema actúa ante cada uno de ellos, ver los puntos débiles y mejorarlos para evitar problemas de seguridad a futuro.

Con el pentesting lo que se busca es fingir uno o varios ataques malignos, pero sin ninguna intención de perjudicar, al contrario, el fin de estos ataques es identificar y comprobar potenciales fallos en la seguridad comprometiendo los sistemas informáticos. Estas pruebas son comunes en el ámbito de la seguridad de softwares y sitios web. El aplicar el pentesting permite aumentar la seguridad de muchos de los componentes tecnológicos, así también proteger la información almacenada por las distintas aplicaciones. (Fernández, 2022)

Tipos de ataques a los sistemas informáticos

Los ataques informáticos tienen una gran relevancia en estos tiempos, dado a que estamos en la plena era tecnológica donde el estar conectado es un esencial de la vida cotidiana, los datos que de esta se obtienen cogen un valor importante para cualquier tipo de persona o entidad, dichos datos se guardan en infraestructuras tecnologías en donde son procesadas y se convierten en

información valiosa, por lo que, estos sistemas son carne de calidad para los cazadores en el ámbito informático. Debido a esto los atacantes buscan maneras y formas de vulnerar un sistema basándose en muchos tipos de ataques para la obtención de recursos valiosos de la empresa.

En este ámbito tenemos una diversa cantidad de ataques a los sistemas informáticos, de los cuales hablaremos a continuación:

- **Virus:**

Un virus es un programa malicioso el cual está expresamente diseñado por hackers con amplios conocimientos en programación con el propósito de vulnerar uno o varios equipos informáticos, este se encarga de infectar toda la máquina inyectando código malicioso dejándola así desprotegida y a merced de los atacantes.

Otra forma de describirlo sería que, "Un virus informático es un programa o código malicioso y autor replicante que se introduce en cualquier dispositivo tecnológico sin su conocimiento ni permiso provocando daños, problemas o molestias al sistema informático y, por ende, al usuario."(Robalino et al. 2022)

- **Troyano:**

Un troyano se crea mediante la codificación se hace pasar por un software legítimo, que después, este luego de su activación se convierte en una aplicación que va a permitir el acceso casi invisible a la información de un equipo y tener acceso al sistema informático.

De acuerdo con (Guaña-Moya et al., 2022) Los troyanos son constantemente utilizados por los atacantes para cumplir sus objetivos maliciosos, de los cuales estos pueden ser el acceder a backdoors (puertas traseras), manipular el dispositivo de la víctima atacada, recolectar información

y datos del equipo afectado con el fin de ser enviados y recibidos por el atacante, de tal forma descargar y ejecutar en la PC o dispositivo del usuario software malicioso adicional.

Los troyanos son de los ataques más comunes es suplantar un software existente, haciendo que los usuarios ejecuten el programa infectando el equipo que lo ejecuta.

- **Spyware:**

Es un software malicioso que, al ser instalado en el ordenador, este software hará una recopilación de todas las actividades hechas por el usuario, recopila información crítica como contraseñas, tarjetas de crédito, pin, etc. El spyware es un virus que funciona como espía y los datos que va recopilando los va enviando a personas externas.

Estos son difíciles de detectarlos, este software suele venir escondida a través de archivos o por la instalación de aplicaciones de dudosa procedencia. Esta puede ser instalada silenciosamente sin que el usuario se dé cuenta, lo cual es muy conveniente para los atacantes ya que este programa puede estar muchos días, meses o años sin que el propietario del dispositivo se dé cuenta. El software expiatorio es una clase de software que se utiliza para la obtención de información relacionada de los usuarios, sus equipos informáticos o sus comportamientos a la hora de navegar en Internet. Aplica un rastreo de todas sus actividades sin consentimiento alguno y envía los datos recolectados a otro dispositivo ubicado fuera de la red. También puede recibir y ubicar otros paquetes malintencionados de Internet. (García et al., 2021)

- **Gusanos:**

Un gusano es un malware que afecta a los dispositivos por medio de la red, este infecta ordenadores y servidores autorreproduciéndose y reduciendo espacio en el disco duro, quitando así rendimiento produciendo ralentizaciones al equipo. Este tipo de virus busca colapsar a los

computadores y las redes informáticas de tal manera impedir el perfecto funcionamiento de los softwares en el sistema operativo, este virus se aloja dentro del sistema sin que pueda ser detectado hasta un determinado tiempo para después paralizar el ordenador e impedir el trabajo del usuario. (Robalino et al., 2022)

- **Ransomware:**

Este es uno de los virus más problemáticos que puede haber, este virus priva de todo acceso que pueda tener el usuario a sus dispositivos, con esto los atacantes secuestran todos los archivos almacenados en sus equipos e impide al usuario acceder a su sistema. Quienes comenten estas fechorías exigen sumas monetarias de alto valor para la liberación de estos, provocando pérdidas sustanciales cuando hablamos de ataques a gran escala. Los archivos privados se encriptan y se bloquea el acceso que tiene el usuario. El código maligno que esta introducido en el ramsonware comunica al usuario que para poder desencriptar los archivos o desbloquear la computadora, se debe realizar un pago.(González González, 2023)

El ransomware se distingue de diferentes agresiones a la ciberseguridad en que el acceso no autorizado a la información, tales como la intromisión a datos de tarjetas de crédito, propiedad intelectual o información personal de identificación que son recibidas de manera furtiva y después esta es exfiltrada con fines de monetización; el ransomware representa una fuerte peligros que atrae consigo repercusiones de manera inmediata sobre las operaciones empresariales. (Guaña-Moya et al., 2022)

- **Phishing:**

Este tipo de ataque perteneciente a la clase de ingeniería social se basa en el enviar correos electrónicos para la obtención de información, este método es usado para engañar a personas o

empresas usando la suplantación de otro ente, por lo consiguiente los usuarios que caigan en este ataque estarán dando información privilegiada a una persona externa, este ataque es uno de los más comunes pero efectivos en estos tiempos.

Los autores Hernández Domínguez & García, 2023) nos definen que:

El phishing es un método que utiliza técnicas de ingeniería social para la suplantación de identidad electrónica y con esto poder engañar a los usuarios y muestren información sensible. Al abusar la confianza de los usuarios en las redes de datos, el phishing en el ciberespacio tiene un efecto negativo. Desafortunadamente, ninguna entidad es salva de estos ataques, por lo que deben implementar un plan ordenado de prevención, con el objetivo de reducir los riesgos ante una exposición directa.

- **Ataque de DDoS (Denegación de servicio distribuido):**

Un ataque de DDoS tiene como principal objetivo los diferentes elementos más importantes del sistema, con la condición de que se procede desde un gran número de dispositivos, los cuales se encuentran contaminados por software malicioso (malware), dicho software está bajo el control del atacante.(García et al., 2021)

Con esto podemos decir que un ataque de servicio distribuido (DDoS) es un ataque a un sistema en la cual el atacante tiene varios dispositivos afectados con un malware, estos dispositivos están esperando órdenes para ser activados, una vez se activen todos estos atacaran a un sistema informático dejándolo totalmente saturado y dejando los servicios inaccesibles a los usuarios.

- **SQL injection:**

Este tipo de ataque ocurre cuando un pirata informático introduce código realizado por sí mismo hacia un sitio web con el fin de quebrantar la seguridad y de tal manera entrar a datos vitales que están protegidos, este ataque va francamente dirigido hacia las bases de datos, que es donde se guarda toda la información.

La inyección SQL sucede cuando un hacker introduce sentencias SQL maliciosas en una aplicación web. Si logra conseguirlo, ellos podrán tener acceso a datos críticos de la base de datos. En 2023, las SQL injection siguen siendo varios de los ataques más comunes en la web. Sólo en 2022, se añadieron 1162 vulnerabilidades de inyección SQL a la base de datos de seguridad CVE. (Daityari, 2023)

Protección contra amenazas y vulnerabilidades

- **Nmap:**

Nmap es una herramienta que viene preinstalada en Kali Linux, esta se es utilizada para escanear redes y encontrar puntos débiles en esta, escanea las direcciones ip y puertos que tiene la red, con esto puede detectar servicios y puertos abiertos que puedan provocar un fallo en la infraestructura, con ello se lo puede identificar y dar solución a tiempo.

Gracias a su potencial y polivalencia, este software se ha transformado en un factor básico en la armería de los profesionales de la ciberseguridad, administradores de sistemas y hackers éticos. (Buenning, 2023)

Beneficios de usar Nmap:

Mapear una red	Permite identifica dispositivos que se encuentran conectados dentro de una red.

Identificar servicios en ejecución	Conocer todos los servicios que se ejecutan dentro de la red, brindando información clave.
Realizar una auditoría de seguridad	Esta herramienta es fundamental para realizar una auditoria en la red.
Detectar sistemas operativos	Permite identificar el sistema operativo que están corriendo en los distintos dispositivos que se conectan a la red.

- **Antispyware:**

Una de las herramientas de suma importancia para proteger los dispositivos son los antispyware, estos otorgan una excelente privacidad cuando se navega en internet. Con las crecientes amenazas denominadas como spyware, esta herramienta se ha convertido en una pieza indispensable en la defensa contra softwares malignos. (García, 2023)

Características del antispyware:

Detección	Identifica una gran cantidad de spyware y los previene evitando contaminar los dispositivos.
Escaneo en tiempo real	Los buenos antispyware pueden detectar spyware antes de que estos provoquen perjuicios.

Protección en línea	Con estos los usuarios pueden estar protegidos cuando estos estén navegando en internet.
Actualizaciones regulares	Estos se mantienen actualizados y van agregando nuevas medidas de protección ante la salida de nuevos spyware.
Integración con otros productos de seguridad	Los antispyware se pueden integran con otros productos de seguridad, como antivirus o firewall.

- **Encriptadores:**

Los encriptadores permiten cifrar los archivos, documentos, datos y enviarlos de forma en que sean ilegibles y de tal forma poder evitar el robo de información. Una de las grandes funcionalidades es que, al navegar por internet, todos los datos que se envíen van a estar cifrados y fuera del alcance de los delincuentes cibernéticos.

Encriptar una información se trata de cubrir el contenido de un mensaje y no pueda ser leído, de manera que haga falta una colaboración concreta para poder mostrar este contenido. El contenido de este mensaje pueden ser cualquier tipo de información tales como: archivos, datos, mensajes o que se te ocurra. (Fernández Y. , 2020)

Hoy en día son muchas las empresas que ofrecen software de encriptación de las cuales una empresa puede hacerse, esta para tener una mayor protección en su información.

- **Nessus:**

Con Nessus podremos hacer un escaneo de diversas vulnerabilidades que pueda presentar los distintos sistemas operativos, esta evalúa todos los distintos parámetros y con ello buscar puntos débiles que estén dentro de estos, esto ayuda agilizar el descubrimiento de vulnerabilidades.

Nessus se emplea para identificar y analizar muchas de las vulnerabilidades en la seguridad de los SO, sotfware y dispositivos de redes. Esta tiene la capacidad de escanear todo tipo de dispositivos, como firewall y routers. (Sepulveda, 2023)

MARCO METODOLOGICO

El presente estudio de caso es de tipo investigación aplicada dado a que se busca dar una propuesta de aseguramiento de la información que pueda aplicar la empresa, se hace uso de conocimientos que se van adquiriendo para aplicarlos posteriormente. La investigación evaluativa que es una de los tipos de la investigación aplicada y esta nos brinda la facilidad de examinar la gran variedad de información disponible sobre el tema a investigar, esta nos guía por la objetividad la cual nos hace basarnos en todos los datos recolectados de los temas, esta también ayuda a tomar las mejores decisiones para la planificación de la propuesta de aseguramiento.

Para la realización investigativa se hizo un énfasis en el enfoque cualitativo, dado a que se evaluó la realidad de la infraestructura tecnológica de la empresa para la protección de la información, mediante el análisis y la utilización de los instrumentos que nos ayudan a recolectar todo tipo de información, como lo son la observación y la entrevistas de donde se sacaron varios puntos claves para la formulación de soluciones. También se optó por la investigación documental debido a que con esta técnica se puede recolectar y seleccionar un sin número de información a través de la lectura de múltiples libros, documentos, artículos, revistas. Con este tipo de investigación se puede obtener información de diversas fuentes y así incrementar el conocimiento sobre todas las variables dentro de la investigación.

Esta investigación se centra analíticamente en los procesos de seguridad de la empresa “Internet Los Ríos”, buscando estar documentadas y fundamentadas para establecer procesos que ayuden en la mitigación de amenazas, esto con la ayuda de las metodologías que facilitan técnicas de aprendizaje e investigación para la formulación de soluciones.

En la investigación se realizó una entrevista a un empleado con las siguientes preguntas:

1. ¿Han tenido alguna vez un ataque informático?
2. ¿Conoce usted sobre las vulnerabilidades informáticas que tiene la empresa?
3. ¿Han realizado pruebas de pentesting en la empresa?
4. ¿Usan software de encriptación?
5. ¿Tiene conocimiento sobre las clases de peligros informáticos que existen?
6. ¿Cuántos sistemas operativos se maneja la empresa?
7. ¿Sabe usted sobre el ethical hacking?
8. ¿Tiene conocimientos sobre softwares que les permitan hacer pruebas de vulnerabilidades?
9. ¿Usted invertiría en unos de estos softwares para la implementación de estos en la empresa?
10. ¿Estaría dispuesto en hacer capacitaciones sobre temas de seguridad informática?

RESULTADOS

A partir del análisis del presente caso de estudio se han obtenido resultados sobre las principales causas que conlleva la violación de privacidad, extorciones, robos y hurto a la información de cualquier empresa. Para “Internet Los Ríos”, el procurar salvaguardar la integridad de la información de los clientes es esencial, por lo que al hacerse con medidas de seguridad que ayuden a proteger todos estos componentes dentro de su infraestructura es primordial, por ello en esta indagación se obtuvieron puntos clave que nos ayudarán a brindar siempre el mejor servicio.

Unos de los puntos importantes es el tener conocimiento sobre las principales técnicas que utilizan los delincuentes informáticos a la hora de realizar ataques, para ello estar fundamentados nos pondrán alertar sobre cualquier intrusión que quiera hacerse al sistema.

Una de las herramientas vistas en el proceso investigativo es la herramienta nmap, esta nos ayudará a saber todos los dispositivos y puertos que están en nuestra red, para ello la empresa debe siempre monitorear los puertos que estén abiertos y tomar medidas de prevención para cada uno de ellos.

Unas de las técnicas que brindará un mayor aseguramiento de la seguridad es el pentesting, dado a que esta se encarga de realizar varias pruebas de penetración y de tal forma encontrar vulnerabilidades dentro de una infraestructura tecnológica, implementarla en la empresa evitaría correr riesgos de seguridad a futuro, brindaría una mayor confiabilidad y otorgaría a la entidad un mayor prestigio.

Otras de las herramientas que puede optar la empresa para mejorar su eficiencia en encontrar fallos y vulnerabilidades es el software Nessus ya que con ayuda de esta nos dará un panorama extenso y preciso sobre todos los puntos de flacidez que llegase a poseer la entidad.

DISCUSIÓN DE RESULTADOS

En base a los resultados obtenidos se puede decir que el implementar medidas, protocolos, softwares de seguridad, entre otros, es la mejor opción que puede optar la empresa, la seguridad es un papel importante y para ello es indispensable tomar medidas al asunto. Dentro de "Internet Los Ríos" el implementar todas estas bases de ciberseguridad sentaría el comienzo de una buena longevidad y sin tantas complicaciones, previniendo amenazas futuras que puedan dañar gravemente los sistemas de información de la empresa.

El utilizar el pentesting el cual cuenta con diversas técnicas y herramientas para la comprobación de seguridad en los procesos internos de la empresa. El vigilar y testear todos estos procesos provocará un efecto positivo, llevando a cabo grandes avances en la protección de los datos.

Una de las herramientas básicas, que a su vez es clave para este proceso de testeo, es la herramienta nmap, dado que con esta tendremos una amplia información de los dispositivos que están conectados dentro de una red. Con ella podremos analizar las direcciones ip, saber cuáles puertos tienen, cuáles están abiertos, el nombre y la versión de los servicios que cuenta la máquina, el sistema operativo que posee y muchos atributos más, esta herramienta es una de las más usadas al hacer pentesting.

Un buen análisis de todas estas vulnerabilidades debe estar bien documentadas, la empresa debe tomar cartas sobre el asunto, implementar políticas de seguridad que permitan el correcto flujo de la información sin ninguna fuga, ya que el tener buenos componentes dentro de la infraestructura y una buena configuración dentro de ella, hará que el sistema de información sea robusto y casi impenetrable, evitando la invasión de personas externas a la información.

El uso de herramientas para la búsqueda de vulnerabilidades es una de las grandes opciones a tomar en cuenta, estas herramientas permiten de manera rápida, eficaz y segura ver los múltiples fallos que pueda tener el sistema, estas ahorran tiempos y disgustos al buscar estos fallos de manera manual. El implementar una de estas sería de gran beneficio, dado a que de una manera rápida y sencilla se podrá hacer un análisis e informe sobre todas las fallas de seguridad pertinentes dentro de la empresa y de las cuales se deberán corregir con anticipación, siendo estas las más afectadas y por las cuales los atacantes pueden actuar.

Dado a todo esto una de las mejores herramientas a usar sería el software de Nessus, este software otorgará a la empresa un escáner de vulnerabilidades a todos los sistemas que haya, esta ofrecerá a "Internet Los Ríos" el ejecutar un fácil escaneo para corroborar la existencia de desprotección dentro del sistema, esto ayudará a acelerar la detección de amenazas y priorización de los problemas que ocurran.

El aplicar dentro de la entidad un software de encriptación hará que la seguridad en enviar y recibir datos críticos de la empresa siempre esté a salvo, creando así un camino seguro para la emisión y recepción de los mismos, en la encriptación el cifrado es importante, de esta manera hará que cualquier agente externo que quiera capturar información, se le sea imposible hacerlo, con esto la comunicación estará siempre salvaguardada, efectuando así las características de la seguridad informática que es la autenticidad, confidencialidad, integridad y el no repudio.

La seguridad siempre va a ser un factor que debe estar presente en cualquier ámbito y más cuando se trata de la información, la información desde los inicios siempre ha sido una gran arma de dominación, por ello los malhechores del ciberespacio quieren hacerse con ella y el deber de la empresa es implementar medidas que prevean estos problemas y mitigar cualquier riesgo que pueda haber a futuro.

CONCLUSIONES

En conclusión, este estudio de caso refleja de forma sencilla y factible la forma en la que la empresa debe tomar medidas de seguridad en los aspectos informáticos. Para ello se identifica y analiza cada una de las vulnerabilidades que pueda haber dentro del sistema mediante el uso de técnicas enfocadas en la protección de los datos, con esto y con la ayuda de herramientas se puede evaluar de manera rápida y practica la infraestructura tecnología y conllevar a la formulación de estrategias para el aseguramiento de la información.

Determinar múltiples técnicas y pruebas de pentesting con la ayuda de las herramientas que esta trae consigo, permite encontrar fallos críticos que comprometan la integridad de cada uno de los componentes tecnológicos, por lo cual el hacer y aplicar estas dentro de la organización facilitará el precisar estas vulnerabilidades y de tal forma poder mitigar cada una de estas. Con ayuda de sistemas operativos como Kali Linux en donde agrupa un sinnúmero de estas herramientas, estas las cuales se utilizan para el análisis y pruebas de seguridad dentro de la empresa “Internet Los Ríos” se podrá priorizar la mejora de la robustes y eficacia de la infraestructura tecnológica.

Con todas las pruebas de seguridad que se puedan hacer, se podrá establecer procedimientos que ayuden a prevenir y mitigar los riegos que se vayan presentando, así mismo establecer políticas que se deben cumplir para el aseguramiento de la misma, todo esto permitirá responder de forma clara y contundente cualquier incidencia que surja en relación con la seguridad informática.

RECOMENDACIONES

Hacer una constante revisión sobre las vulnerabilidades tecnológicas dentro de los sistemas de la empresa. De tal manera realizar un seguimiento continuo de todos los procesos y protocolos dentro de ella, que permitan examinar y evaluar cada uno de los puntos críticos que se establezcan.

Contratar especialistas en la ciberseguridad para el testeo y la realización de estudios pertinentes al pentesting para examinar, evaluar y mejorar la seguridad de su sistema, con el fin de aumentar significativamente la calidad de la seguridad y salvaguardar la integridad de la información.

Realizar y establecer políticas de seguridad estrictas dentro de la empresa, manteniendo un orden y control dentro de ella, otorgando acceso privilegiado solo a un pequeño grupo de personas de confianza. Así mismo el proceder a hacer capacitaciones a los empleados sobre el cómo actuar y protegerse antes los distintos tipos de peligros cibernéticos.

REFERENCIAS

García, S., Tutor, B., Manuel, Á., & Juarez, O. (2021). DETECCIÓN Y ANÁLISIS DE ARTEFACTOS EN LOS PRINCIPALES TIPOS DE CIBERATAQUES.

González González, J. M. (2023). Uso de las Técnicas Del Hacking Ético para la Reducción de Amenazas de Ciberseguridad.

Guaña-Moya, J., Sánchez-Zumba, A., Chérrez-Vintimilla, P., Chulde-Obando, L., Jaramillo-Flores, P., & Pillajo-Rea, C. (2022). Ataques informáticos más comunes en el mundo digitalizado.

Hernández Dominguez, A., & García, W. B. (2023). Modelo para la detección de ataques de phishing contra el servicio de correo electrónico Model for phishing email detection. Revista Cubana de Ciencias Informáticas, 17. http://rcci.uci.cuPág.132-147

Jorge Enrique Che Centurión. (2019). SEGURIDAD DE LA INFORMACIÓN.

Patricio Robalino Willian Geovanny Yanza Chávez Johana Katerine Montoya Lunavictoria, A. (2022). Auditoría Informática.

Pinilla Alexander. (2022). Resiliencia en la Seguridad Informática.

Romero, M. I., Grace, C., Figueroa, L., Denisse, M., Vera, S., José, N., Álava, E., Galo, C., Parrales, R., Christian, A., Álava, J., Ángel, M., Murillo Quimiz, L., Adriana, M., & Merino, C. (2018). INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES.

Samaniego, E. A., Jéssica, M., & Ponce Ordóñez, A. (2021). Fundamentos de seguridad informática.

Una guía de aproximación para el empresario. (2020). Glosario de términos de ciberseguridad.

Valencia Martínez, N. A., Yulán Valencia, C. M., & Chipe Valencia, B. D. (2023). Resiliencia en la informática. RECIMUNDO, 7(1), 79–86. https://doi.org/10.26820/recimundo/7.(1).enero.2023.79-86

Vivar Franco Itati Aandreina. (2023). EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA PRUEBA PRÁCTICA PREVIO A LA OBTENCIÓN DEL TÍTULO DE.

Armándola, M. (16 de 8 de 2021). Ciberseguridad: por qué es clave la capacitación continua del personal. Obtenido de Ciberseguridad: por qué es clave la capacitación continua del personal: https://es.linkedin.com/pulse/ciberseguridad-por-qu%C3%A9-es-clave-la-capacitaci%C3%B3n-del-mat%C3%ADas-arm%C3%A1ndola

Bermúdez, J. (17 de Octubre de 2022). Router vs Módem ¿Cuáles son sus diferencias y para qué sirve cada uno? Obtenido de Router vs Módem ¿Cuáles son sus diferencias y para qué sirve cada uno?: https://www.pccomponentes.com/router-vs-modem

Buenning, M. (18 de Diciembre de 2023). Cómo usar Nmap: guía completa con ejemplos. Obtenido de Cómo usar Nmap: guía completa con ejemplos: https://www.ninjaone.com/es/blog/utilizar-nmap-guia-completa/

Daityari, S. (11 de Octubre de 2023). Inyección SQL: Guía Detallada para Usuarios de WordPress. Obtenido de Inyección SQL: Guía Detallada para Usuarios de WordPress: https://kinsta.com/es/blog/inyeccion-sql/

Fernández, E. C. (27 de Octubre de 2022). ¿Qué es y en qué consiste el pentesting? Obtenido de ¿Qué es y en qué consiste el pentesting?: https://www.tokioschool.com/noticias/pentesting/

Fernández, Y. (6 de Marzo de 2020). Encriptar: qué es, para qué sirve y cómo cifrar tus archivos. Obtenido de Encriptar: qué es, para qué sirve y cómo cifrar tus archivos: https://www.xataka.com/basics/encriptar-que-sirve-como-cifrar-tus-archivos

García, D. (3 de Mayo de 2023). Antispyware: qué es, características, tecnicas y ejemplos. Obtenido de Antispyware: qué es, características, tecnicas y ejemplos: https://msmk.university/ciberseguridad/antispyware

Gómez, J. A. (2 de Febrero de 2023). ¿Qué es un Backdoor o Puerta Trasera?: 5 consejos para evitarlos. Obtenido de ¿Qué es un Backdoor o Puerta Trasera?: 5 consejos para evitarlos: https://www.deltaprotect.com/blog/backdoor-o-puerta-trasera

Ordoñez, W. (12 de agosto de 2023). Qué es Kali Linux y porque es el más utilizado en ciberseguridad. Obtenido de Qué es Kali Linux y porque es el más utilizado en ciberseguridad: https://www.grouphacking.com/linux/kali-linux/que-es-kali-linux-y-porque-es-el-mas-utilizado-en-ciberseguridad/#Que_es_Kali_Linux

Ortega, K. (7 de Febrero de 2023). ¿En qué se diferencia un hacker de un cracker? Obtenido de ¿En qué se diferencia un hacker de un cracker?: https://worldcampus.saintleo.edu/noticias/cual-es-la-diferencia-entre-un-hacker-y-un-cracker

Pachón, C. (24 de Marzo de 2023). AP (Access Point) ¿Qué son y para qué se utilizan? Obtenido de AP (Access Point) ¿Qué son y para qué se utilizan?: https://revistaseguridad360.com/noticias/access-point-que-es-y-para-que-sirve/

Redacción Banco Pichincha. (29 de Agosto de 2022). ¿Qué hacen los hackers y qué tipos existen? Obtenido de ¿Qué hacen los hackers y qué tipos existen?: https://www.pichincha.com/blog/que-es-un-hacker

Redacción KeepCoding. (2 de Octubre de 2023). ¿Qué es un payload? Obtenido de ¿Qué es un payload?: https://keepcoding.io/blog/que-es-un-payload/

Ruiz, V. (23 de Mayo de 2023). Conceptos y beneficios de la seguridad ofensiva. Obtenido de Conceptos y beneficios de la seguridad ofensiva: https://es.linkedin.com/pulse/conceptos-y-beneficios-de-la-seguridad-ofensiva-victor-ruiz

Sepulveda, M. (23 de Febrero de 2023). Que es Nessus y como utilizarlo. Obtenido de Que es Nessus y como utilizarlo: https://ciberseguridad.club/que-es-nessus-y-como-utilizarlo/

ANEXOS

Babahoyo, 16 de febrero del 2024.

Magister
Eduardo Galeas Guijarro
DECANO DE LA FACULTAD DE ADMINISTRACIÓN FINANZAS E INFORMÁTICA
En su despacho.

De mis consideraciones:

Yo: **SOLORZANO PALMA VALENTIN GREGORIO**, con cédula de identidad 120879405-5 estudiante de la carrera de "Ingeniería en Sistemas o Ingeniería Sistemas de Información" matriculado(a) en el proceso de titulación periodo Octubre 2023– Marzo 2024, le solicito a usted de la manera más comedida se sirva autorizar a quien corresponda se proceda a elaborar un oficio dirigido a INTERNET LOS RIOS ubicada en las calles SUCRE Y RICAURTE, representante legal de la empresa Jefe Local Sr. Eduardo Gustavo Moran Cabello, requiriendo el permiso respectivo para realizar mi Caso de estudio denominado ANALISIS DE VULNERABILIDAD Y PROPUESTA DE ASEGURAMIENTO DE LA SEGURIDAD DE LA INFORMACION EN LA INFRAESTRUCTURA TECNOLOGICA DE LA EMPRESA "INTERNET LOS RIOS" el cual es requisito indispensable para poder titularme.

Esperando una respuesta favorable quedo de usted muy agradecido(a).

Del señor Decano muy atentamente

V Solorzano

SOLORZANO PALMA VALENTIN GREGORIO
C.I. 120879405-5

Recibido 27 Enero 2024

RECIBIDO
UNIVERSIDAD TÉCNICA DE BABAHOYO
SECRETARIA FAFI
16-02-24 FECHA:
10:59 HORA:

UNIVERSIDAD TÉCNICA DE BABAHOYO
FACULTAD ADMINISTRACION FINANZAS E INFÓRMATICA
DECANATO

Babahoyo, 16 de febrero de 2024
D-FAFI-UTB-0181-2024

Sr.
Eduardo Moran Cabello.
REPRESENTANTE LEGAL DE LA EMPRESA INTERNET LOS RIOS.
Ciudad. -

De mis consideraciones:

Reciba un cordial saludo por parte de la Facultad de Administración, Finanzas e Informática de la Universidad Técnica de Babahoyo, donde formamos profesionales altamente capacitados en los campos de Tecnologías de la Información y de Administración, competentes, con principios y valores cuya practica contribuye al desarrollo integral de la sociedad, es por ello que buscamos prestigiosas Empresas e Instituciones Públicas y Privadas en las cuales nuestros futuros profesionales tengan la oportunidad de afianzar sus conocimientos.

El señor **VALENTIN GREGORIO SOLORZANO PALMA,** con cédula de identidad No. **120879405-5** estudiante de la Carrera de Ingeniería en Sistemas de Información, matriculado en el proceso de titulación en el periodo NOVIEMBRE 2023 – ABRIL 2024, trabajo de titulación modalidad examen de carácter complexivo, previo a la obtención del grado académico profesional universitario de tercer nivel como INGENIERO EN SISTEMAS DE INFORMACIÓN, solicita por intermedio del Decanato de esta Facultad el debido permiso para realizar su Estudio de Caso con su tema: **"ANÁLISIS DE VULNERABILIDAD Y PROPUESTA DE ASEGURAMIENTO DE LA SEGURIDAD DE LA INFORMACIÓN EN LA INFRAESTRUCTURA TECNOLÓGICA DE LA EMPRESA INTERNET LOS RÍOS".**

Atentamente,

Lcdo. Eduardo Galeas Guijarro, MAE.
DECANO

c.c: Archivo

Recibido
27 febrero 2024
9:00 am

Av. Universitaria Km 2 ½ vía Montalvo. Teléfono (05) 2572024 e-mail: decanatofafi@utb.edu.ec	Elaborado por: Ing. Marilyn Coloma Aguilar	Revisado por: Lcdo. Eduardo Galeas Guijarro, MAE

Vinces, 24 de febrero de 2024

Magister

Eduardo Galeas Guijarro

DECANO DE LA FACULTAD DE ADMINISTRACION FINANZAS E INFORMATICA

En su despacho.

De mis consideraciones:

Yo **EDUARDO GUSTAVO MORAN CABELLO** representante legal de la empresa "Interne Los Ríos" con cedula de identidad **120312437-3** permito que el estudiante **VALENTIN GREGORIO SOLORZANO PALMA** con cedula de identidad **120879405-5** pueda realizar su estudio de caso con el tema: **"ANALISIS DE VULNERAVILIDAD Y PROPUESTA DE ASEGURAMIENTO DE LA SEGURIDAD DE LA INFORMACION EN LA INFRAESTRUCTURA TECNOLOGICA DE LA EMPRESA INTERNET LOS RIOS"**

Atentamente,

Sr. Eduardo Gustavo Moran Cabello

C. I. 120312437-3

RECIBIDO
UNIVERSIDAD TÉCNICA DE BABAHOYO
SECRETARIA FAFI
28-02-24 08:13
FECHA: HORA:

ENCUESTA REALIZADA A UN TRABAJADOR	
1. ¿Han tenido alguna vez un ataque informático?	De momento no hemos tenido indicios de ataques informáticos
2. ¿Conoce usted sobre las vulnerabilidades informáticas que tiene la empresa?	No, no conozco sobre las vulnerabilidades que pueda haber en la empresa
3. ¿Han realizado pruebas de pentesting en la empresa?	Han realizado, pero han sido pocas veces, incluso seria solo al inicio cuando se fundó la empresa.
4. ¿Usan software de encriptación?	No usamos software de encriptación de datos.
5. ¿Tiene conocimiento sobre las clases de peligros informáticos que existen?	Tengo conocimiento de algunos básicos, pero los demás no se.
6. ¿Cuántos sistemas operativos se maneja la empresa?	Se maneja con 2 sistemas operativos, Windows 10 y Linux en máquinas virtuales.
7. ¿Sabe usted sobre el ethical hacking?	Eh escuchado hablar sobre ello, pero tengo pocos conocimientos sobre el tema.
8. ¿Tiene conocimientos sobre softwares que les permitan hacer pruebas de vulnerabilidades?	No tengo conocimiento sobre ello, pero si me gustaría estar al tanto de ello.
9. ¿Usted invertiría en unos de estos softwares para la implementación de estos en la empresa?	Si invertiría, el poder conocer sobre los problemas con anticipación evitaría que tengamos perdidas.
10. ¿Estaría dispuesto en hacer capacitaciones sobre temas de seguridad informática?	SI, claro que lo haría