

Actividad [#3] – [Auditoría y Bitácora ] [“Seguridad Informática II”]

Ingeniería en Desarrollo de Software

**Tutor: Elizabeth Guevara Roa**

**Alumno: Manuel Enrique Ramirez Lopez**

**Fecha: 21/09/2022**

***Indice***

*[Introduccion](#_Toc26927)* [1](#_Toc26927)

*[Justificación](#_Toc1785)* [2](#_Toc1785)

*[Contexto](#_Toc23754)* [3](#_Toc23754)

*[Auditoria y Bitacora](#_Toc20220)* [4](#_Toc20220)

[Auditoría de equipo. 4](#_Toc23015)

[Bitácora 5](#_Toc8015)

[Importancia de seguridad (prevención, monitoreo, auditoría) 6](#_Toc15506)

[Resultados obtenidos 7](#_Toc31881)

*[Conclucion](#_Toc5329)* [8](#_Toc5329)

*[Referencias](#_Toc9507)* [9](#_Toc9507)

# *Introduccion*

A lo largo de la trayectoria recorrida durante estas pocas semanas se an abordado diferentes temas referentes hacia el uso continuo de los procesos ya establecidos donde el principal objetivo de las grandes empresas es mejorar y que no ocurran fallos que pueda perjudicar social y económicamente donde la satisfacer las necesidades del cliente es el principal objetivo y para ello se han visto varios temas que son de suma importancia para lograr estos objetivos:

La detección y prevención de ataques donde la palabra lo menciona prevenir antes que suceda con esto gracias a las diferentes técnicas y herramientas se puede lograr o al menos retrasándolo principalmente ocurre de manera intangible donde se buscan errores de software.

Monitoreo de red ocurre cuando ya tenemos el producto en marcha donde logramos identificar amenazas físicas donde se escanean todos los equipos de la red “local” y se detectan posibles ataques dentro de la red.

A continuación aboraderemos los temas antes mencionados puestos en marcha donde se une el software con el hardware lo físico con lo intangible en un ambiente lo mas cercano a los real...

# *Justificación*

En cualquier organización, las evaluaciones son de primordial importancia ya que nos aseguramos de que se sigan de acuerdo con las pautas establecidas cuando se llevarán a cabo las actividades. Para evitar malas prácticas u omisiones en los procesos que son de suma importancia para entregar el producto con la calidad deseada, otra de las razones por las que realizan este tipo de pruebas es para "prevenir" fallas en el producto que pueden aparecer o desaparecer. información sensible como: datos personales del cliente o información importante sobre métodos de recolección de recursos y así lograr que nosotros como organización valoremos los datos del cliente ya que es la parte más importante del modelo de negocio y siempre nos preguntamos desde el centro de trabajo donde nos encontramos actualmente "Hay una razón para los procesos" para futuras vulnerabilidades o problemas.

# *Contexto*

**Contextualización:** Se pretende utilizar algunas técnicas de protección ante ataques de explotación y obtención de acceso a sistemas de una entidad de crédito. En este sentido, deberás analizar los factores que enfatizan la importancia de la seguridad y que se describen a continuación:

**Escenario principal:** Acrecer es una organización privada dedicada a otorgar préstamos a terceros. Realiza el manejo de la información desde un servidor principal haciendo uso de una base de datos en Oracle. Además, maneja un sistema de control y registro de actividades relacionadas a financieras.

**Escenario secundario:** La financiera requiere el manejo de su seguridad ante posibles ataques, motivo por el cual se te solicita formar parte del proyecto como analista e implementador de mecanismos de seguridad informática. Por consiguiente, el gerente necesita lo siguiente:

● Prevenir los ataques de acceso.

● Prevenir accesos a las redes.

● Validar las licencias de sus recursos por cuestiones de los aspectos legales y regulatorios.

● Control total y auditoría cada semana del sistema, hardware, software, licencias y red.

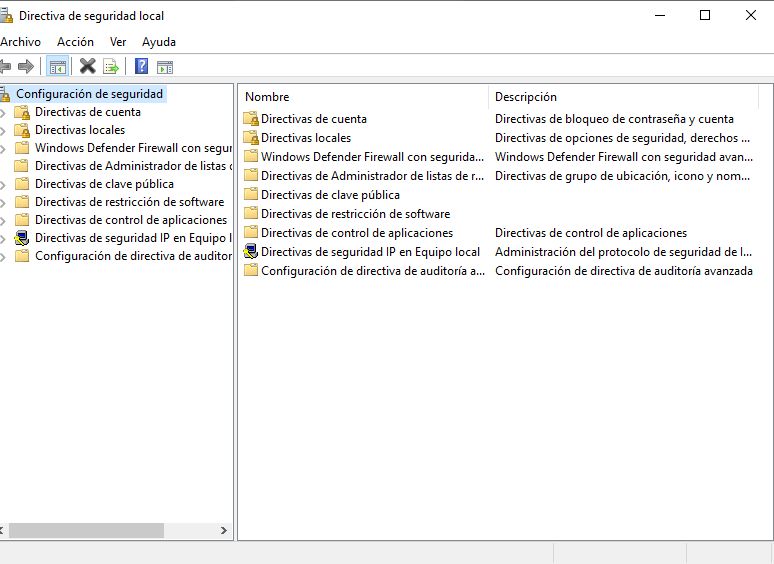
● Monitoreo completo de la red.

● Es importante que se guarde la bitácora, eliminarla e iniciar una nueva para detectar los cambios desde el día 1.

# *Auditoria y Bitacora*

# **Auditoría de equipo.**

# **Bitácora**



## **Importancia de seguridad (prevención, monitoreo, auditoría)**

**● Prevenir los ataques de acceso.**

Al contar con acceso total a la red se mantiene un estricto control de accesos a personas no autorizadas donde los equipos conectados son oficiales y con sus debidas restricciones.

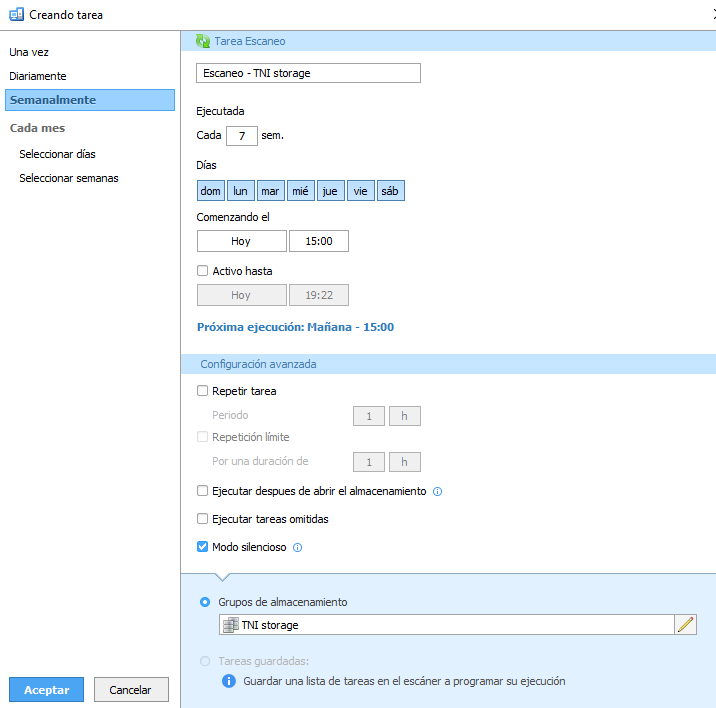
**● Prevenir accesos a las redes.**

Gracias a la infraestructura se mantiene privada el acceso por terceros tanto de alcance por los diversos routers como por interferencia hacia lugares no deseados.

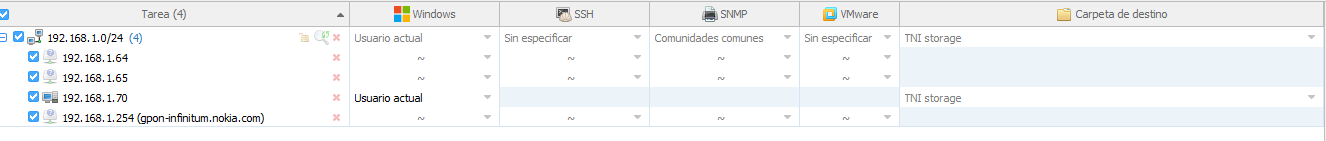
**● Validar las licencias de sus recursos por cuestiones de los aspectos legales y regulatorios.**

Gracias al despliegue remoto que se tiene en las instalaciones se mantiene el constante control sobre las licencias activas y su duración.

**● Control total y auditoría cada semana del sistema, hardware, software, licencias y red.**

Auditorias programadas para la ejecución cada semana adjunto a la revicion de licencias de cada equipo.

**● Monitoreo completo de la red.**

Actualmente los equipos son limitados, esto se logro recabar de el escaneo completo de la red.

## **Resultados obtenidos**

Los resultados obtenidos son los esperados hacia el cliente donde se le garantiza un uso seguro de sus equipos y poder lograr desempeñar sus funciones debidamente, también se implemento la lógica de prevención de ataques hacia las redes activas y acceso a la informacion de la empresa u o clientes.

Gracias a los escaneos programados y la cultura de prevención de ataques se logro que el cliente tenga la seguridad de que cuenta con las bases para mejorarlo a futuro sin muchas complicaciones.

# *Conclucion*

A lo largo de esta unidad se han abordado temas que van desde lo lógico hasta lo físico que son las vulnerabilidades al momento de desarrollar el proyecto cuidando cada rubro o aspecto mínimo gracias a las diferentes metodologías donde se busca prevenir o actuar antes de que sucedan posibles catástrofes y sea mas fácil la corrección para dichos posibles errores, de manera física buscando de manera minuciosa y desde un punto de vista critico por así llamarlo ver y analizar las posibles fallas que puedan llegar a ocurrir por la falta de procesos que podría ser no tener en cuenta dispositivos conectados vía inalámbrica o dejar al descubierto equipos clave con los que puedan ser infectados o falta de capacitación del personal por acciones no debidas en estaciones de trabajo como puede ser el uso de redes sociales o cualquier programa dentro de las estaciones oficiales de trabajo.

En Conclucion las auditorias son para prevenir y dar a conocer y corregir los fallos que han sido descubierto para mejorar a su vez el sistema y o procesos.

# *Referencias*

Lopez, E. (2022). *Monitoreo de Red*. Seguridad informatica 2.

López, E. (2022a). *Detección y Prevención de Ataques de Acceso* . Seguridad Informática 2.

Alva, I. (s. f.). *LA IMPORTANCIA DEL USO DE BITÁCORAS EN COMPONENTES CLAVE COMO ACTIVE DIRECTORY*. Recuperado 20 de septiembre de 2022, de https://blog.smartekh.com/bitacoras-componentesclave-activedirectory