CORPORACIÓN UNIVERSITARIA UNITEC	RESUMEN ANALÍTICO DE INVESTIGACIÓN (RAI)		
	Código:	**Fecha:**	**Versión No.**

Fecha de elaboración: 10.04.2023 [del RAI]			
Tipo de documento	TID:	Obra Creación:	Proyecto Investigación: X
Título	**Evaluación De Riesgos Y Vulnerabilidades Informáticas Que Se Presentan En Una Organización Del Sector Educativo**		
Autor(es)	**CRISTHIAN FERNANDO SUAREZ ANTOLINEZ** **EDWARD CAMILO SANCHEZ GARCIA SANCHEZ**		
Tutor(es)	**FABIO ANTONIO GONZALEZ MENDIETA**		
Fecha de finalización	10.04.2023 [del proyecto de investigación]		
Temática	**SEGURIDAD INFORMATICA**		
Tipo de investigación	**Cuantitativa**		

Resumen

Este proyecto de investigación identifica y evalúa las vulnerabilidades y riesgos que afronta la institución educativa respecto a la seguridad informática. Mediante el método cuantitativo se examina las políticas de seguridad y determina si las herramientas o lineamientos que usa la institución están acordes a reducir las brechas identificadas. Se establecen parámetros y se propone la actualización de sus políticas de seguridad, con esto se desea ayudar a mitigar o eliminar las brechas de seguridad físicas y lógicas que se encontraron en la institución. Con encuestas se revisaron los roles y tareas de cada uno de los integrantes del área de sistemas. Se pretende estructurar y educar a todos los actores que intervienen en la institución ya sea colaboradores directos del área de sistemas, directivas, administrativos y usuarios que utilicen los servicios informáticos de la institución.

Palabras clave

Análisis de Riesgos, Confidencialidad, Control Informático, Disponibilidad, Integridad, Políticas de Seguridad, Riesgos, Seguridad Informática, Sistema de Gestión, Seguridad en las Redes, Vulnerabilidades Físicas, Vulnerabilidades Lógicas.

Planteamiento del problema

En la actualidad el bien más preciado para todas las organizaciones son los datos, sin importar que tipo y clase de información manejen, la seguridad e integridad de esta es lo primordial para el funcionamiento y continuidad del negocio. No todas las organizaciones cuentan con el presupuesto y el personal especializado e idóneo para crear políticas de seguridad y realizar estudios de vulnerabilidad de la información ya sean físicas o lógicas.

Todas las instituciones ya sean grandes, medianas o pequeñas, nuevas o existentes, tienen probabilidades de sufrir perdida de información y ataques informáticos, porque no cuentan con herramientas de monitoreo o referentes suficientes para crear políticas de seguridad y sistemas que ayuden a mitigar todas las vulnerabilidades o riesgos que se encuentren.

Se desea encontrar las vulnerabilidades y medir el nivel de riesgo que puede sufrir esta organización. Implementar herramientas de bajo valor adquisitivo para monitorear sus redes (redes LAN, WIFI), sus terminales de trabajo (equipos de cómputo, servidores) y sus datos masivos. Implementar políticas de seguridad, estándares informáticos organizacionales para realizar en estas.

Pregunta

¿Cómo evaluar mediante un modelo de investigación cuantitativo las vulnerabilidades y riesgos que tienen una organización del sector educativo en sus diferentes sistemas informáticos como datos masivos, redes y hardware?

Objetivos

Objetivo General

- Evaluar las vulnerabilidades y riesgos que tienen una organización del sector educativo en los sistemas de información, infraestructura de red y datos masivos.

Objetivos Específicos

- Identificar los tipos de vulnerabilidades y riesgos presentes en la organización.
- Estructurar un informe de mitigación de vulnerabilidades y riesgos que se presentan dentro de una organización.
- Analizar que tipos de software se adecuan para poder identificar vulnerabilidades y riesgos acordes a la organización.
- Estructurar las políticas de seguridad de la institución.

Marco teórico

Resuma únicamente los principales referentes teóricos o artísticos que siguió su trabajo. Señale los números de las páginas de su documento en los que se encuentra la información completa.

Páginas 14-20

Según (Romero, Figueroa, & Vera, 2018)*, "Los datos son valores, números, medidas, textos, documentos en bruto, la información es el valor de esos datos, es lo que aporta conocimiento";* la unión de los datos se convierte en información la cual se ha convertido en el bien más preciado de todas las organizaciones y es el bien que más se desea proteger.

Los pilares fundamentales de la seguridad de la información son la base de todo el manejo de la información y de ahí su gran importancia. La integridad, la disponibilidad y la confidencialidad actúan como uno para minimizar los riesgos. Por esta razón se debe tener claro en que se basa cada uno de estos pilares.

"La confidencialidad es el pilar que se encarga en que solo el personal autorizado tenga acceso a la información correspondiente, con esto se pretende garantizar que cada individuo o sistema tenga acceso a los recursos que necesita para ejecutar sus tareas o labores" (Costas, 2011).

"Consiste en asegurarse de que la información no se pierde ni se ve comprometida voluntaria e involuntariamente, el hecho de trabajar con

información errónea puede ser tan nocivo para las actividades como perder la información, de hecho, si la manipulación de la información es lo suficientemente sutil puede causar que se arrastre una cadena de errores acumulativos y que sucesivamente se tome decisiones equivocadas" (Costas, 2011).

La información debe estar disponible en todo momento para el usuario o sistema que la requiera.

"Se debe implementar las medidas necesarias para que tanto la información como los servicios estén disponibles, por ejemplo, un ataque distribuido de denegación de servicio o DDoS puede dejar inutilizada una tienda online impidiendo que los clientes accedan a la misma y puedan comprar" (Costas, 2011).

Según Campos (2020), para gestionar las vulnerabilidades de los sistemas de informacion nos debemos enforcar en tres tipos de seguridades que son: la seguridad de red, la seguridad de software y la seguridad de hadware.

A) La seguridad de red: es necesaria para evitar que cualquier individuo no autorizado acceda a la información dentro de la red. También evita, controla y mitiga accesos y ataques comunes como:

- Virus, gusanos y troyanos
- Software espía y publicitario
- Ataques de hackers
- Ataques de denegación de servicio
- Intercepción o robo de datos
- Robo de identidad

Según (Antokoletz, 2010), "*Con la ingeniería social no solo se puede obtener acceso a información confidencial de una organización y controlar la infraestructura (servidores redes) también lograr tener un impacto y acceder a cualquier usuario de la red".* La ingeniería social se basa en la confianza. El ingeniero social quiere que la víctima confíe en él por completo, o al menos lo suficiente como para no sospechar que está siendo engañado.

Uno de los principales objetivos de la ingeniería social en el campo organizacional es obtener acceso encubierto a los sistemas de información. Los motivos de tales visitas de búsqueda pueden ser simple curiosidad y autoexamen de ver hasta dónde puedo llegar solo por pasión por lograrlo.

En los últimos años sobre las redes internas de los centros universitarios ocurren fallas o afectaciones a la seguridad del sistema de información, a causa de esto surge la necesidad de realizar estudios, investigaciones para identificar las diferentes formas que ejecutan las personas mal intencionadas para obtener la información de los recursos más importante de las instituciones, sean personal, contraseñas, datos de base de datos así poner en riesgo la seguridad de la información y causen problemas económicos, de reputación y prestigio de las instituciones.

Método

Resuma únicamente los principales elementos metodológicos que empleó en su investigación. Señale los números de las páginas de su documento en los que se encuentra la información completa.

PAGINA 44-45

La siguiente investigación seguirá los parámetros de una metodología cuantitativa, a partir de manejo estadístico descriptivo de la información obtenida y analizada en la organización de educación superior.

La metodología PHVA fue creada por Walter Shewhart en los años 20 y luego popularizada por Edwards Deming de donde toma su nombre más popular, el ciclo de Deming.

Según (Villamil & Moyano Hernandez, 2021), *"El uso del ciclo PHVA en la gestión de proyectos, nace a partir de los beneficios que genera esta herramienta de mejora continua, sobre los procesos de las organizaciones que la aplican; las cuales logran percibir mejoras en un corto plazo con resultados visibles; tales como la reducción de productos defectuosos, la disminución en*

costos y el menor tiempo, aspectos que representan a las variables de la triple restricción que debe sortear cualquier tipo de proyecto".

Además, la herramienta genera el incremento de la productividad, promoviendo la competitividad en el sector propio de la organización. "Por este motivo la integración de esta herramienta, en la gestión de proyectos busca orientar la calidad en los procesos y la toma de decisiones para la gestión de los recursos, el cronograma y los costos, en el desarrollo de diferentes tipos de proyectos." ("ANÁLISIS DEL CICLO PHVA EN LA GESTIÓN DE PROYECTOS, UNA REVISIÓN DOCUMENTAL") Este artículo muestra entonces el enfoque de la literatura expuesta por diferentes autores que han investigado sobre el tema, de forma que se pueda fortalecer dentro de las organizaciones, a las áreas encargadas de la gestión proyectos, con algunos ejemplos de incorporación de esta herramienta en los procesos de gestión anteriormente enunciados.

Planificar: se establecen los objetivos y los procesos necesarios para conseguir resultados según las necesidades de los clientes y la política de seguridad de la organización.

Hacer: se implantan los procesos.

Verificar: se revisan y se evalúan tanto lo servicios como los procesos comprándolos con las políticas, los objetivos y los requisitos de información sobre los resultados.

Actuar: comienzan a emprender acciones para mejorar el rendimiento del Sistema de Gestión Ambiental de forma continua.

Resultados, hallazgos u obra realizada

Presente el resumen de los principales resultados o hallazgos de su investigación o una sinopsis de la obra creada. Señale los números de las páginas de su documento en los que se encuentra la información completa.

PAGINA 49 A 54

Prueba 1. Prueba de penetración:

Reconocimiento pasivo

Objetivo: Identificar

Resultado del comando: Al realizar la consulta al dominio correspondiente podemos evidenciar la fecha de creación, la fecha de expiración, datos de quien registro el dominio, también los DNS que contiene.

¿Cómo podemos usar está información?

•Se pueden tomar los DNS que muestra la consulta para facilitar el reconocimiento y poder intervenir y causar daños.
•Se puede tomar la fecha de expiración del dominio para apoderarse del mismo y poder suplantar el sitio web, con esto se engañaría al visitante y obtener información.

Prueba 2. Reconocimiento pasivo – identificación IP
Reconocimiento pasivo – identificación IP
Objetivo: Reconocer IP
Resultado: Al ingresar el comando nslookup muestra en pantalla la información de la puerta de enlace, también nos enseña la dirección IP del dominio registrado donde se puede enviar los ataques IP.

Prueba 3. Reconocimiento pasivo – Escaneo DNS
Objetivo: Obtener las direcciones de los DNS
Ejecución: dnsrecon -t std -d
Resultado: Al ingresar el comando el escaneo de tipo (-t) estándar (std) al dominio (-d) obtenemos el registro SOA el cual es el encargado de la transferencia de información entre servidores, también evidenciamos que dichos servidores usan seguridad

Prueba 4. Reconocimiento pasivo – Escaneo RED
Objetivo: Mostrar dispositivos conectados a la red
Herramienta: Terminal Kali Linux, comando Nmap
Ejecución: nmap -sP red x.x.x.x/x
Resultado: Nos muestra los diferentes dispositivos conectados a la red interna, donde podemos extraer datos tales como la IP que toma, la dirección MAC y la marca del dispositivo.

Prueba 5 Reconocimiento activo – Escaneo puertos BD
Objetivo: Encontrar puertos abiertos
Herramienta: Terminal Kali Linux
Ejecución: nmap -O X.X.X.X
Resultado: Tres ejecutar el comando en nuestra consola evidenciamos los puertos que se encuentran abiertos y de encontrar alguna de base de datos podrías generar un ataque por ese puerto.

Prueba 6. Reconocimiento activo – Identificación BD
Objetivo: Identificar que se esté ejecutando el GBD
Herramienta: Terminal Kali Linux, Nmap

Ejecución: nmap –sTV –Pn –n –p1433 x.x.x.x
Resultado: Se evidencia el motor de base de datos, versión por donde podemos generar ataques de inyección SQL.

Prueba 7 Escaneo vulnerabilidades – script de auth

Objetivo: Identificar vulnerabilidades
Herramienta: Terminal Kali Linux, Nmap, script auth
Ejecución: nmap –f -sS -sV -script auth x.x.x.x
Resultado: Con esté comando se puede evidenciar el puerto que se tienen permitido el ingreso de usuarios anónimos, también se puede observar si la cuenta de la MYSQL tiene o no contraseña, esté script nos permite realizar análisis de autenticación el cual nos permitirá ver las vulnerabilidades.

Conclusiones
Presente el resumen de las conclusiones a las que llegó. Señale los números de las páginas de su documento en los que se encuentra la información completa.

PAGINA 61 A 62

- Si se ha podido probar la hipótesis de identificar las vulnerabilidades y riesgos que tiene la institución del sector educativo en sus diferentes sistemas informáticos a través de un modelo de investigación cuantitativo. El modelo de investigación cuantitativo es una herramienta útil para identificar las vulnerabilidades y riesgos que tienen una organización del sector educativo en sus diferentes sistemas informáticos y tomar medidas para mejorar su seguridad.
- En conclusión, la evaluación de las vulnerabilidades y riesgos que se realizó en la institución del sector educativo en sus sistemas de información, infraestructura de red y datos masivos es fundamental para garantizar la seguridad y protección de la información de esta y de sus usuarios. Este proyecto ayudara a tomar medidas preventivas para minimizar la probabilidad de incidentes de seguridad y proteger la información crítica de la organización. Es importante destacar que la evaluación de las vulnerabilidades y riesgos no es un único proceso, sino que debe realizarse de forma periódica para garantizar que los sistemas de la organización sigan siendo seguros y estén protegidos contra posibles amenazas.

- Es importante identificar los tipos de vulnerabilidades y riesgos presentes en la organización porque permite tomar medidas preventivas y

correctivas para proteger la integridad, confidencialidad y disponibilidad de los recursos críticos de la institución.

- Al estructurar un informe de mitigación de vulnerabilidades y riesgos proporciona una visión general de los riesgos críticos para la organización y ayuda a establecer prioridades y objetivos de seguridad claros
- En conclusión, existen varias herramientas de código abierto que son accesibles a cualquier persona interesada en aprender sobre seguridad informática y realizar pruebas de penetración.

  Kali Linux es una herramienta importante en el arsenal de cualquier profesional de la seguridad informática ya que permite identificar vulnerabilidades en los sistemas y aplicaciones, así como detectar posibles amenazas y ataques.
- Aprendimos la importancia de analizar y estructurar las políticas de seguridad de la institución para proteger la información, cumplir con las normas y regulaciones, sensibilizar al personal, prevenir incidentes de seguridad y mejorar continuamente la seguridad de la información.

Productos derivados

Referencie los artículos, libros, capítulos de libro, ponencias, etc., que fueron resultado de su proceso investigativo.

Evaluación De Riesgos Y Vulnerabilidades Informáticas Que Se Presentan En Una Organización Del Sector Educativo

CRISTHIAN F. SUAREZ ANTOLINEZ

Cod. 12226021

EDWARD C. GARCIA SANCHEZ

Cod. 12226016

Corporación Universitaria Unitec

Escuela de Ingeniería

Programa de Especialización en Seguridad de la información

Bogotá, Distrito Capital

10 de abril de 2023

Evaluación De Riesgos Y Vulnerabilidades Informáticas Que Se Presentan En Una Organización Del Sector Educativo

CRISTHIAN F. SUAREZ ANTOLINEZ

Cod. 12226021

EDWARD C. GARCIA SANCHEZ

Cod. 12226016

Docente FABIO A. GONZALEZ MENDIETA

Corporación universitaria UNITEC

Especialización seguridad de la información

Seminario de investigación II

Bogotá, Colombia

10 de abril de 2023

Tabla de contenido

Tabla de Figuras

Indicé de Tablas

RESUMEN

Este proyecto de investigación identifica y evalúa las vulnerabilidades y riesgos que afronta la institución educativa respecto a la seguridad informática. Mediante el método cuantitativo se examina las políticas de seguridad y determina si las herramientas o lineamientos que usa la institución están acordes a reducir las brechas identificadas. Se establecen parámetros y se propone la actualización de sus políticas de seguridad, con esto se desea ayudar a mitigar o eliminar las brechas de seguridad físicas y lógicas que se encontraron en la institución. Con encuestas se revisaron los roles y tareas de cada uno de los integrantes del área de sistemas. Se pretende estructurar y educar a todos los actores que intervienen en la institución ya sea colaboradores directos del área de sistemas, directivas, administrativos y usuarios que utilicen los servicios informáticos de la institución.

PALABRAS CLAVES

Análisis de Riesgos, Confidencialidad, Control Informático, Disponibilidad, Integridad, Políticas de Seguridad, Riesgos, Seguridad Informática, Sistema de Gestión, Seguridad en las Redes, Vulnerabilidades Físicas, Vulnerabilidades Lógicas.

1. PLANTEAMIENTO DEL PROBLEMA

De acuerdo con Castro (2022), en la actualidad el bien más preciado para todas las organizaciones son los datos, sin importar que tipo y clase de información manejen, la seguridad e integridad de esta es lo primordial para el funcionamiento y continuidad del negocio. No todas las organizaciones cuentan con el presupuesto y el personal especializado e idóneo para crear políticas de seguridad y realizar estudios de vulnerabilidad de la información ya sean físicas o lógicas.

Todas las instituciones ya sean grandes, medianas o pequeñas, nuevas o existentes, tienen probabilidades de sufrir perdida de información y ataques informáticos, porque no cuentan con herramientas de monitoreo o referentes suficientes para crear políticas de seguridad y sistemas que ayuden a mitigar todas las vulnerabilidades o riesgos que se encuentren.

Se desea encontrar las vulnerabilidades y medir el nivel de riesgo que puede sufrir esta organización. Implementar herramientas de bajo valor adquisitivo para monitorear sus redes (redes LAN, WIFI), sus terminales de trabajo (equipos de cómputo, servidores) y sus datos masivos. Implementar políticas de seguridad, estándares informáticos organizacionales para realizar en estas.

1.1. LIMITACIONES

Al no haber sido implementado antes de este proyecto una política de seguridad clara y concisa, la institución tiene un vacío en la seguridad de la información el cual es mitigado con la correcta adaptación de este proyecto cuya limitante es el factor económico destinado para la ejecución de este, de igual manera se realiza la respectiva entrega de la documentación a la junta, con el fin de que ser aprobada y ejecutada.

Para las intervenciones en la ejecución de este mecanismo serán proyectados solo si hay riesgos que argumenten una observación de manera precisa, de no ser así, esto conllevara a un fracaso en relación con el dinero que se utiliza en esto.

2. JUSTIFICACION

Según Castro (2022), Las organizaciones educativas de educación superior buscan tener un alto nivel tecnológico para lograr un desarrollo más equilibrado en su crecimiento, dependiendo su énfasis, sus recursos van enfocados en gran porcentaje a otra clase de desarrollos y no cuentan con el capital suficiente ni necesario para realizar la inversión completa de implementaciones de arquitecturas y sistemas de información que controlen las vulnerabilidades y limiten los riesgos de estas. Tal vez en su presupuesto no está contemplado contratar personal especializado e idóneo para implementar políticas de seguridad o estándares que lleguen a resguardar la información y adquirir un Software de elevado costo para evaluar las vulnerabilidades físicas, lógicas, de actualización y desarrollo.

Todas las empresas u organizaciones por más pequeñas que sean necesitan contar con herramientas que ayuden a mitigar los riesgos o vulnerabilidades de perdida de información.

Con este estudio de vulnerabilidades deseamos dar un aporte metodológico para reducir el riesgo con los que cuentan estas instituciones y resolver una necesidad con poca inversión y si muy sustanciosa para la continuidad y protección de la información del negocio.

3. PREGUNTA PROBLEMA

¿Cómo evaluar mediante un modelo de investigación cuantitativo las vulnerabilidades y riesgos que tienen una organización del sector educativo en sus diferentes sistemas informáticos como datos masivos, redes y hardware?

4. OBJETIVOS

4.1. Objetivo General

- Evaluar las vulnerabilidades y riesgos que tienen una organización del sector educativo en los sistemas de información, infraestructura de red y datos masivos.

4.2. Objetivos Específicos

- Identificar los tipos de vulnerabilidades y riesgos presentes en la organización.
- Estructurar un informe de mitigación de vulnerabilidades y riesgos que se presentan dentro de una organización.
- Analizar que tipos de software se adecuan para poder identificar vulnerabilidades y riesgos acordes a la organización.
- Estructurar las políticas de seguridad de la institución.

5. MARCO REFERENCIAL

5.1.1. MARCO TEORICO

5.1.1. Principios de la seguridad informática

Según (Romero, Figueroa, & Vera, 2018)*, "Los datos son valores, números, medidas, textos, documentos en bruto, la información es el valor de esos datos, es lo que aporta conocimiento";* la unión de los datos se convierte en información la cual se ha convertido en el bien más preciado de todas las organizaciones y es el bien que más se desea proteger.

Los pilares fundamentales de la seguridad de la información son la base de todo el manejo de la información y de ahí su gran importancia. La integridad, la disponibilidad y la confidencialidad actúan como uno para minimizar los riesgos. Por esta razón se debe tener claro en que se basa cada uno de estos pilares.

La Figura 1. Tres pilares de la seguridad de la información.

Figura 1. Pilares de seguridad

Fuente: (Romero, Figueroa, & Vera, 2018)

Confidencialidad:

"La confidencialidad es el pilar que se encarga en que solo el personal autorizado tenga acceso a la información correspondiente, con esto se pretende garantizar que cada individuo o sistema tenga acceso a los recursos que necesita para ejecutar sus tareas o labores" (Costas, 2011).

A continuación, se mencionan las características principales que ayudan a gestionar la confidencialidad:

• Autenticación de usuarios

• Gestión de privilegios

• Cifrado de información

La integridad

"Consiste en asegurarse de que la información no se pierde ni se ve comprometida voluntaria e involuntariamente, el hecho de trabajar con información errónea puede ser tan nocivo para las actividades como perder la información, de hecho, si la manipulación de la información es lo suficientemente sutil puede causar que se arrastre una cadena de errores acumulativos y que sucesivamente se tome decisiones equivocadas" (Costas, 2011).

Para gestionar la integridad de la información se debe contemplar los siguientes aspectos:

- Auditar los sistemas para implementar políticas de auditorías que registre quien hace que, cuando y con qué información.
- Copias de seguridad
- Monitorear el tráfico de la red.
- Implementar sistemas de control de cambios, algo tan sencillo como por ejemplo comprobar los resúmenes de los archivos de información almacenados en sistema para comprobar si cambian o no.

Disponibilidad

La información debe estar disponible en todo momento para el usuario o sistema que la requiera.

"Se debe implementar las medidas necesarias para que tanto la información como los servicios estén disponibles, por ejemplo, un ataque distribuido de denegación de servicio o DDoS puede dejar inutilizada una tienda online impidiendo que los clientes accedan a la misma y puedan comprar" (Costas, 2011).

Para este propósito se implementan políticas de control como:

• El acuerdo de nivel de servicio o (SLA).

• Balanceadores de carga de tráfico para minimizar el impacto de DDoS.

• Copias de seguridad para restauración de información perdida.

• Disponer de recursos alternativos a los primarios.

Según (Carpentier, 2016) , *"Indica que el uso de sistemas de información implica establecer normas y procedimientos aplicados al uso y sistemas de información ante posibles amenazas como: Elaborar varias normas y procedimientos, Definición de acciones que deben emprender las personas y Definición del perímetro que se va a afectar".*

5.1.2. Tipos de Seguridad

Según Campos (2020), para gestionar las vulnerabilidades de los sistemas de informacion nos debemos enforcar en tres tipos de seguridades que son: la seguridad de red, la seguridad de software y la seguridad de hadware.

A) La seguridad de red: es necesaria para evitar que cualquier individuo no autorizado acceda a la información dentro de la red. También evita, controla y mitiga accesos y ataques comunes como:

• Virus, gusanos y troyanos

• Software espía y publicitario

• Ataques de hackers

• Ataques de denegación de servicio

• Intercepción o robo de datos

• Robo de identidad

B) La seguridad de software protege el software contra ataques maliciosos de hackers y otros riesgos, las buenas prácticas de ingeniería de software implican pensar en la seguridad al principio del ciclo de vida del desarrollo de software.

C) La seguridad de hardware según (Campos, 2020) *"Garantizan la confianza, integridad y autenticidad de los circuitos integrados (IC) y los sistemas electrónicos. Las soluciones de seguridad de hardware pueden venir en forma de dispositivos de red: los cortafuegos, enrutadores e incluso conmutadores pueden funcionar para proporcionar un cierto nivel de seguridad. En general, estos dispositivos son computadoras dedicadas que ejecutan software propietario".*

5.1.3. Ingeniería social

Según (Antokoletz, 2010), "*Con la ingeniería social no solo se puede obtener acceso a información confidencial de una organización y controlar la infraestructura (servidores redes) también lograr tener un impacto y acceder a cualquier usuario de la red".* La ingeniería social se basa en la confianza. El ingeniero social quiere que la víctima confíe en él por completo, o al menos lo suficiente como para no sospechar que está siendo engañado.

Uno de los principales objetivos de la ingeniería social en el campo organizacional es obtener acceso encubierto a los sistemas de información. Los motivos de tales visitas de búsqueda pueden ser simple curiosidad y autoexamen de ver hasta dónde puedo llegar solo por pasión por lograrlo.

5.1.4. Superficie de ataque

De acuerdo con Romero, et al, (2018), Todos los elementos que integran una red son susceptibles a recibir ataques, todos estos elementos tienen vulnerabilidades y pueden ser explotadas por un incidente natural o por un ataque deliberado.

Elementos que conforman una superficie de ataque:

- Sistemas operativos, aplicaciones y fireware
- Router, switch o firewall.
- Sistemas de almacenamiento en red de la infraestructura.
- Computadoras, servidores.
- Las personas que usan y administran los recursos tecnológicos.

La Figura 2 muestra el detalle de superficie de ataque de la infraestructura de TI.

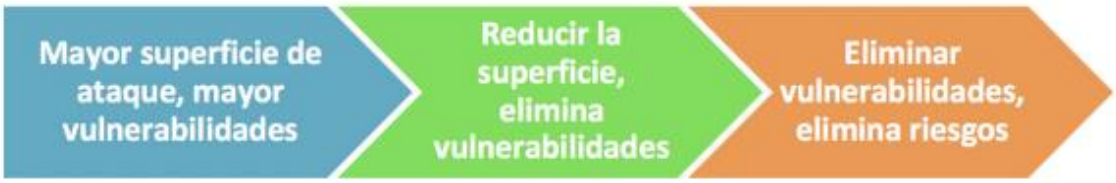
Figura 2. Superficie de ataque en infraestructura de TI.

Fuente: (Romero, Figueroa, & Vera, 2018)

Según Romero (2018), entre mas elementos compongan una red mas probabilidades hay que existan vulnerabilidades y los riesgos pueden aumentar.

La Figura 3. muestra los riesgos en la superficie de ataque.

Figura 3. Superficie de ataque vs riesgos.



Fuente: (Romero, Figueroa, & Vera, 2018)

Al analizar las diferentes superficies de ataque se puede resaltar dos formas de ataque, el ataque pasivo y el ataque activo.

El ataque pasivo de acuerdo con (Romero, et al, 2018), *"Consiste en monitorear al sujeto atacado, es un ataque no invasivo ya que no afecta a la infraestructura, pero monitoriza lo que esta puede almacenar o transmitir, incluso información que es directamente pública. Para este tipo de ataques se pueden atizar técnicas de monitorización de tráfico en busca de documentos, contraseñas o fuentes abiertas de información conocidas como OSINT".*

Según (Romero, et al, 2018) *"Los ataques pasivos están orientados exclusivamente a obtener información que puede ser suficiente en sí misma o ser empleada para posteriores ataques activos, es por esto, que identificar un ataque pasivo puede poner en alerta al usuario respecto a uno activo".*

La Figura 4 muestra los elementos del ataque pasivo.

Figura 4. Fuentes del ataque pasivo.

Fuente: (Romero, Figueroa, & Vera, 2018)

5.1.5. Vulnerabilidades

"Las vulnerabilidades son fallas en los sistemas, no son puertas abiertas diseñadas de liberadamente, sino errores de diseño, configuración o implementación que generan oportunidades de ataque, es decir que hacen viable una amenaza". ("Introducción a la Seguridad Informática y el Análisis de ... - StuDocu") (Romero, et al, 2018).

Se puede segmentar y analizar las distintas vulnerabilidades que tiene cada superficie de ataque.

Vulnerabilidades de software

Está constituido por aplicaciones, páginas web, servicios como NFTP, TELNET entre otros. Las vulnerabilidades que se presentan son fallas en la programación o compilación de los programas que se ejecutan en los computadores o en los servidores, ocasionando el mal funcionamiento del software o fallos en el sistema.

Según Romero, et al, (2018), Las vulnerabilidades lógicas afectan directamente la infraestructura y desarrollo de estos aplicativos o software y se debe complementar la configuración, actualización y desarrollo. una de esta recomendación conlleva a minimizar el uso de software instalado en los equipos de cómputo y servidores, además de ser software legal, verificar que estos contengas todos los parches y actualizaciones que referencia su desarrollador.

De acuerdo Romero, et al, (2018), Las configuraciones en el sistema operativo, aplicaciones del servidor, firewalls y la infraestructura perimetral son elementos importantes que pueden tener vulnerabilidades si no se gestionan adecuadamente. La falta de actualización de los sistemas también puede ser un problema común, ya que las vulnerabilidades pueden aparecer y ser explotadas por los atacantes.

Vulnerabilidades de Hardware

"Todo Hardware de la infraestructura está o puede estar expuesto como dispositivo en sí mismo, por sus puertos y protocolos de comunicaciones, aplicaciones e interfaces" (Romero, et al, 2018).

En este contexto, las amenazas naturales como el envejecimiento de los equipos o los desastres como robos, incendios o inundaciones pueden afectar significativamente la superficie de ataque. Además, los ataques al hardware pueden ocurrir a través de la red o mediante la manipulación del medio físico de transmisión.

Para reducir la superficie de ataque, es necesario proteger físicamente los equipos mediante la instalación de medidas de seguridad, como controles de acceso y sistemas de vigilancia para evitar incidentes y sabotajes. También es importante implementar políticas de seguridad adecuadas para minimizar el riesgo de ataques físicos.

Además, se deben tomar medidas para proteger los sistemas de comunicación inalámbrica, como la implementación de técnicas de encriptación y la configuración adecuada de los dispositivos de red para evitar interrupciones y ataques de perturbadores de señal.

En general, la protección física y de red adecuada es esencial para reducir la superficie de ataque y minimizar el riesgo de vulnerabilidades y ataques a los sistemas críticos y la infraestructura de una organización.

Se debe configurar los equipos cerrando todo puerto innecesario y deshabilitando cualquier protocolo de comunicación no pertinente, en el entorno de red se puede desplegar firewalls, sistemas de detección de intrusión y sistemas de gestión y balanceo de carga de tráfico. Al igual que con el software se debe mantener el firmware actualizado de los equipos y evitar que personal no autorizado pueda manipular su configuración.

Por ultimo las vulnerabilidades que corresponden o hacen referencia al recurso humano según (Romero, et al, 2018), *“Es la última superficie de ataque que pueden actuar contra los intereses de la organización por descontento, error, engaño o coacción. Además de implementar y exigir el cumplimiento de protocolos de actuación, es aconsejable implementar sistemas de registro y auditoría para verificar quién hace qué y cuándo”.*

5.1.6. Escáneres de vulnerabilidades

A continuación, se enlista una lista de estas herramientas para evaluar las vulnerabilidades de la red.

Según Zambrano (2018), En el mercado existe una gran variedad de escáner de vulnerabilidades. En su gran mayoría son plataformas de pago, pero existen otros de código abierto o libres que se pueden utilizar sin restricción alguna.

Kali Linux Está disponible como una distribución de Linux gratuita y se puede descargar desde el sitio web oficial de Kali Linux. es una distribución de Linux basada

en Debian diseñada específicamente para pruebas de penetración y evaluación de vulnerabilidades. Es una herramienta popular utilizada por profesionales de la seguridad y hackers éticos para realizar pruebas de seguridad en redes y sistemas. Viene con una amplia variedad de herramientas de seguridad integradas, incluyendo herramientas de escaneo de vulnerabilidades, herramientas de análisis de red, herramientas de análisis de código, herramientas de pruebas de penetración y muchas otras. La distribución es altamente personalizable y se puede adaptar para adaptarse a las necesidades específicas del usuario.

Acunetix es una herramienta de pago, es un escáner de vulnerabilidades web utilizado para detectar y administrar debilidades de seguridad en aplicaciones web. Está diseñado para detectar automáticamente vulnerabilidades comunes como la inyección SQL, el cross-site scripting (XSS) y otros.

Netsparker es una herramienta de pago que nos ayuda con el escaneo de vulnerabilidades web, se utiliza para identificar y remediar vulnerabilidades en aplicaciones web y sitios web.

ProxyStrike es una herramienta de código abierto que se ejecuta en Linux y unix. Es una herramienta de prueba de penetración de red que se utiliza para evaluar la seguridad de una red mediante la identificación de vulnerabilidades y la explotación de ellas. su principal función es interceptar el tráfico de red que pasa entre el cliente y el servidor, permitiendo a los usuarios identificar y analizar las vulnerabilidades de seguridad.

Nessus se ejecuta en sistemas operativos Windows, Linux y Mac OS X, y es compatible con una amplia variedad de dispositivos de red, incluyendo routers, switches, firewalls y dispositivos móviles. También se integra con otros sistemas de gestión de vulnerabilidades y software de seguridad para proporcionar una solución completa de gestión de vulnerabilidades. La herramienta está disponible en diferentes versiones, incluyendo una versión gratuita y varias versiones comerciales con diferentes características y capacidades de escaneo.

Nexpose está disponible en diferentes versiones, incluyendo una versión gratuita y varias versiones comerciales con diferentes características y capacidades de escaneo. es una herramienta de escaneo de vulnerabilidades de red que se utiliza para identificar y evaluar las vulnerabilidades de seguridad en sistemas y redes. Es una herramienta de seguridad de red de alta calidad que es utilizada por profesionales de la seguridad para evaluar la seguridad de la infraestructura de red.

5.1.7. Tipos de ataques

En los últimos años sobre las redes internas de los centros universitarios ocurren fallas o afectaciones a la seguridad del sistema de información, a causa de esto surge la necesidad de realizar estudios, investigaciones para identificar las diferentes formas que ejecutan las personas mal intencionadas para obtener la información de los recursos más importante de las instituciones, sean personal, contraseñas, datos de base de datos así poner en riesgo la seguridad de la información y causen problemas económicos, de reputación y prestigio de las instituciones.

Por esto a continuación se hablará un poco de los ataques más comunes que se pueden encontrar a nivel de redes de datos.

Envenenamiento ARP

Según Pérez (2005), El protocolo ARP es esencial en las redes de comunicación, ya que se encarga de la resolución de direcciones MAC para transmitir datos en redes Ethernet. Sin embargo, esta importante función también puede ser explotada por atacantes.

ARP Spoofing:

Respecto a Pérez (2005), Este tipo de ataque consiste en falsificar las respuestas de ARP para hacer que un dispositivo de red envíe datos a un destinatario equivocado, lo que podría permitir a un atacante interceptar y manipular la información transmitida. Por lo tanto, es importante que los administradores de red tomen medidas para protegerse contra este tipo de vulnerabilidad del protocolo ARP.

Ataque Man-in-the-Middle

Para Narvaez & Romero (2016), es un tipo de ataque en el que un atacante intercepta y manipula las comunicaciones entre dos partes que creen estar comunicándose directamente entre sí. En este tipo de ataque, el atacante se sitúa entre la víctima y el destino y actúa como intermediario, recibiendo y reenviando información entre ambos extremos.

Ataque de denegación de servicio (DoS)

Según Narvaez & Romero (2016), Un ataque de denegación de servicio (DoS) es un tipo de ataque informático que tiene como objetivo inundar un sistema o red con tráfico malicioso o solicitudes, lo que provoca una sobrecarga en los recursos y una interrupción del servicio para los usuarios legítimos. El objetivo principal del ataque de denegación de servicio es impedir que los usuarios legítimos puedan acceder a los servicios o recursos en línea.

Phishing

Según Leguizamon, (2015), es una técnica de ingeniería social en la que un atacante intenta engañar a una persona para que revele información confidencial, como contraseñas, datos bancarios o información personal, haciéndose pasar por una entidad legítima, como un banco, una empresa o una organización gubernamental.

Ataques de día cero

De acuerdo con Toro & Guisao (2014), es un tipo de ataque informático que explota una vulnerabilidad de seguridad previamente desconocida en un software o sistema operativo, lo que significa que el desarrollador no ha tenido tiempo para crear un parche o actualización de seguridad para solucionar el problema.

Errores web

Para (Cañón, 2015), "*Otros tipos de vulnerabilidades son las WEB, aquí simple y sencillamente se tiene errores de validación de input, Scripts inseguros, errores de configuración de aplicaciones web, entre algunas otras situaciones, que a final de cuenta todos y cada uno de esos errores son los medios para algún ataque de XSS*

(Cross Site Scripting) o inyección SQL". ("Introducción a la Seguridad Informática y el Análisis de ... - StuDocu") (Romero, et al, 2018).

Según Cañón (2015), la inyección por SQL es uno de los ataques más utilizados en la actualidad, consiste en acceder a las tablas de la base de datos incluyendo información sobre el usuario y su clave, este ataque está caracterizado porque es fácil de ejecutar porque modifica la cadena de consulta SQL hacia la base de datos.

También (Cañón, 2015), *"Indica que los ataques tipos Cross Site Scripting consisten en infectar un sitio web mediante scripts maliciosos con el objetivo de obtener acceso a una determinada cuenta de usuario".*

Detección de vulnerabilidades

La detección de vulnerabilidades es un proceso importante para la seguridad de un sistema, y existen diferentes herramientas y métodos para realizarla. Los escáneres de vulnerabilidades son una herramienta valiosa para encontrar rápidamente posibles vulnerabilidades en un sistema. Sin embargo, también es importante realizar análisis manuales y consultas de información para detectar vulnerabilidades que los escáneres no puedan encontrar. La combinación de diferentes herramientas y métodos de detección de vulnerabilidades puede mejorar significativamente la seguridad de un sistema.

5.1.8. Métodos de escaneo de vulnerabilidades

A continuación, se mencionan varios métodos de escaneo para analizar las vulnerabilidades:

Caja blanca

Según Campos (2020), el método de escaneo de caja blanca implica tener acceso total a la red y a los sistemas que se quieren analizar, como un usuario legítimo con ciertos privilegios. Esto permite que el equipo de auditoría pueda realizar una revisión exhaustiva de todos los sistemas y servicios disponibles, y evaluar la seguridad de los mismos desde una perspectiva interna.

Al tener acceso como un usuario legítimo, el equipo de auditoría puede realizar pruebas de vulnerabilidades en todos los sistemas y servicios disponibles, utilizando diversas herramientas y técnicas de análisis. Además, al tener acceso a los privilegios adecuados, pueden verificar si es posible realizar alguna acción adicional que pudiera comprometer la seguridad del sistema.

Caja negra

Según Campos (2020), se enfoca en encontrar vulnerabilidades en sistemas y redes sin tener información detallada sobre ellos, como una dirección IP o un nombre de empresa. En este método, los analistas buscan recopilar la mayor cantidad de información posible sobre la red y los sistemas dentro del alcance del análisis, utilizando herramientas de escaneo y otras técnicas de recopilación de información.

Una vez que se ha recopilado la información, se busca identificar posibles vulnerabilidades en los sistemas y servicios que se han descubierto. En este proceso, se pueden utilizar diversas herramientas y técnicas de análisis, incluyendo pruebas de penetración (pentesting) para probar la explotación de las vulnerabilidades.

Remediación de vulnerabilidades

las vulnerabilidades es una parte fundamental del proceso de seguridad de la información. A continuación, se detallan algunos pasos que se pueden seguir para remediar las vulnerabilidades identificadas:

- Priorizar las vulnerabilidades: es importante clasificar las vulnerabilidades según su nivel de criticidad y prioridad. Las vulnerabilidades críticas que pueden tener un impacto significativo en la seguridad del sistema deben ser atendidas primero.
- Establecer un plan de acción: una vez que se han priorizado las vulnerabilidades, se debe establecer un plan de acción para remediarlas. Este plan debe incluir los pasos necesarios para corregir las vulnerabilidades y los plazos para hacerlo.
- Aplicar parches y actualizaciones: en muchos casos, las vulnerabilidades se pueden remediar mediante la aplicación de parches y actualizaciones

proporcionados por el fabricante del software. Es importante aplicar estos parches y actualizaciones tan pronto como estén disponibles.

- Configurar correctamente los sistemas y servicios: muchas vulnerabilidades se deben a una configuración incorrecta de los sistemas y servicios. Es importante asegurarse de que todos los sistemas y servicios estén configurados correctamente para minimizar el riesgo de vulnerabilidades.
- Utilizar medidas de seguridad adicionales: además de aplicar parches y actualizar los sistemas, se pueden utilizar medidas de seguridad adicionales para mitigar el riesgo de vulnerabilidades. Por ejemplo, se pueden utilizar firewalls, sistemas de detección de intrusiones y sistemas de prevención de intrusiones.
- Realizar pruebas de penetración: una vez que se han corregido las vulnerabilidades, es importante realizar pruebas de penetración para asegurarse de que las medidas de seguridad implementadas sean efectivas y no haya nuevas vulnerabilidades.

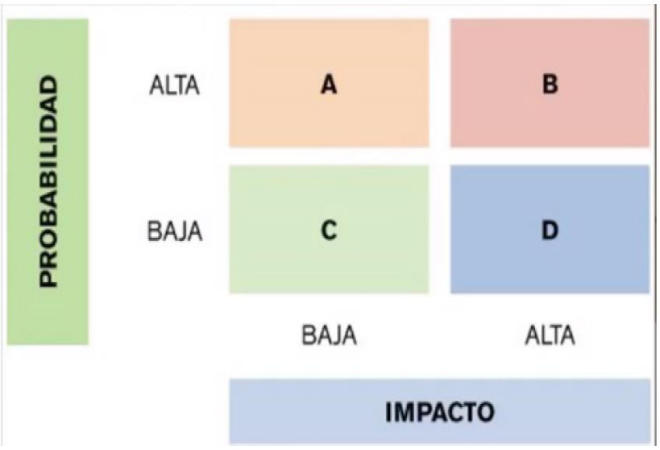
Clasificar y priorizar riesgos

Para Romero, et al (2018), Para clasificar los riesgos, se pueden utilizar diferentes criterios, como la probabilidad de que la vulnerabilidad sea explotada, la severidad del impacto en caso de una explotación exitosa, la criticidad del sistema afectado, entre otros. Estos criterios se pueden combinar en una matriz de riesgos para determinar la prioridad de las acciones de mitigación.

Además, es importante tener en cuenta que la priorización de los riesgos debe ser un proceso continuo y dinámico, ya que las amenazas y vulnerabilidades cambian constantemente. Por lo tanto, se deben revisar regularmente los riesgos y actualizar la clasificación y priorización según sea necesario.

Los escáneres inclusive en ocasiones permiten crear un esquema automáticamente como el que se muestra en la Figura 6, que viene a ser una matriz de riesgos.

Figura 6. Matriz de riesgos.



Fuente: (Romero, Figueroa, & Vera, 2018)

Probar parches y configuraciones

Según Romero, et al (2018), una vez que se ha priorizado las vulnerabilidades, el siguiente paso es aplicar parches y cambios de configuración necesarios para remediarlas. Es importante realizar pruebas antes de implementar los parches en todos los sistemas y dispositivos de la organización, para evitar posibles problemas y fallas. También es crucial descargar los parches de sitios oficiales del fabricante y no de sitios de terceros, para evitar el riesgo de malware o versiones anteriores con errores. Además, los reportes del escáner pueden proporcionar instrucciones detalladas sobre cómo proceder con el parcheo o cambio de configuración requerido.

Aplicar parches y configuraciones

De acuerdo con Romero, et al (2018), Es muy importante implementar los parches y cambios de configuración en todas las máquinas de la red después de haberlos probado en una sola máquina, ya que, dependiendo del tamaño de la red, puede ser un proceso laborioso y complejo, pero es fundamental para mantener la seguridad de la red.

En cuanto a las soluciones automáticas de implementación de parches, estas pueden ser de gran ayuda para automatizar y agilizar el proceso de parcheo en grandes redes. Sin embargo, es importante tener en cuenta que siempre se debe realizar una prueba en una sola máquina antes de implementar el parche en todas las demás, ya que incluso las soluciones automáticas pueden tener errores o incompatibilidades con algunos sistemas.

5.1.9. ANTECEDENTES INVESTIGATIVOS

La seguridad informática constituye un marco importante en todas las organizaciones cuyo objetivo es proteger la integridad, disponibilidad y confidencialidad de datos, son varios los estudios e implementación de proyectos que sean realizado para mitigar los posibles riesgos y amenazas a los que se puede enfrentar las instituciones educativas.

A continuación, se citan estudios que se toman como referente para la elaboración de esta investigación. Estupiñan, Pulido, & Bohada, (2013)

- Análisis de riesgos en seguridad de la información, Ana del Carmen Abril Estupiñán, Jarol Alexander Pulido, John Alexander Bohada Jaime, Fundación Universitaria Juan de Castellanos. (“Análisis de riesgos en seguridad de la información”) Este artículo destaca algunas de las opciones y permite generar argumentos sólidos sobre qué enfoque del análisis de riesgos brinda mejores oportunidades para la toma de decisiones dentro de una organización en comparación con la custodia de la información, que se ha convertido en uno de los activos más importantes del entorno empresarial y significa utilizar y conservar en su totalidad para garantizar la seguridad y la continuidad del negocio.

- Análisis de riesgos y vulnerabilidades de seguridad informática aplicando técnicas de inteligencia artificial orientado a instituciones de educación superior, J.J. Castro Maldonado. En este articulo La seguridad informática ha sido vista como una herramienta importante A la hora de proteger los activos

más importantes de la organización actual, como son los datos y la información, por su valor interno Correcta gestión del conocimiento.

5.2. MARCO CONCEPTUAL

En los últimos años sobre las redes internas de los centros universitarios ocurren fallas o afectaciones de seguridad donde se ven involucrados ciertos activos que hacen parte del sistema de información, a causa de esto surge la necesidad de realizar estudios e investigaciones para identificar las diferentes formas que usan las personas mal intencionadas para obtener información de los recursos de las instituciones donde se puede ver perjudicados datos personales, contraseñas de ingreso al sistema de la compañía, perdida de información de las bases de datos y así poner en riesgo toda la parte del sistema de información donde con lleva a problemas económicos, pérdida de prestigio y de reputación.

Por esto se hablará de algunos conceptos básicos para comprender un poco más el tema.

ATAQUE INFORMATICO

Según Mieres (2009), un ataque informático implica aprovechar ciertas fallas o errores (vulnerabilidades) en el software, hardware o incluso humanos en el entorno informático para obtener beneficios, generalmente de naturaleza económica, socavar la seguridad del sistema y luego impactar directamente en el activo dentro de la compañía.

VULNERABILIDAD

Según Urbina (2016), En informática se define como una brecha o debilidad que encuentran personas mal intencionadas para poder acceder al sistema y robar información así mismo comprometer la seguridad en la red.

VIRUS

Según Gomez (2022), es un programa informático escrito en un lenguaje específico que es capaz de infectar un sistema informático utilizando una variedad de mecanismos de propagación, contiene una sustancia específica que es dañina para el sistema infectado e incluye algunas características de autoprotección para ayudarlo a sobrevivir.

CIBERDELINCUENCIA

Según Arrollo (2020), Se refiere a las actividades delictivas que realizan los individuos contra las computadoras, donde las computadoras son encadenadas para robar información que puede ser utilizada de diferentes formas.

CIBERSEGURIDAD

Según Fonfria (2020), este concepto implica un conjunto de herramientas, políticas, conceptos de seguridad, controles de seguridad, lineamientos y cualquier práctica que se utilice para proteger la seguridad de la información, los activos de la organización y los usuarios.

HACKER

Según Quispe (2009), Persona o individuo con profundo conocimiento en informática donde su objetivo principal es demostrar que puede acceder a una red u ordenador con técnicas específicas, los hay buenos y malos según el escenario y para que sea utilizado.

5.3. MARCO LEGAL Y NORMATIVIDAD

A continuación, se relacionan las leyes y normatividad colombiana actualizadas a septiembre del 2022 donde se involucra el tema de seguridad informática y se crea una jurisprudencia relacionada a este.

El primer documento que hace referencia a temas relacionados con la información de las personas es la Constitución Política de Colombia (Senado de la República de Colombia, 1991), que establece en su artículo 15 lo siguiente:

"Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución". ("Artículo 15 de la Constitución Política de Colombia")

Ley 1266 de 2008 de diciembre 31

"Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se

dictan otras disposiciones". ("Leyes desde 1992 - Vigencia expresa y control de constitucionalidad ...")

Ley 1273 del 5 de enero de 2009

Denominada "De la protección de la información y de los datos" por el congreso de la república, por la cual se modifica el código penal y se crea un nuevo mecanismo legal, cuyo objetivo es sancionar los comportamientos ilícitos asociados a la comisión de los delitos informáticos en el país. Esta ley de delitos informáticos definió nueve tipos penales destinados al bien jurídico de protección de la información y de los datos, y la preservación integral de los sistemas que utilicen las tecnologías de la información y las comunicaciones; el capítulo I trata los atentados contra la Confidencialidad, la Integridad y la Disponibilidad de los datos en Sistemas Informáticos y los tipifica como:

► Acceso abusivo a un sistema informático

► Obstaculización ilegitima de un sistema informático o red de telecomunicación

► Interceptación de datos informáticos

► Daño informático

► Uso de software malicioso

► Violación de datos personales

► Suplantación en sitios web para capturar datos personales

► Circunstancias de agravación punitiva; incrementa la pena según las circunstancias

Ley 1581 de 2012 o ley de protección de datos personales

Por la cual se protegen los datos de las personas dándole carácter legal a su violación, esencialmente por la manipulación y publicación sin autorización del propietario; también quien almacene esta información deberá protegerla de ser extraída pues tanto la organización que la almacena como quien la extrae y la divulga sin autorización pueden ser sancionados con consecuencias legales por la violación de esta ley.

Política Nacional de Seguridad Digital publicado el 11 de abril del 2016, atendiendo al creciente entorno digital para el desarrollo de actividades económicas y sociales en Colombia, evitando así, la materialización de amenazas o ataques cibernéticos con efectos indeseados para el país y sus ciudadanos. Se incorpora la gestión de riesgo en los entornos digitales como estrategia para abordar la seguridad digital bajo cuatro principios fundamentales y cinco dimensiones estratégicas para alcanzar el objetivo fundamental que es*: "fortalecer las capacidades de las múltiples partes interesadas, para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital", (COMPES, 2016).*

5.4. MARCO METODOLOGICO

5.4.1. Tipo de investigación

La siguiente investigación seguirá los parámetros de una metodología cuantitativa, a partir de manejo estadístico descriptivo de la información obtenida y analizada en la organización de educación superior.

La metodología PHVA fue creada por Walter Shewhart en los años 20 y luego popularizada por Edwards Deming de donde toma su nombre más popular, el ciclo de Deming.

5.4.2. Metodología PHVA

Según (Villamil & Moyano Hernandez, 2021), *"El uso del ciclo PHVA en la gestión de proyectos, nace a partir de los beneficios que genera esta herramienta de mejora continua, sobre los procesos de las organizaciones que la aplican; las cuales logran percibir mejoras en un corto plazo con resultados visibles; tales como la reducción de productos defectuosos, la disminución en costos y el menor tiempo, aspectos que representan a las variables de la triple restricción que debe sortear cualquier tipo de proyecto".*

Además, la herramienta genera el incremento de la productividad, promoviendo la competitividad en el sector propio de la organización. "Por este motivo la integración de esta herramienta, en la gestión de proyectos busca orientar la calidad en los

procesos y la toma de decisiones para la gestión de los recursos, el cronograma y los costos, en el desarrollo de diferentes tipos de proyectos." (“ANÁLISIS DEL CICLO PHVA EN LA GESTIÓN DE PROYECTOS, UNA REVISIÓN DOCUMENTAL”) Este artículo muestra entonces el enfoque de la literatura expuesta por diferentes autores que han investigado sobre el tema, de forma que se pueda fortalecer dentro de las organizaciones, a las áreas encargadas de la gestión proyectos, con algunos ejemplos de incorporación de esta herramienta en los procesos de gestión anteriormente enunciados.

La metodología PHVA se describir de la siguiente forma:

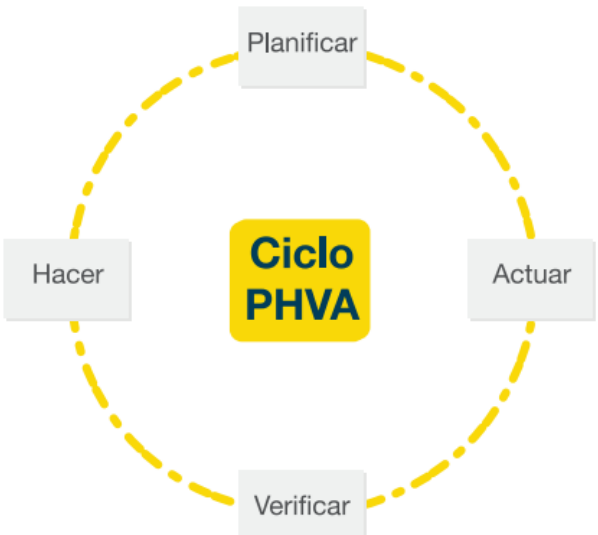
Planificar: se establecen los objetivos y los procesos necesarios para conseguir resultados según las necesidades de los clientes y la política de seguridad de la organización.

Hacer: se implantan los procesos.

Verificar: se revisan y se evalúan tanto lo servicios como los procesos comprándolos con las políticas, los objetivos y los requisitos de información sobre los resultados.

Actuar: comienzan a emprender acciones para mejorar el rendimiento del Sistema de Gestión Ambiental de forma continua.

Figura 7 Ciclos PHVA



Fuente: (GESTIÓN DE RIESGO Y CONTROL INFORMÁTICO, 2023)

5.4.3. Población

La población del siguiente estudio será la sede principal de la organización de educación superior ubicada en la ciudad de Bogotá, donde se realizará el proceso de investigación y la implementación de resultados.

5.4.4. Recolección y análisis de la información

Esta investigación se realizará mediante un hacking ético buscando vulnerabilidades y riesgos que tenga la organización en sistemas de información, infraestructura de red y datos masivos.

5.4.5. Hipótesis

5.4.5.1. HI

Es posible Identificar las vulnerabilidades y riesgos que tienen una organización del sector educativo en sus diferentes sistemas informáticos como: datos masivos, redes y hardware, mediante un modelo de investigación cuantitativo.

5.4.5.2. HO

No es posible Identificar las vulnerabilidades y riesgos que tienen una organización del sector educativo en sus diferentes sistemas informáticos como: datos masivos, redes y hardware, mediante un modelo de investigación cuantitativo.

5.4.6. ALCANCE

El alcance de este proyecto se realizará de una forma explicativa, para este proyecto el diseño y la correcta implementación de estrategia y/o política de seguridad encaminada al acatamiento de las inspecciones con el fin de minimizar las diferentes vulnerabilidades críticas y los posibles riesgos relevantes dentro de la organización, para este caso sectorizada en el sector educativo, ceñidos a los sistemas de información y a la infraestructura de red. Este proyecto contempla la etapa de diseño de la política de seguridad, por lo tanto, depende de la institución llevar a cabo su implementación. Como modelo de trabajo, se efectúa la ejecución de un instrumento de medición y monitoreo para los equipos dentro del Datacenter además de las diferentes áreas de la institución, para todos los dispositivos finales y dispositivos intermedios de red, por supuesto aprovechando cada uno de los aditamentos creados en la política de seguridad; de esta manera el esquema de infraestructura física y lógica que se relaciona como medio de comunicación enfocada al manejo de esta herramienta con la elección de ser diligente en el uso de otros servicios integrados en el área tecnológica.

Dentro de los elementos financieros se establece el valor que la institución considera, conforme con los procesos o servicios que manipula esta.

5.4.7. Técnica e instrumento de Investigación

5.4.7.1. La encuesta

Con el uso de la encuesta pudimos observar el conocimiento sobre seguridad informática y el rol que tiene cada actor o integrante en el equipo de informática y la aplicación que se da a esta dentro de la institución.

La encuesta se aplicó a los principales actores del área de sistemas.

Tabla 1. Personas a las que se le realizo la encuesta

CARGO EN LA INSTIRUCION
Director de sistemas
Coordinador de Sistemas
Analista de sistemas
Analista de sistemas
Analista de sistemas
Analista de sistemas
DBA
Auxiliar de sistemas

Programador

Fuente: Elaboración propia

5.4.7.2. PROCESAMIENTO Y ANALISIS DE LA INFORMACION

Tabla 2. Procesamiento de la información

	SI	NO	NO SABE	NO RESPONDE			
1. ¿Cuentan con políticas de seguridad en la Institución?	7			2			
2. ¿Cuentan con software o consola para administrar el software de seguridad de la institución?	6		3				
3. ¿Cuentan con software o consola para administrar los activos de la compañía?	6		3				
4. ¿Con qué frecuencia actualizas un software antivirus?	a. Se hace automáticamente	b. Al menos dos veces por semana	c. Al menos una vez a la semana	d. Al menos una vez al mes	e. No se hace		
	9						
5. ¿Quién es el responsable de mantener y administrar el software o consola de seguridad de la institución?	Director de sistemas						
	Coordinador de sistemas						
	Área de sistemas						
6. ¿Qué versión de Windows está instalada en los equipos de la institución?	a. Windows 11	b. Windows 10	c. Windows 8	d. Windows 7	e. Otros		
	x	X		X	X		
7. ¿Consideras que han tenido problemas de seguridad donde se vea comprometida la	SI	NO	NO SABE	NO RESPONDE			

información de la institución o usuarios?	5	1		3			
8. ¿Has tenido algún problema con?	a. Malware	b. Virus	c. Gusano	d. Troyano	e. Spyware	f. Adware	g. Ransommware
	x	X					X
9. ¿Actualmente realizan mantenimientos periódicos sobre las computadoras de la empresa?	SI	NO	NO SABE	NO RESPONDE			
	4	1	1	3			
10. Generalmente realizan copias de seguridad de su información	SI	NO	NO SABE	NO RESPONDE			
	4	5					
11. ¿Cada Cuanto se realizan las copias de seguridad?	a. Diario	b. Semanal	c. Mensual	d.no se hace			
	2	2		5			
12. ¿Realizan algún tipo de capacitación en cuanto a seguridad informática hacia los usuarios?	a. Contraseñas	b. Antivirus	c. Firewall	d. Anti Spyware	e. Antimalware	f. Sistema de detección de intrusos	g. Otro:
	x	x					
13. ¿Cuentan con una red VPN en su empresa?	SI	NO	NO SABE	NO RESPONDE			
	9						
14. ¿Generalmente realizan pruebas de seguridad en sus redes?	2		7				
15. La frecuencia con la que realizan las pruebas es	a. Ninguna	b. Cada 3 meses	c. Cada 6 meses	d. Cada año	e. Cada 2 años o mas		
	X	X	X				
16. ¿Qué tan frecuentemente se preparan ante problemas de seguridad?	a. Cada mes	b. Cada trimestre	c. Cada 6 meses	d. Cada año	e. Más de un año		
		X			X		
17. ¿Tiene proyectado invertir en seguridad informática en los siguientes?	f. 3 meses	g. 6 meses	h. 1 año	i. 2 años	j. Más de 2 años		
		X			X		

Fuente: Propia

La información recolectada en esta encuesta nos proporcionó los datos necesarios para saber los conocimientos que tiene cada integrante sobre seguridad informática y el conocimiento que cada uno tiene sobre la infraestructura de la institución y el rol que cada uno ejerce para llevar los lineamientos de seguridad.

5.4.7.3. Hallazgos

- Se logro identificar las falencias que tienen los integrantes del área de sistemas sobre seguridad informática.

- Las políticas de seguridad de la institución están desactualizadas.
- La inversión que se realiza en el campo de la seguridad informática está limitada.
- Los roles de cada integrante del grupo de sistemas no esta definido para seguir los lineamientos de seguridad de la institución.

6. RESULTADOS

6.1. Prueba 1. Prueba de penetración:

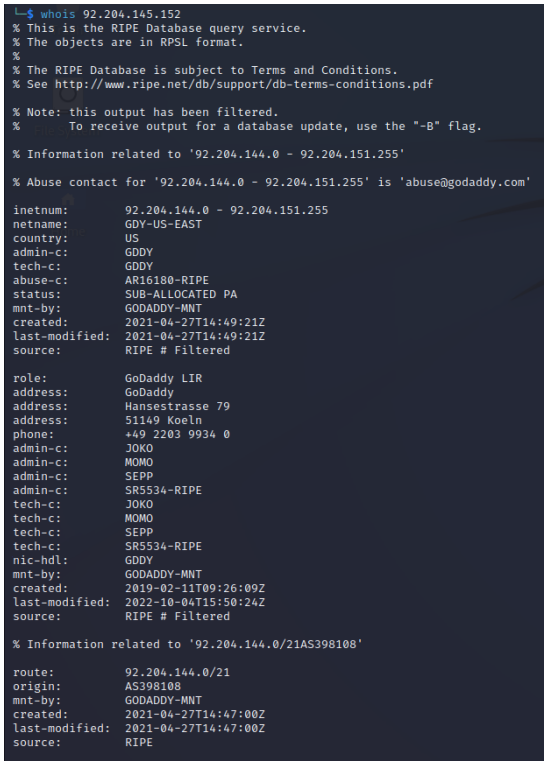
Reconocimiento pasivo

Objetivo: Identificar

Herramienta: Terminal Kali Linux, comando who is

Ejecución:

Figura 8: Reconocimiento pasivo



Fuente: Elaboración propia

Resultado del comando: Al realizar la consulta al dominio correspondiente podemos evidenciar la fecha de creación, la fecha de expiración, datos de quien registro el dominio, también los DNS que contiene.

¿Cómo podemos usar está información?

- Se pueden tomar los DNS que muestra la consulta para facilitar el reconocimiento y poder intervenir y causar daños.
- Se puede tomar la fecha de expiración del dominio para apoderarse del mismo y poder suplantar el sitio web, con esto se engañaría al visitante y obtener información.

6.2. Prueba 2. Reconocimiento pasivo – identificación IP

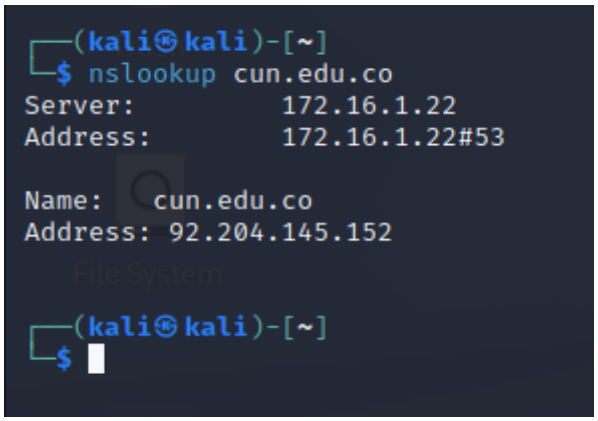
Reconocimiento pasivo – identificación IP

Objetivo: Reconocer IP

Herramienta: Terminal Kali Linux, comando nslookup

Ejecución:

Figura 9: Reconocimiento pasivo – identificación IP



Fuente: elaboración propia

Resultado: Al ingresar el comando nslookup muestra en pantalla la información de la puerta de enlace, también nos enseña la dirección IP del dominio registrado donde se puede enviar los ataques IP.

6.3. Prueba 3. Reconocimiento pasivo – Escaneo DNS

Objetivo: Obtener las direcciones de los DNS

Herramienta: Terminal Kali Linux, comando dnsrecon

Ejecución: dnsrecon -t std -d

Resultado: Al ingresar el comando el escaneo de tipo (-t) estándar (std) al dominio (-d) obtenemos el registro SOA el cual es el encargado de la transferencia de información entre servidores, también evidenciamos que dichos servidores usan seguridad

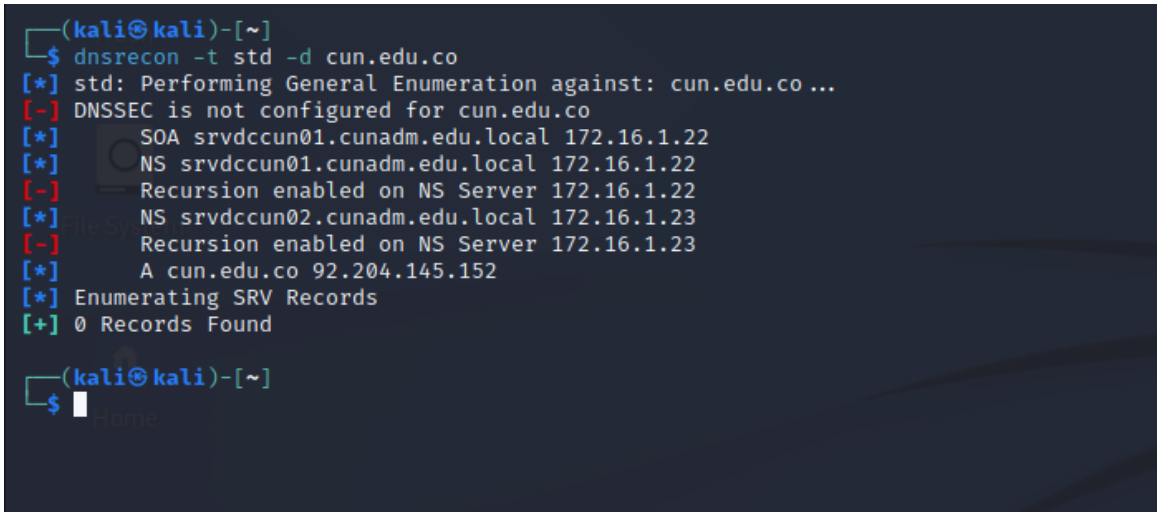
6.4. Prueba 4. Reconocimiento pasivo – Escaneo RED

Objetivo: Mostrar dispositivos conectados a la red

Herramienta: Terminal Kali Linux, comando Nmap

Ejecución: nmap -sP red x.x.x.x/x

Figura 10. Reconocimiento pasivo – Escaneo RED



Fuente: Elaboración propia

Resultado: Nos muestra los diferentes dispositivos conectados a la red interna, donde podemos extraer datos tales como la IP que toma, la dirección MAC y la marca del dispositivo.

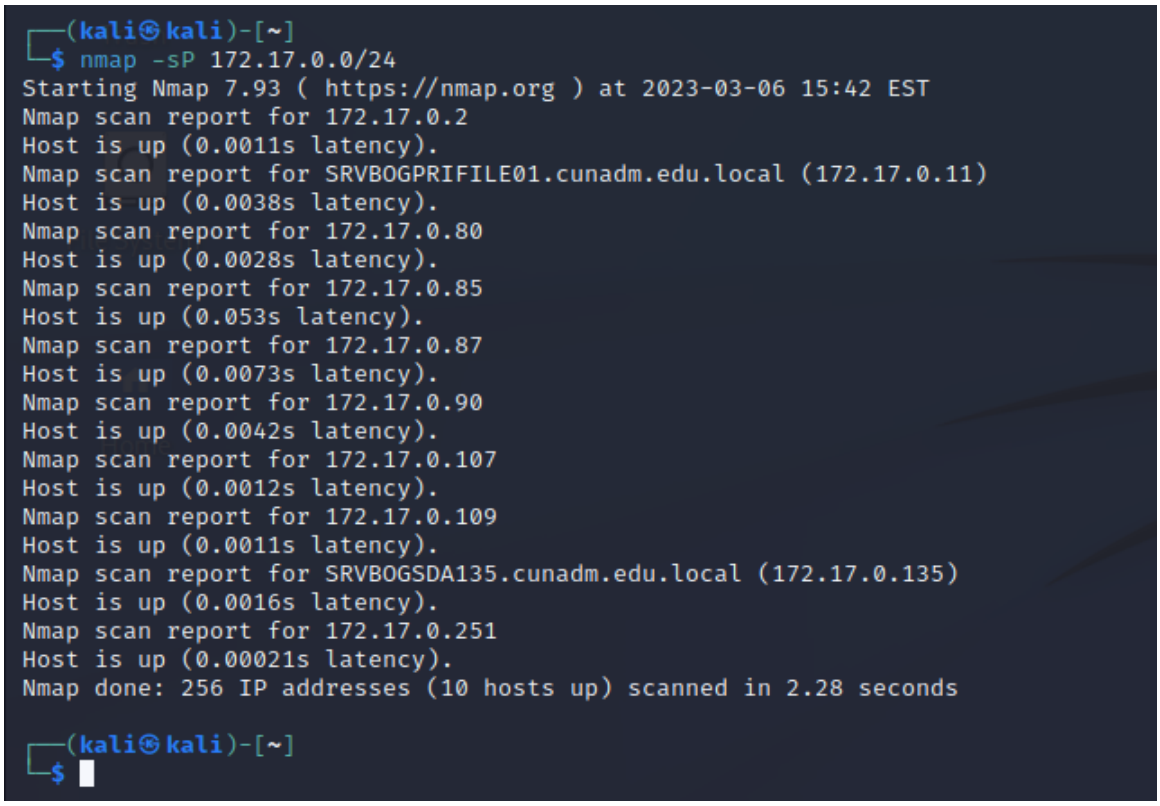
6.5. Prueba 5 Reconocimiento activo – Escaneo puertos BD

Objetivo: Encontrar puertos abiertos

Herramienta: Terminal Kali Linux

Ejecución: nmap -O X.X.X.X

Figura11: Reconocimiento activo – Escaneo puertos BD



Fuente: elaboración propia

Resultado: Tres ejecutar el comando en nuestra consola evidenciamos los puertos que se encuentran abiertos y de encontrar alguna de base de datos podrías generar un ataque por ese puerto.

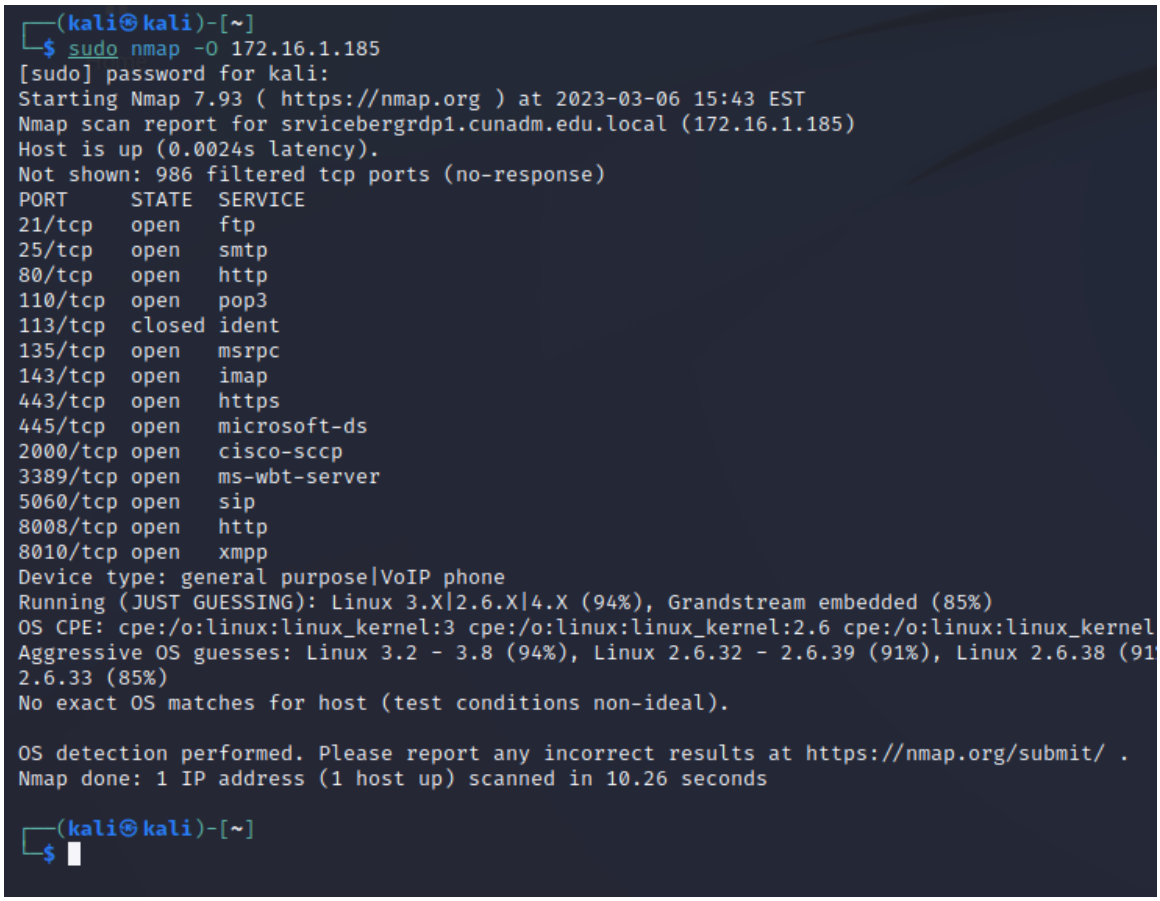
6.6. Prueba 6. Reconocimiento activo – Identificación BD

Objetivo: Identificar que se esté ejecutando el GBD

Herramienta: Terminal Kali Linux, Nmap

Ejecución: nmap –sTV –Pn –n –p1433 x.x.x.x

Figura 12: Reconocimiento activo – Identificación BD



Fuente: Elaboración propia

Resultado: Se evidencia el motor de base de datos, versión por donde podemos generar ataques de inyección SQL.

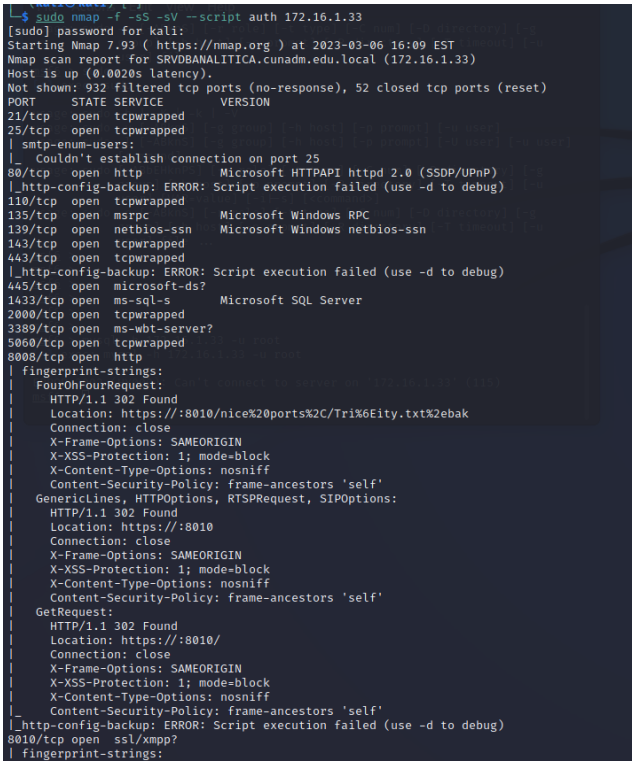
6.7. Prueba 7 Escaneo vulnerabilidades – script de auth

Objetivo: Identificar vulnerabilidades

Herramienta: Terminal Kali Linux, Nmap, script auth

Ejecución: nmap –f -sS -sV -script auth x.x.x.x

Figura13: Escaneo vulnerabilidades – script de auth



Fuente: Elaboración propia

Resultado: Con esté comando se puede evidenciar el puerto que se tienen permitido el ingreso de usuarios anónimos, también se puede observar si la cuenta de la MYSQL tiene o no contraseña, esté script nos permite realizar análisis de autenticación el cual nos permitirá ver las vulnerabilidades.

7. Recomendaciones

7.1. Recomendaciones Prueba 1

Al ser información pública, toda consulta realizada por el comando whois a cualquier dominio no puede ser registrada, cualquier persona puede acceder a ella sin problemas, lo recomendable es configurar el servidor para exponer la menor cantidad de información pública posible.

7.2. Recomendaciones Prueba 2

Usar una VPN permite que los ataques se retrasen, así poder anticipar y tomar las correspondientes medidas.

Cabe resaltar que es inevitable mostrar la IP del dominio por ellos se recomienda la VPN.

7.3. Recomendaciones Prueba 3

Se podría enmascarar y ocultar las IP con un NAT o VPN. Cabe resaltar que es inevitable mostrar la IP del dominio por ellos se recomienda la VPN.

7.4. Recomendaciones Prueba 4

En este tipo de escaneo solo se puede realizar si se tiene acceso a la red interna, se recomienda reforzar posibles entradas para los atacantes como la redes Wi-Fi o redes inalámbricas.

7.5. Recomendaciones Prueba 5

Al poner en línea un servidor ya sea local o en red por defecto vienen los puertos 3306 para MySQL o 5432 para PostgreSQL y al usar base de datos los puertos tendrán que estar abiertos. La recomendación es tener un firewall para evitar comprometer el equipo, usar puertos que no sean estándar y usar IDS.

7.6. Recomendaciones Prueba 6

Tener un firewall para evitar comprometer el equipo, usar puertos que no sean estándar y usar IDS (Sistema de detección de intrusos).

7.7. Recomendaciones Prueba 7

Recomendación: Dejar los puertos abiertos que se van a utilizar, también dejar con contraseña los servidores y los GBD.

7.8. Estructuración de las Políticas de seguridad

Al evaluar las políticas de seguridad de la institución evidenciamos que estas no se encuentras actualizadas.

Desde el guarda de seguridad, archivador, auxiliar, analista, coordinador, gerente y dirección, en una organización todos somos un eslabón de una cadena y tenemos el deber de velar y resguardar la información.

Así que sugerimos las siguientes políticas para usuarios para mejorar la seguridad de la información de la institución.

7.9. 11 políticas de seguridad

- Proteja su computadora contra robos en todo momento.

Proteger las computadoras corporativas contra robos es vital para proteger la propiedad intelectual, la continuidad del negocio, el cumplimiento de normativas, la imagen de la institución y los costos económicos.

- Clasificar y manejar los datos del cliente y de la institución correctamente.

Implica identificar los tipos de datos, establecer medidas de seguridad adecuadas, establecer políticas claras de privacidad y seguridad, garantizar el acceso controlado a los datos, establecer procedimientos claros de gestión de datos, y capacitar al personal adecuadamente.

- Protege tu contraseña y otras credenciales de acceso.

Proteger la contraseña y otras credenciales de acceso es crucial para mantener la seguridad de la información personal y evitar que terceros no autorizados accedan a nuestras cuentas y datos sensibles

- Proteja los datos con encriptación segura de protectores de pantalla o contraseña de BIOS.

Proteger los datos con encriptación segura, protectores de pantalla o contraseña de BIOS son medidas importantes para asegurar la privacidad y confidencialidad de la información.

- Asegúrese de que el antivirus y los parches estén actualizados.

Mantener actualizado el antivirus y los parches de seguridad es fundamental para proteger los sistemas informáticos y reducir el riesgo de infección por virus y malware. La falta de actualización puede dejar a los sistemas vulnerables a los ataques informáticos, lo que podría comprometer la seguridad y la privacidad de los datos. Por lo tanto, es importante realizar actualizaciones regulares para mantener los sistemas informáticos seguros y protegidos.

- Asegúrese de que se realice una copia de seguridad de los datos críticos.

Asegurarse de que se realice una copia de seguridad de los datos críticos es una medida esencial para proteger la información importante y garantizar la continuidad del negocio en caso de fallos técnicos o desastres naturales. Además, las copias de seguridad son importantes para cumplir con las obligaciones legales, proteger contra el ransomware y minimizar el tiempo de inactividad en caso de una interrupción en las operaciones normales.

- Proteger con contraseña o limitar el acceso al archivo a archivos compartidos.

Proteger con contraseña o limitar el acceso a archivos compartidos es una medida de seguridad importante para proteger la información confidencial y sensible, cumplir con las obligaciones legales, controlar el acceso a la información y prevenir la pérdida de datos. Las organizaciones deben implementar medidas de seguridad adecuadas para proteger sus archivos compartidos y garantizar que solo las personas autorizadas tengan acceso a la información.

- Use solo software aprobado y licenciado.

Utilizar software aprobado y licenciado es una medida importante de seguridad que las organizaciones deben tomar en cuenta para garantizar la fiabilidad del software, recibir soporte técnico y actualizaciones, cumplir con las obligaciones legales y prevenir riesgos de seguridad. Las organizaciones deben asegurarse de utilizar software aprobado y licenciado en todos sus sistemas informáticos y evitar el uso de software no aprobado o pirata.

- Uso limitado no comercial de la dirección de correo electrónico de la institución.

Limitar el uso no comercial de la dirección de correo electrónico de la institución es importante para proteger la información confidencial, garantizar el uso efectivo de los recursos de la institución, cumplir con las políticas y evitar el spam y el phishing. Las organizaciones deben establecer políticas claras y comunicarlas a sus empleados para garantizar que la dirección de correo electrónico de la institución se utilice de manera responsable y segura.

- Almacenar y desechar adecuadamente los medios renovables.

Es importante almacenar y desechar adecuadamente los medios renovables para proteger la información confidencial, prevenir la pérdida de datos, cumplir con las regulaciones y reducir el riesgo de fraude y robo de identidad. Las organizaciones deben establecer políticas claras y comunicarlas a sus empleados para garantizar que los medios renovables se manejen de manera responsable y segura.

- Informar sobre riesgos de seguridad e incidentes a través de la mesa de ayuda.

informar sobre riesgos de seguridad e incidentes a través de la mesa de ayuda es una práctica importante para garantizar la seguridad de la información en una organización. Las organizaciones deben establecer políticas claras para informar sobre incidentes de seguridad y capacitar a los empleados sobre cómo identificar y reportar amenazas de seguridad.

8. CRONOGRAMA

A continuación, se establece en el cronograma las actividades a desarrollar a lo largo de estos dos semestres.

Tabla 3. Cronograma

CRONOGRAMA DE ACTIVIDADES								
	2022					2023		
ACTIVIDAD	AGOSTO	SEPTIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE	ENERO	FEBRERO	MARZO
IDENTIFICACION DEL TEMA								
PLANTEAMIENTO DEL PROBLEMA A TRATAR								
JUSTIFICACION								
IDENTIFICACION DE OBJETIVOS								
MARCO CONCEPTUAL								
METODOLOGIA DE LA INVESTIGACION								
MARCO TEORICO								
ANTECEDENTES INVESTIGATIVOS								
ANALISIS Y ESTUDIO DE SOFWARE PARA REALIZAR VULNERABILIDADES								
INSTALACION Y EJECUCION DE VULNERABILIDADES								
RECOLECCION DE HALLASGOS								
ANALISIS DE DATOS								
CONCLUSIONES Y RECOMENDACIONES								

Fuente: Creación propia

9. PRESUPUESTO

Tabla.4 Presupuesto

		Valor por persona	Total
	Sueldos y salarios		$ -
1	Consultores		$ -
	Materiales y suministros		$ -
1	Material de oficina específico para el proyecto	$ 100.000,00	$ 300.000,00
2	Comunicaciones	$ 65.000,00	$ 195.000,00
	Equipo		$ -
1	Instalación de equipos		$ -
	Viajes		$ -
1	Trabajo de campo	$ 120.000,00	$ 360.000,00
2	Viajes de consulta y consultores		$ -
	Otros		$ -
1	Alimentación	$ 180.000,00	$ 540.000,00
2	Servicios públicos	$ 100.000,00	$ 300.000,00
	Total		$ 1.695.000,00

Fuente: Creación Propia

10. CONCLUSIONES

- Si se ha podido probar la hipótesis de identificar las vulnerabilidades y riesgos que tiene la institución del sector educativo en sus diferentes sistemas informáticos a través de un modelo de investigación cuantitativo. El modelo de investigación cuantitativo es una herramienta útil para identificar las vulnerabilidades y riesgos que tienen una organización del sector educativo en sus diferentes sistemas informáticos y tomar medidas para mejorar su seguridad.

- En conclusión, la evaluación de las vulnerabilidades y riesgos que se realizó en la institución del sector educativo en sus sistemas de información, infraestructura de red y datos masivos es fundamental para garantizar la seguridad y protección de la información de esta y de sus usuarios. Este proyecto ayudara a tomar medidas preventivas para minimizar la probabilidad de incidentes de seguridad y proteger la información crítica de la organización. Es importante destacar que la evaluación de las vulnerabilidades y riesgos no es un único proceso, sino que debe realizarse de forma periódica para garantizar que los sistemas de la organización sigan siendo seguros y estén protegidos contra posibles amenazas.

- Es importante identificar los tipos de vulnerabilidades y riesgos presentes en la organización porque permite tomar medidas preventivas y correctivas para proteger la integridad, confidencialidad y disponibilidad de los recursos críticos de la institución.
- Al estructurar un informe de mitigación de vulnerabilidades y riesgos proporciona una visión general de los riesgos críticos para la organización y ayuda a establecer prioridades y objetivos de seguridad claros
- En conclusión, existen varias herramientas de código abierto que son accesibles a cualquier persona interesada en aprender sobre seguridad informática y realizar pruebas de penetración.

Kali Linux es una herramienta importante en el arsenal de cualquier profesional de la seguridad informática ya que permite identificar vulnerabilidades en los sistemas y aplicaciones, así como detectar posibles amenazas y ataques.

- Aprendimos la importancia de analizar y estructurar las políticas de seguridad de la institución para proteger la información, cumplir con las normas y regulaciones, sensibilizar al personal, prevenir incidentes de seguridad y mejorar continuamente la seguridad de la información.

11. Bibliografía

Acosta, S. (2018). Ingeniería Social en Instituciones de Educación Superior. . *REVISTA COLOMBIANA DE TECNOLOGIAS DE AVANZADA (RCTA)*.

Antokoletz, D. (2010). *Ingenieria Social.* Segu-info.

Arrollo, S. (2020). La cibercriminologia y el perfil del ciberdelincuente. Derecho y Cambio Social.

Borghello, C. (2009). *El arma infalible. la ingenieria social.* ESET latinoamerica.

Campos, M. A. (2020). *Implementación de un security information and event management (SIEM) para detectar vulnerabilidades y amenazas expuestas en las plataformas informáticas y redes de una entidad financiera.*

Cañon, L. (2015). Ataques informáticos. *Ethical Hacking y conciencia de seguridad informática en niños*.

Carpentier, J. F. (2016). La seguridad informática en la PYME. *Situación actual y mejores prácticas. Ediciones ENI*.

Castro, J. (2022). Modelo de evaluación de riesgos informáticos basado en analítica de datos para la comunidad educativa del centro de servicios y gestión empresarial del SENA Regional Antioquia. *Ciencia Latina Revista Científica Multidisciplinar*, 323-346. Obtenido de https://doi.org/10.37811/cl_rcm.v6i2.2230

Castro, J. (2021). Análisis de riesgos y vulnerabilidades de seguridad informática aplicando técnicas de inteligencia artificial orientado a instituciones de educación superior. *Revista MODUM*.

COMPES. (2016). *CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL.* Obtenido de https://colaboracion.dnp.gov.co/

Costas, J. (2011). Seguridad informática. Bogota.

Estupiñan, A., Pulido, H., & Bohada, J. (2013). Análisis de Riesgos en Seguridad de la Información. *Revista ciencia, innovación y tecnología*, 40-53.

Fonfria, A. (2020). Elementos para una politica de ciberseguridad efectiva. Analisis del Real Instituto Elcano.

(2023). *GESTIÓN DE RIESGO Y CONTROL INFORMÁTICO.* Bogota: unitec.

Gomez , A. (2022). Auditoria de Seguridad Informatica. Ediciones de la U.

Leguizamon, M. (2015). *El phishing.*

Mieres, J. (2009). *Ataques informáticos.*

Narvaez, D., & Romero, C. (2016). Evaluación de ataques de Denegación de servicio DoS y DDoS, y mecanismos de protección. *GEEKS DECC-REPORTS*.

Perez, C. (2005). *Envenenamiento ARP.*

Quispe, C. (2009). Tipos de Hackers.

Romero, M. I., Figueroa, G., & Vera, D. (2018). INTRODUCCIÓN A LA SEGURIDAD INFORMATICA Y EL ANALISIS DE VULNERABILIDADES.

Sauceda, A., & Miranda, J. (2015). Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones web. *Revista electrónica de Computación, Informática, Biomédica y Electrónica*.

Senado de la República de Colombia. (1991). *Constitución Política de Colombia.* Obtenido de http://www.secretariasenado.gov.co/index.php/constitucion-politica

Toro, J., & Guisao, J. (2014). Detección y mitigación de vulnerabilidades día cero. *Cuaderno Activa*.

Urbina, G. (2016). Introduccion ala seguridad informatica. Grupo editorial Patria .

Villamil, D., & Moyano Hernandez, F. (2021). Análisis del ciclo PHVA en la gestión de proyectos, una revisión documental. *Revista Politécnica*, 55-69.

Zambrano, A. (2018). Introducción a la seguridad informática y el análisis de vulnerabilidades. *Vol. 46. 3Ciencias*.

12. ANEXOS

12.1. ANEXOS A. Encuesta.

Encuesta seguridad informática

Cargo: _____

Fecha de diligenciamiento: _____

1. ¿Cuentan con políticas de seguridad en la Institución?

   Si: _____ No: _____ No Sabe: _____ No Responde: _____

2. ¿Cuentan con software o consola para administrar la seguridad de la institución?

   Si: _____ No: _____ No Sabe: _____ No Responde: _____

3. ¿Cuentan con software o consola para administrar los activos de la compañía?

   Si: _____ No: _____ No Sabe: _____ si su respuesta es si cual: _____

4. ¿Con qué frecuencia actualizas un software antivirus?

   a. Se hace automáticamente
   b. Al menos dos veces por semana
   c. Al menos una vez a la semana
   d. Al menos una vez al mes

5. ¿Quién es el responsable de mantener y administrar el software o consola de seguridad de la institución?

   _____

6. ¿Qué versión de Windows está instalada en los equipos de la institución?
   a. Windows 11
   b. Windows 10
   c. Windows 8
   d. Windows 7
   e. Otros

7. ¿Consideras que han tenido problemas de seguridad donde se vea comprometida la información de la institución o usuarios?

   Si: _____ No: _____ No Sabe: _____ No Responde: _____

8. ¿Has tenido algún problema con?
   a. Malware
   b. Virus
   c. Gusano
   d. Troyano
   e. Spyware
   f. Adware
   g. Ranssomware

9. ¿Actualmente realizan mantenimientos periódicos sobre las computadoras de la empresa?

Si: _____ No: _____ No Sabe: _____ No Responde: _____

10. Generalmente realizan copias de seguridad de su información

Si: _____ No: _____ No Sabe: _____ No Responde: _____

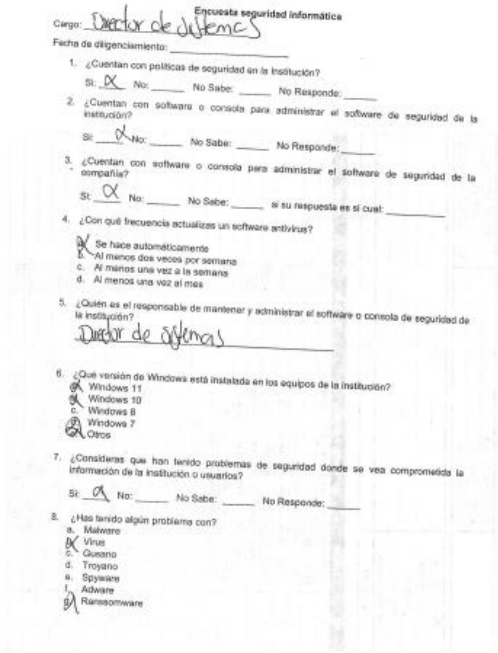
11. ¿Cada Cuanto se realizan las copias de seguridad?
    a. Diario
    b. Semanal
    c. Mensual

12. Realizan algún tipo de capacitación en cuanto a seguridad informática hacia los usuarios
    a. Contraseñas
    b. Antivirus
    c. Firewall
    d. AntiSpyware
    e. Antimalware
    f. Sistema de detección de intrusos
    g. Otro:
13. ¿Cuentan con una red VPN en su empresa?

Si: _____ No: _____ No Sabe: _____ No Responde: _____

14. ¿Generalmente realizan pruebas de seguridad en sus redes?
    Si: _____ No: _____ No Sabe: _____ No Responde: _____
15. La frecuencia con la que realizan las pruebas es
    a. Ninguna
    b. Cada 3 meses
    c. Cada 6 meses
    d. Cada año
    e. Cada 2 años o mas
16. ¿Qué tan frecuentemente se preparan ante problemas de seguridad?
    a. Cada mes
    b. Cada trimestre
    c. Cada 6 meses
    d. Cada año
    e. Más de un año
17. ¿Tiene proyectado invertir en seguridad informática en los siguientes?
    f. 3 meses
    g. 6 meses
    h. 1 año
    i. 2 años
    j. Más de 2 años

ANEXO B. Encuestas desarrolladas

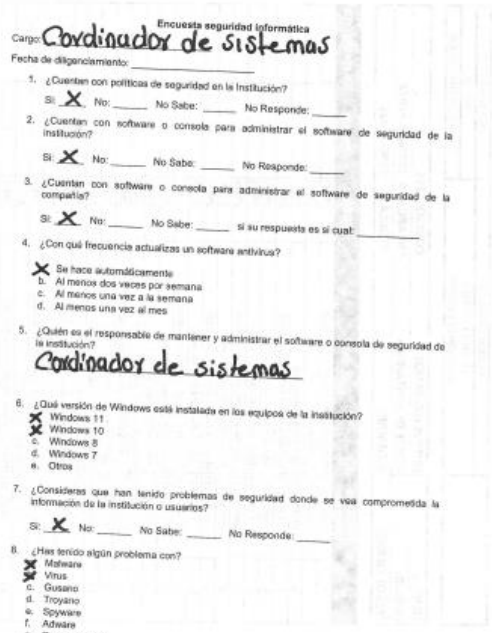


Encuesta seguridad informática

Cargo: Director de sistemas

Fecha de diligenciamiento: _____

1. ¿Cuentan con políticas de seguridad en la institución?
   Si: X No: _____ No Sabe: _____ No Responde: _____
2. ¿Cuentan con software o consola para administrar el software de seguridad de la institución?
   Si: X No: _____ No Sabe: _____ No Responde: _____
3. ¿Cuentan con software o consola para administrar el software de seguridad de la compañía?
   Si: X No: _____ No Sabe: _____ si su respuesta es si cual: _____
4. ¿Con qué frecuencia actualizas un software antivirus?
   a. X Se hace automáticamente
   b. Al menos dos veces por semana
   c. Al menos una vez a la semana
   d. Al menos una vez al mes
5. ¿Quién es el responsable de mantener y administrar el software o consola de seguridad de la institución?
   Director de sistemas
6. ¿Qué versión de Windows está instalada en los equipos de la institución?
   a. X Windows 11
   b. X Windows 10
   c. Windows 8
   d. X Windows 7
   e. Otros
7. ¿Consideras que han tenido problemas de seguridad donde se vea comprometida la información de la institución o usuarios?
   Si: X No: _____ No Sabe: _____ No Responde: _____
8. ¿Has tenido algún problema con?
   a. Malware
   b. X Virus
   c. Gusano
   d. Troyano
   e. Spyware
   f. Adware
   g. X Ransomware

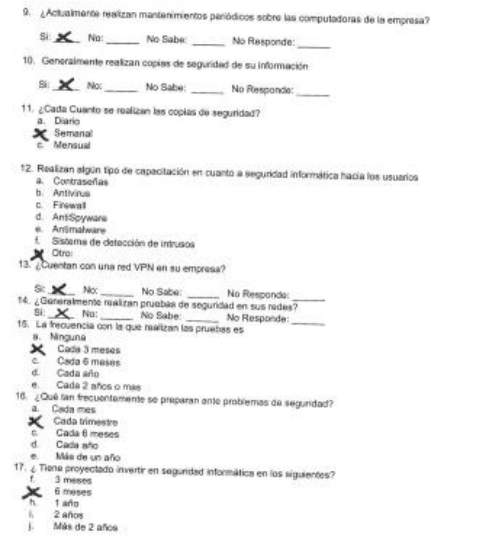


Encuesta seguridad informática

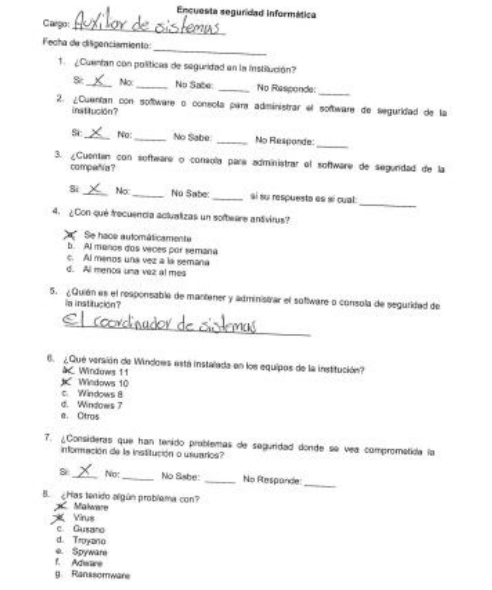
Cargo: Cordinador de sistemas

Fecha de diligenciamiento: _____

1. ¿Cuentan con políticas de seguridad en la institución?
   Si: X No: _____ No Sabe: _____ No Responde: _____
2. ¿Cuentan con software o consola para administrar el software de seguridad de la institución?
   Si: X No: _____ No Sabe: _____ No Responde: _____
3. ¿Cuentan con software o consola para administrar el software de seguridad de la compañía?
   Si: X No: _____ No Sabe: _____ si su respuesta es si cual: _____
4. ¿Con qué frecuencia actualizas un software antivirus?
   a. X Se hace automáticamente
   b. Al menos dos veces por semana
   c. Al menos una vez a la semana
   d. Al menos una vez al mes
5. ¿Quién es el responsable de mantener y administrar el software o consola de seguridad de la institución?
   Cordinador de sistemas
6. ¿Qué versión de Windows está instalada en los equipos de la institución?
   a. X Windows 11
   b. X Windows 10
   c. Windows 8
   d. Windows 7
   e. Otros
7. ¿Consideras que han tenido problemas de seguridad donde se vea comprometida la información de la institución o usuarios?
   Si: X No: _____ No Sabe: _____ No Responde: _____
8. ¿Has tenido algún problema con?
   a. X Malware
   b. X Virus
   c. Gusano
   d. Troyano
   e. Spyware
   f. Adware
   g. Ransomware



9. ¿Actualmente realizan mantenimientos periódicos sobre las computadoras de la empresa?
   Si: X No: _____ No Sabe: _____ No Responde: _____
10. Generalmente realizan copias de seguridad de su información
    Si: X No: _____ No Sabe: _____ No Responde: _____
11. ¿Cada Cuanto se realizan las copias de seguridad?
    a. Diario
    b. X Semanal
    c. Mensual
12. Realizan algún tipo de capacitación en cuanto a seguridad informática hacia los usuarios
    a. Contraseñas
    b. Antivirus
    c. Firewall
    d. AntiSpyware
    e. Antimalware
    f. Sistema de detección de intrusos
    g. X Otro:
13. ¿Cuentan con una red VPN en su empresa?
    Si: X No: _____ No Sabe: _____ No Responde: _____
14. ¿Generalmente realizan pruebas de seguridad en sus redes?
    Si: X No: _____ No Sabe: _____ No Responde: _____
15. La frecuencia con la que realizan las pruebas es
    a. Ninguna
    b. X Cada 3 meses
    c. Cada 6 meses
    d. Cada año
    e. Cada 2 años o mas
16. ¿Qué tan frecuentemente se preparan ante problemas de seguridad?
    a. Cada mes
    b. X Cada trimestre
    c. Cada 6 meses
    d. Cada año
    e. Más de un año
17. ¿ Tiene proyectado invertir en seguridad informática en los siguientes?
    f. 3 meses
    g. X 6 meses
    h. 1 año
    i. 2 años
    j. Más de 2 años



Encuesta seguridad informática

Cargo: Auxiliar de sistemas

Fecha de diligenciamiento: _____

1. ¿Cuentan con políticas de seguridad en la institución?
   Si: X No: _____ No Sabe: _____ No Responde: _____
2. ¿Cuentan con software o consola para administrar el software de seguridad de la institución?
   Si: X No: _____ No Sabe: _____ No Responde: _____
3. ¿Cuentan con software o consola para administrar el software de seguridad de la compañía?
   Si: X No: _____ No Sabe: _____ si su respuesta es si cual: _____
4. ¿Con qué frecuencia actualizas un software antivirus?
   a. X Se hace automáticamente
   b. Al menos dos veces por semana
   c. Al menos una vez a la semana
   d. Al menos una vez al mes
5. ¿Quién es el responsable de mantener y administrar el software o consola de seguridad de la institución?
   El coordinador de sistemas
6. ¿Qué versión de Windows está instalada en los equipos de la institución?
   a. X Windows 11
   b. X Windows 10
   c. Windows 8
   d. Windows 7
   e. Otros
7. ¿Consideras que han tenido problemas de seguridad donde se vea comprometida la información de la institución o usuarios?
   Si: X No: _____ No Sabe: _____ No Responde: _____
8. ¿Has tenido algún problema con?
   a. X Malware
   b. X Virus
   c. Gusano
   d. Troyano
   e. Spyware
   f. Adware
   g. Ransomware

9. ¿Actualmente realizan mantenimientos periódicos sobre las computadoras de la empresa?

Si: X No: _____ No Sabe: _____ No Responde: _____

10. Generalmente realizan copias de seguridad de su información

Si: X No: _____ No Sabe: _____ No Responde: _____

11. ¿Cada Cuanto se realizan las copias de seguridad?
a. Diario
X c. Semanal
c. Mensual

12. Realizan algún tipo de capacitación en cuanto a seguridad informática hacia los usuarios
a. Contraseñas
b. Antivirus
c. Firewall
d. AntiSpyware
e. Antimalware
f. Sistema de detección de intrusos
X Otro:

13. ¿Cuentan con una red VPN en su empresa?

Si: X No: _____ No Sabe: _____ No Responde: _____

14. ¿Generalmente realizan pruebas de seguridad en sus redes?
Si: X No: _____ No Sabe: _____ No Responde: _____

15. La frecuencia con la que realizan las pruebas es
a. Ninguna
X c. Cada 3 meses
c. Cada 6 meses
d. Cada año
e. Cada 2 años o mas

16. ¿Qué tan frecuentemente se preparan ante problemas de seguridad?
a. Cada mes
X c. Cada trimestre
c. Cada 6 meses
d. Cada año
e. Más de un año

17. ¿ Tiene proyectado invertir en seguridad informática en los siguientes?
f. 3 meses
X h. 6 meses
h. 1 año
i. 2 años
j. Más de 2 años

Encuesta seguridad informática

Cargo: Analista Sistemas

Fecha de diligenciamiento: Marzo 3 - 2023

1. ¿Cuentan con políticas de seguridad en la Institución?
Si: X No: _____ No Sabe: _____ No Responde: _____

2. ¿Cuentan con software o consola para administrar el software de seguridad de la institución?
Si: X No: _____ No Sabe: _____ No Responde: _____

3. ¿Cuentan con software o consola para administrar el software de seguridad de la compañía?
Si: X No: _____ No Sabe: _____ si su respuesta es si cual: _____

4. ¿Con qué frecuencia actualizas un software antivirus?
(a) Se hace automáticamente
b. Al menos dos veces por semana
c. Al menos una vez a la semana
d. Al menos una vez al mes

5. ¿Quién es el responsable de mantener y administrar el software o consola de seguridad de la institución?
Director del área TI

6. ¿Qué versión de Windows está instalada en los equipos de la institución?
(a) Windows 11
(b) Windows 10
c. Windows 8
d. Windows 7
(e) Otros

7. ¿Consideras que han tenido problemas de seguridad donde se vea comprometida la información de la institución o usuarios?
Si: X No: _____ No Sabe: _____ No Responde: _____

8. ¿Has tenido algún problema con?
a. Malware
b. Virus
c. Gusano
d. Troyano
e. Spyware
f. Adware
(g) Ransomware

9. ¿Actualmente realizan mantenimientos periódicos sobre las computadoras de la empresa?

Si: _____ No: X No Sabe: _____ No Responde: _____

10. Generalmente realizan copias de seguridad de su información

Si: _____ No: X No Sabe: _____ No Responde: _____

11. ¿Cada Cuanto se realizan las copias de seguridad?
a. Diario
b. Semanal
(c) Mensual

12. Realizan algún tipo de capacitación en cuanto a seguridad informática hacia los usuarios
(a) Contraseñas
b. Antivirus
c. Firewall
d. AntiSpyware
e. Antimalware
f. Sistema de detección de intrusos
g. Otro:

13. ¿Cuentan con una red VPN en su empresa?

Si: X No: _____ No Sabe: _____ No Responde: _____

14. ¿Generalmente realizan pruebas de seguridad en sus redes?
Si: _____ No: X No Sabe: _____ No Responde: _____

15. La frecuencia con la que realizan las pruebas es
(a) Ninguna
b. Cada 3 meses
c. Cada 6 meses
d. Cada año
e. Cada 2 años o mas

16. ¿Qué tan frecuentemente se preparan ante problemas de seguridad?
a. Cada mes
b. Cada trimestre
c. Cada 6 meses
d. Cada año
(e) Más de un año

17. ¿ Tiene proyectado invertir en seguridad informática en los siguientes?
f. 3 meses
g. 6 meses
h. 1 año
i. 2 años
(j) Más de 2 años

Encuesta seguridad informática

Cargo: Analista de Sistemas

Fecha de diligenciamiento: Marzo 2023

1. ¿Cuentan con políticas de seguridad en la Institución?
Si: X No: _____ No Sabe: _____ No Responde: _____

2. ¿Cuentan con software o consola para administrar el software de seguridad de la institución?
Si: _____ No: _____ No Sabe: X No Responde: _____

3. ¿Cuentan con software o consola para administrar el software de seguridad de la compañía?
Si: _____ No: _____ No Sabe: X si su respuesta es si cual: _____

4. ¿Con qué frecuencia actualizas un software antivirus?
X a. Se hace automáticamente
b. Al menos dos veces por semana
c. Al menos una vez a la semana
d. Al menos una vez al mes

5. ¿Quién es el responsable de mantener y administrar el software o consola de seguridad de la institución?
El area de TI,Temas

6. ¿Qué versión de Windows está instalada en los equipos de la institución?
X. Windows 11
X. Windows 10
X. Windows 8
X. Windows 7
e. Otros

7. ¿Consideras que han tenido problemas de seguridad donde se vea comprometida la información de la institución o usuarios?
Si: _____ No: X No Sabe: _____ No Responde: _____

8. ¿Has tenido algún problema con?
X. Malware
b. Virus
c. Gusano
d. Troyano
e. Spyware
f. Adware
g. Ransomware

9. ¿Actualmente realizan mantenimientos periódicos sobre las computadoras de la empresa?
   Si: X No: ____ No Sabe: ____ No Responde: ____
10. Generalmente realizan copias de seguridad de su información
    Si: X No: ____ No Sabe: ____ No Responde: ____
11. ¿Cada Cuanto se realizan las copias de seguridad?
    a. Diario
    b. Semanal
    X. Mensual
12. Realizan algún tipo de capacitación en cuanto a seguridad informática hacia los usuarios
    X. Contraseñas
    b. Antivirus
    c. Firewall
    d. AntiSpyware
    e. Antimalware
    f. Sistema de detección de intrusos
    g. Otro:
13. ¿Cuentan con una red VPN en su empresa?
    Si: X No: ____ No Sabe: ____ No Responde: ____
14. ¿Generalmente realizan pruebas de seguridad en sus redes?
    Si: ____ No: ____ No Sabe: X No Responde: ____
15. La frecuencia con la que realizan las pruebas es
    X. Ninguna
    b. Cada 3 meses
    c. Cada 6 meses
    d. Cada año
    e. Cada 2 años o mas
16. ¿Qué tan frecuentemente se preparan ante problemas de seguridad?
    a. Cada mes
    b. Cada trimestre
    c. Cada 6 meses
    X. Cada año
    e. Más de un año
17. ¿ Tiene proyectado invertir en seguridad informática en los siguientes?
    f. 3 meses
    g. 6 meses
    h. 1 año
    i. 2 años
    X. Más de 2 años

9. ¿Actualmente realizan mantenimientos periódicos sobre las computadoras de la empresa?
   Si: ____ No: ____ No Sabe: X No Responde: ____
10. Generalmente realizan copias de seguridad de su información
    Si: X No: ____ No Sabe: ____ No Responde: ____
11. ¿Cada Cuanto se realizan las copias de seguridad?
    X. Diario
    b. Semanal
    c. Mensual
12. Realizan algún tipo de capacitación en cuanto a seguridad informática hacia los usuarios
    a. Contraseñas
    b. Antivirus
    c. Firewall
    d. AntiSpyware
    e. Antimalware
    f. Sistema de detección de intrusos
    g. Otro: NO
13. ¿Cuentan con una red VPN en su empresa?
    Si: X No: ____ No Sabe: ____ No Responde: ____
14. ¿Generalmente realizan pruebas de seguridad en sus redes?
    Si: ____ No: X No Sabe: ____ No Responde: ____
15. La frecuencia con la que realizan las pruebas es
    X. Ninguna
    b. Cada 3 meses
    c. Cada 6 meses
    d. Cada año
    e. Cada 2 años o mas
16. ¿Qué tan frecuentemente se preparan ante problemas de seguridad?
    a. Cada mes
    b. Cada trimestre
    c. Cada 6 meses
    d. Cada año
    X. Más de un año
17. ¿Tiene proyectado invertir en seguridad informática en los siguientes?
    X. 3 meses
    g. 6 meses
    h. 1 año
    i. 2 años
    j. Más de 2 años

Encuesta seguridad informática

Cargo: DBA
Fecha de diligenciamiento: ____

1. ¿Cuentan con políticas de seguridad en la institución?
   Si: X No: ____ No Sabe: ____ No Responde: ____
2. ¿Cuentan con software o consola para administrar el software de seguridad de la institución?
   Si: X No: ____ No Sabe: ____ No Responde: ____
3. ¿Cuentan con software o consola para administrar el software de seguridad de la compañía?
   Si: X No: ____ No Sabe: ____ si su respuesta es si cual: ____
4. ¿Con qué frecuencia actualizas un software antivirus?
   X. Se hace automáticamente
   b. Al menos dos veces por semana
   c. Al menos una vez a la semana
   d. Al menos una vez al mes
5. ¿Quién es el responsable de mantener y administrar el software o consola de seguridad de la institución?
   Director de Sistemas
6. ¿Qué versión de Windows está instalada en los equipos de la institución?
   X. Windows 11
   b. Windows 10
   c. Windows 8
   d. Windows 7
   e. Otros
7. ¿Consideras que han tenido problemas de seguridad donde se vea comprometida la información de la institución o usuarios?
   Si: X No: ____ No Sabe: ____ No Responde: ____
8. ¿Has tenido algún problema con?
   a. Malware
   b. Virus
   c. Gusano
   d. Troyano
   X. Spyware
   f. Adware
   g. Ransomware

Encuesta seguridad informática

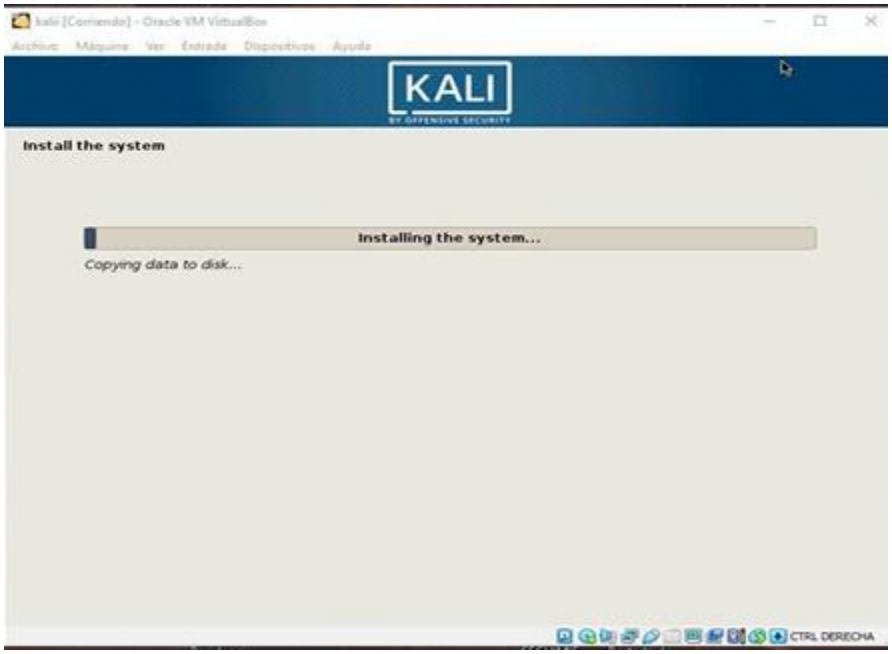
Cargo: Analista Sistemas
Fecha de diligenciamiento: ____

1. ¿Cuentan con políticas de seguridad en la institución?
   Si: X No: ____ No Sabe: ____ No Responde: ____
2. ¿Cuentan con software o consola para administrar el software de seguridad de la institución?
   Si: X No: ____ No Sabe: ____ No Responde: ____
3. ¿Cuentan con software o consola para administrar el software de seguridad de la compañía?
   Si: X No: ____ No Sabe: ____ si su respuesta es si cual: ____
4. ¿Con qué frecuencia actualizas un software antivirus?
   X. Se hace automáticamente
   b. Al menos dos veces por semana
   c. Al menos una vez a la semana
   d. Al menos una vez al mes
5. ¿Quién es el responsable de mantener y administrar el software o consola de seguridad de la institución?
   Jefe infraestructura
6. ¿Qué versión de Windows está instalada en los equipos de la institución?
   a. Windows 11
   X. Windows 10
   c. Windows 8
   d. Windows 7
   e. Otros
7. ¿Consideras que han tenido problemas de seguridad donde se vea comprometida la información de la institución o usuarios?
   Si: ____ No: X No Sabe: ____ No Responde: ____
8. ¿Has tenido algún problema con?
   a. Malware
   X. Virus
   c. Gusano
   d. Troyano
   e. Spyware
   f. Adware
   g. Ransomware

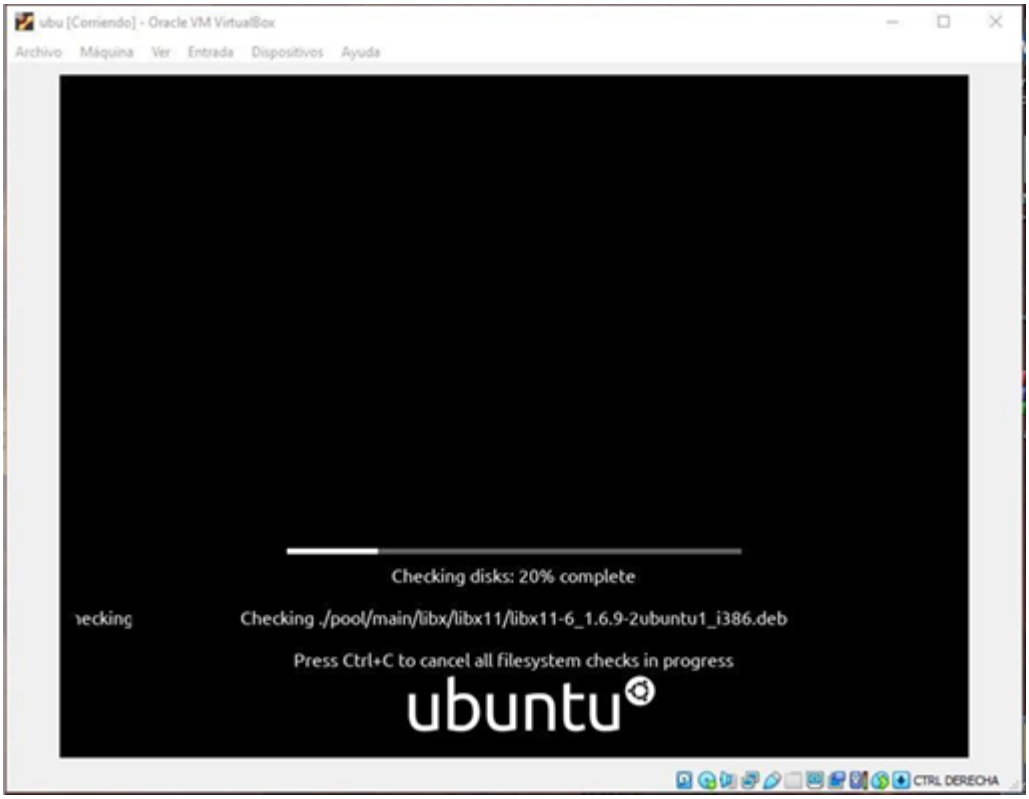
9. ¿Actualmente realizan mantenimientos periódicos sobre las computadoras de la empresa?
   Si: _X_ No: _____ No Sabe: _____ No Responde: _____
10. Generalmente realizan copias de seguridad de su información
    Si: _____ No: _X_ No Sabe: _____ No Responde: _____
11. ¿Cada Cuanto se realizan las copias de seguridad?
    X. Diario
    b. Semanal
    c. Mensual
12. Realizan algún tipo de capacitación en cuanto a seguridad informática hacia los usuarios
    X. Contraseñas
    X. Antivirus
    c. Firewall
    d. AntiSpyware
    e. Antimalware
    X. Sistema de detección de intrusos
    g. Otro:
13. ¿Cuentan con una red VPN en su empresa?
    Si: _X_ No: _____ No Sabe: _____ No Responde: _____
14. ¿Generalmente realizan pruebas de seguridad en sus redes?
    Si: _X_ No: _____ No Sabe: _____ No Responde: _____
15. La frecuencia con la que realizan las pruebas es
    a. Ninguna
    X. Cada 3 meses
    c. Cada 6 meses
    d. Cada año
    e. Cada 2 años o mas
16. ¿Qué tan frecuentemente se preparan ante problemas de seguridad?
    a. Cada mes
    X. Cada trimestre
    c. Cada 6 meses
    d. Cada año
    e. Más de un año
17. ¿ Tiene proyectado invertir en seguridad informática en los siguientes?
    X. 3 meses
    g. 6 meses
    h. 1 año
    i. 2 años
    j. Más de 2 años

Anexos C. Programas utilizados para diagnósticos

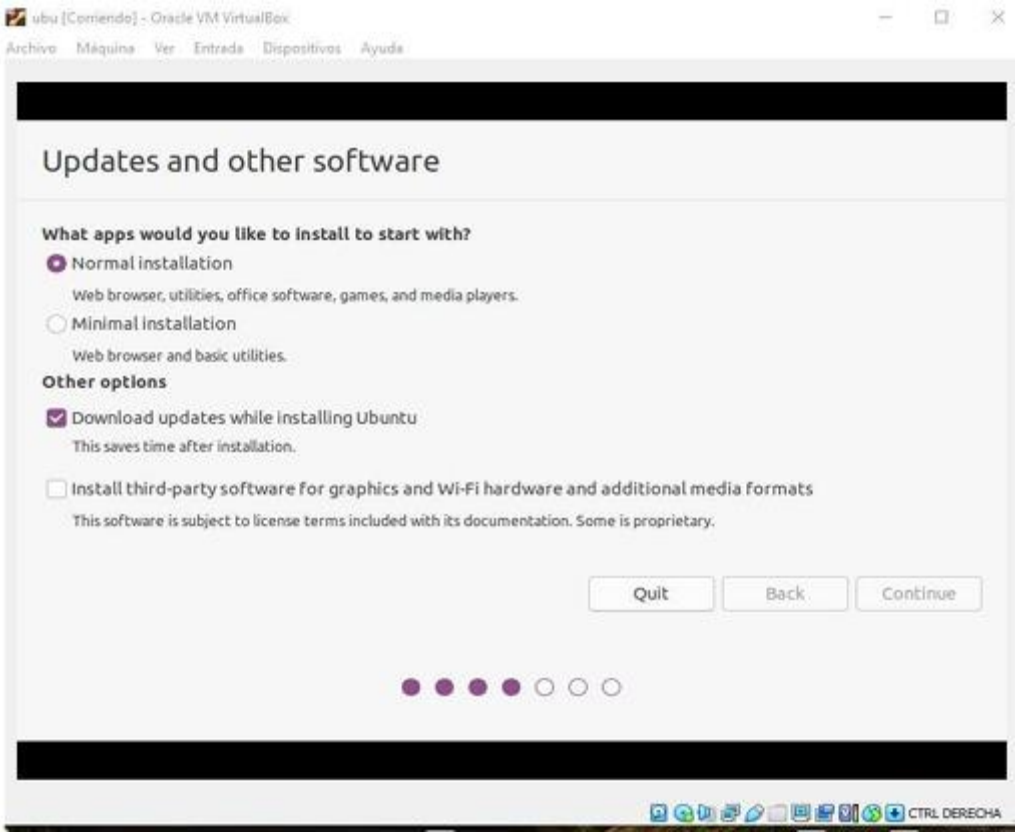
Ventana de instalación kali



Progreso de instalación kali



Ventana instalación ubunto



Instalación actualizaciones Ubuntu

CORPORACIÓN UNIVERSITARIA
UNITEC

Por intermedio del presente documento en mi calidad de autor o titular de los derechos de propiedad intelectual de la obra que adjunto, titulada **Evaluación De Riesgos Y Vulnerabilidades Informáticas Que Se Presentan En Una Organización Del Sector Educativo**, autorizo a la Corporación universitaria Unitec para que utilice en todas sus formas, los derechos patrimoniales de reproducción, comunicación pública, transformación y distribución (alquiler, préstamo público e importación) que me corresponden como creador o titular de la obra objeto del presente documento.

La presente autorización se da sin restricción de tiempo, ni territorio y de manera gratuita. Entiendo que puedo solicitar a la Corporación universitaria Unitec retirar mi obra en cualquier momento tanto de los repositorios como del catálogo si así lo decido.

La presente autorización se otorga de manera no exclusiva, y la misma no implica transferencia de mis derechos patrimoniales en favor de la Corporación universitaria Unitec, por lo que podré utilizar y explotar la obra de la manera que mejor considere. La presente autorización no implica la cesión de los derechos morales y la Corporación universitaria Unitec los reconocerá y velará por el respeto a los mismos.

La presente autorización se hace extensiva no sólo a las facultades y derechos de uso sobre la obra en formato o soporte material, sino también para formato electrónico, y en general para cualquier formato conocido o por conocer. Manifiesto que la obra objeto de la presente autorización es original y la realicé sin violar o usurpar derechos de autor de terceros, por lo tanto, la obra es de mi exclusiva autoría o tengo la titularidad sobre la misma. En caso de presentarse cualquier reclamación o por acción por parte de un tercero en cuanto a los derechos de autor sobre la obra en cuestión asumiré toda la responsabilidad, y saldré en defensa de los derechos aquí autorizados para todos los efectos la Corporación universitaria Unitec actúa como un tercero de buena fe. La sesión otorgada se ajusta a lo que establece la ley 23 de 1982.

Para constancia de lo expresado anteriormente firmo, como aparece a continuación.

Firma 

_____

Nombre CRISTHIAN FERNANDO SUAREZ ANTOLINEZ
CC. 80876434

_____

Nombre EDWARD CAMILO GARCIA SANCHEZ
CC. 1010189038