PROCESO DE GESTIÓN DE FORMACIÓN PROFESIONAL INTEGRAL

FORMATO GUÍA DE APRENDIZAJE

IDENTIFICACIÓN DE LA GUIA DE APRENDIZAJE

- **Denominación del Programa de Formación**: Técnico en Control de la Seguridad Digital
- **Código del Programa de Formación**: 233103
- **Nombre del Proyecto**: Aplicación y documentacion de controles de seguridad digital en entornos Empresariales
- **Fase del Proyecto** : Ejecución
- **Actividad de Proyecto**: Caracterizar los incidentes de seguridad
- **Competencia:** Controlar sistema de seguridad de la información de acuerdo con los procedimientos y normativa técnica
- **Resultados de Aprendizaje Alcanzar**: Recopilar información de incidentes de seguridad digital según criterios técnicos, marcos de referencia y modelo del negocio.
- **Duración de la Guía**: 55 Horas

2. PRESENTACIÓN

Esta guía entrega los lineamientos básicos para poner en marcha un Sistema de Gestión de Incidentes de Seguridad de la información, a través de un modelo propuesto, el cual está concebido para que se puedan integrar los incidentes de seguridad sobre los activos de información, independiente del medio en el que se encuentren para guiar y organizar el aprendizaje de manera que se oriente al desarrollo integral del aprendiz.

El objetivo principal del Modelo de Gestión de Incidentes de seguridad de la información es tener un enfoque estructurado y bien planificado que permita manejar adecuadamente los incidentes de seguridad de la información.



Figura tomada de: https://twitter.com/BuroMC/status

Esta guía le permitirá a los aprendices estar preparados para afrontar cada una de las etapas de preparación, detección y anális, contención erradicación - recuperación y actividades post incidentes

definiendo responsabilidades y procedimientos para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

3. FORMULACIÓN DE LAS ACTIVIDADES DE APRENDIZAJE

3.1. Actividades de Reflexión Inicial:

Reconocer algunos aspectos cotidianos relacionados con el control de incidentes en una red empresarial.

Descripción de la(s) Actividad(es):

Los aprendices deberán responder las siguientes preguntas y en grupos de 3 personas realizar la reflexión de cuál es el impacto que tiene en las organizaciones una adecuada política de seguridad.

¿Cuál considera que es el principal rol de un agente de control de seguridad en una empresa en la actualidad?
¿Cuál considera que es la importancia de las gestiones en políticas de seguridad informática en infraestructura de red?
¿Cuál considera que es la importancia de apropiar conocimientos acerca de prevención en seguridad?
¿Qué ventajas traería en una organización poder identificar rápidamente los posibles detecciones en incidentes de seguridad?

El instructor al finalizar ayudará a los aprendices aclarando las dudas sobre la importancia de las políticas de seguridad y su importancia para las redes de la actualidad, tomando como base su experiencia y las presentaciones realizadas por ellos.

Ambiente requerido: Presencial-Taller 32 A-B

Estrategias o técnicas didácticas activas: mesa redonda

Materiales de formación: PC de escritorio, conectividad a internet, TV

Material de apoyo: Academia Cisco NETACAD

Duración de la actividad: 1 horas.

3.2. Actividades de contextualización e identificación de conocimientos necesarios para el aprendizaje

Identificar la terminología y conceptos bases, necesarios para la identificación de incidentes de seguridad mediante la socialización en grupos colaborativos.

Conformando grupos de trabajo o continuando con el mismo grupo de personas de la Actividad de Reflexión, para esta actividad se deben tener algunos conocimientos básicos en los conceptos de seguridad de equipos activos de interconexión como Servidores, Routers y Switches. Con base a dichos conocimientos previos respondan el siguiente cuestionario:

¿Reconozco esto conceptos?	¿ SI o NO?	Si su respuesta es afirmativa de una breve descripción, si no lo conoce, por favor

		consulte y con sus palabras explique la necesidad de conocer de este concepto.
Análisis Forense		
LOG		
Modelo de Gestión de Incidentes		
Evento de seguridad Informatica		
Virus		
Denegación de Servicio		
CSIRT		
POWER SHELL		
ipconfig		
Relación Cliente y un Servidor		

Ambiente requerido: Presencial-Taller 32 A-B

Estrategias o técnicas didácticas activas: mesa redonda

Materiales de formación: PC de escritorio, conectividad a internet, TV

Material de apoyo: Academia Cisco NETACAD

Duración de la actividad: 1 horas.

3.3. Actividades de apropiación del conocimiento (Conceptualización y Teorización)

Reconocer los conceptos teórico-prácticos, que hacen parte del análisis para una red segura.

Esta actvididad se realizara mediante la participación de la socialización de temas por medio de grupos de trabajo colaborativos.

Para el correcto desarrollo de estas actividades, el instructor repartirá la siguiente lista de temas relacionados con el proceso de validación del impactos de los incidentes de seguridad en un ambiente corporativo por medio de la centralización de dispositivos de cómputo (cliente-servidor), se conformarán grupos de trabajo, y entre estos se distribuirán en partes iguales, los temas. Los aprendices deben cumplir con los objetivos teóricos que el instructor plantee y cada uno de ellos plasmarlos en una presentación.

La socialización tendrá una duración aproximada de 4 horas por cada sub-tema, y será acompañado en todo momento del instructor para aclarar cualquier tipo de duda. Además, al finalizar cada sesión, cada grupo deberá disponer de algún método para interactuar con sus compañeros, ya sea quiz, foro o mesa redonda, el cual le permita determinar si los conceptos claves de cada tema han quedado claros en cada aprendiz. Es obligatorio que las diapositivas se realicen usando la plantilla oficial de la institución para PowerPoint. Este y otros factores acerca del buen uso de las herramientas informáticas, serán establecidos y acordados entre el instructor y los aprendices, previo al desarrollo de los siguientes temas. Se le recomienda al instructor evaluar este tipo de aspectos. Lista de temas:

En el primer momento denominado Conceptos básicos de manejo de Servidores, se asignará de forma individual o en parejas, algunos temas, los cuales serán guiados hacia una consulta puntual y satisfactoria, por medio de las indicaciones del instructor. Los conceptos a tratar en este primer momento serán los siguientes que serán desarrollados por el instructor con material de apoyo dentro de las clases.
1. Características y Versiones de Windows Server.
2. Definición de Dominio, Árbol, Bosque.
3. Definición de Objeto, Unidad Organizativa, D.A.

Para los siguientes temas se conformarán equipos de trabajo colaborativos de **máximo 2 personas**, los cuales posteriormente realizarán la consulta acerca del tema entregado a cada uno de los grupos.

1. Instalación y Configuración de Windows Server
2. Configuración D.A y creación de Objetos y UO.
3. Configuración de Servidor DHCP
4. Configuración de Zonas DNS
5. Administración de Objetos en el D.A.
6. Configuración de GPO y unión al dominio
7. Configuración Relación de confianza

Una vez recopilada la información, cada grupo realizara una presentación en una herramienta digital libre. Esta presentación deberá contener (Portada, introducción, definición, características, Ventajas, desventajas, ejemplos de implementación en el sector productivo, Gráficos, entre otros.), La presentación debe ser clara, sencilla, sintetizada.
El instructor acompañará y revisará previamente las presentaciones que contengan la calidad requerida para luego compartir con los demás compañeros.
Este ejercicio de socialización también implica por parte de los grupos la creación de un juego de preguntas en herramientas digitales para lo cual se propone Kahoot.



Imagen 1. configuración de servicios. Fuente: https://n9.cl/pwjlr

Al finalizar se realizará una Socialización de Cierre y solución de dudas por parte del instructor**.**
Una vez finalizadas las socializaciones de los **servicios básicos de servidores en Windows Server,** cada aprendiz de acuerdo con la disponibilidad de equipos del ambiente de aprendizaje deberá realizar el proceso de Instalar el Sistema Operativo Windows Server y configurar Directorio Activo, promoverlo al dominio DNS, crear los objetos : Unidad Organizativa, grupos y usuarios, instalar el rol y características de DHCP, enrutamiento, GPO y relación de confianza entre servidores y verificar que las configuraciones se vean reflejadas al iniciar sesión en el dominio desde un equipo cliente.
Los aprendices deberán registrar en un vídeo o en un documento pdf, el paso a paso de dicha configuración servicio grupal, luego deberá ser compartido con sus compañeros para que ellos apropien esos conceptos con una guía puntual de cómo realizarlo. Deberán realizar un snapshot del M1.

Ambiente requerido: Presencial-Taller 32 A-B

Estrategias o técnicas didácticas activas: mesa redonda

Materiales de formación: PC de escritorio, conectividad internet, TV, Pendrive, SO Windows 10 pro, SO Windows Server 2019 Standard, VMware, Lightshot

Material de apoyo: Academia Cisco NETACAD

Evidencias de aprendizaje: Presentación de PowerPoint de Conceptos básicos y Servicios implementados, que deberá subirla en plataforma y el portafolio del aprendiz. Evaluación de conocimiento Teórico.

Instrumentos de evaluación: Cuestionario, simulación, Taller

Duración de la actividad: 30 horas.

3.4. Actividad de transferencia del conocimiento

3.4.1 Implementar en el Sistema Operativo Windows Server, todos los controles aplicados a equipos y clientes de acuerdo con las buenas prácticas de gestión de la seguridad informática.



Imagen 2. Implementación de NOS. Fuente: https://n9.cl/exkxx

Descripción de la actividad:

Luego que los grupos expusieron y generaron por cada política con sus respectivos informes en vídeo o documento en pdf, cada aprendiz realizará la implementación, configuración y pruebas, donde cada aprendiz deberá evidenciar que está en la capacidad de configurar todos los controles y políticas trabajadas durante las socializaciones, deberán resolver los talleres prácticos del Momento 1.

Finalmente realizaran esas implementaciones en una actividad de simulacro con tiempo asignado para su desarrollo y de esa manera se preparan para la evaluación práctica final.

Ambiente requerido: Presencial-Taller 32 A-B

Estrategias o técnicas didácticas activas: mesa redonda

Materiales de formación: PC de escritorio, conectividad internet, TV, Pendrive, SO Windows 10 pro, SO Windows Server 2019 Standard, VMware, Lightshot

Material de apoyo: Academia Cisco NETACAD

Evidencias de aprendizaje: Informe en un documento pdf, que ilustren el paso a paso de la implementación de todos los servicios, de las configuraciones de las Máquinas Virtuales con Windows Server 2022 y las respectivas pruebas con el cliente con Windows 10 pro, deberá subirla en plataforma y portafolio del aprendiz, El aprendiz deberá presentar una evaluación de conocimiento con un tiempo establecido.

Instrumentos de evaluación: Cuestionario, simulación, Taller

Duración de la actividad: 23 horas.

4. ACTIVIDADES DE EVALUACIÓN

Fase del proyecto formativo	Actividad del proyecto formativo	Actividad de Aprendizaje	Evidencias de Aprendizaje	Criterios de Evaluación	Técnicas e Instrumentos de Evaluación
F3-Ejecución	Caracterizar los incidentes de seguridad	Reconocer algunos aspectos cotidianos relacionados con el control de incidentes en una red empresarial Identificar la terminología y conceptos bases, necesarios para la identificación de incidentes de seguridad mediante la socialización en grupos colaborativos. Reconocer los conceptos teórico-prácticos, que hacen parte del análisis para una red segura. Implementar en el Sistema Operativo Windows Server, todos los controles	**Conocimiento** ✓ Examen Teórico Final Momento 1- Concepto básicos ✓ Examen Teórico de Momento 2- Servicios de Red empresariales. **Desempeño** ✓ Exposición en Power Point de los temas asignados. ✓ Simulación de máquinas virtuales en VMware. ✓ Evaluación Práctica Momento 1- Configuraciones básica de servidor. ✓ Evaluación Práctica Momento 1- Configuraciones Servicios empresariales. **Producto**	Recopilar información de incidentes de seguridad digital según criterios técnicos, marcos de referencia y modelo del negocio. Interpreta la normativa de gestión de incidentes de ciberseguridad según estándares vigentes. Reconoce y asume las funciones y responsabilidades propias de su rol dentro de la estructura del equipo de respuestas de incidentes de seguridad. Interpreta los procesos de gestión de incidentes de seguridad digital según normativa vigente. Reconoce y aplica procedimientos	**Técnica:** Formulación de preguntas **Instrumentos:** Cuestionario. **Técnica:** Observación **Instrumento:** Lista de chequeo **Técnica:** Valoración del producto **Instrumento:** Lista de chequeo

		aplicados a equipos y clientes de acuerdo con las buenas prácticas de gestión de la seguridad informática.	Informe práctico documento pdf de los momentos 1 y 2	de reporte y escalada de incidentes de seguridad digital según procesos definidos por el equipo de respuesta a incidentes. Utiliza herramientas de hardware y software de seguridad digital para el monitoreo y gestión de eventos de seguridad según las especificaciones de los manuales técnicos. Recopila y clasifica los eventos e incidentes de seguridad digital según política de seguridad digital de la organización.	

5. GLOSARIO DE TÉRMINOS

Red: Una red de computadoras es un conjunto de dos o más computadoras o dispositivos conectados entre sí y que comparten información (archivos), recursos (CD-ROM, impresoras, etc.) y servicios (e-mail, Chat, juegos), etc.

Switch: Un conmutador o switch es un dispositivo digital lógico de interconexión de redes de computadoras que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red.

Router: También conocido como enrutador o encaminador de paquetes— es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra.

Usuario: En telecomunicaciones es la persona, organización u otra entidad que depende de los servicios de un sistema de computación para obtener un resultado deseado.

Cliente: es un programa o computadora que accede a recursos y servicios brindados por otro llamado Servidor.

NTFS: (siglas en inglés de New Technology File System) es un sistema de archivos diseñado específicamente para Windows NT, con el objetivo de crear un sistema de archivos eficiente, robusto y con seguridad incorporada desde su base. También soporta compresión nativa de archivos y encriptación (esto último sólo a partir de Windows 2000).

FAT: (File Allocation Table o "tabla de ubicación de archivos") es el principal sistema de archivos desarrollado para MS-DOS y Windows. El sistema de archivos FAT es relativamente sencillo, y debido a eso es muy popular como formato para disquetes. FAT es un sistema de archivos relativamente anticuado, y debido a esto sufre de varios problemas. Su distribución de archivos simple permite la fragmentación, lo que produce eventuales pérdidas en el desempeño de operaciones sobre archivos. FAT no fue diseñado para redundancia en caso de fallos del sistema. Las primeras versiones de FAT permitían nombres de archivo de hasta 11 caracteres (8 para el nombre y 3 para la extensión), aunque esto fue solucionado por Microsoft al inventar VFAT, el cual permite nombres de hasta 255 caracteres. Finalmente, los sistemas de archivos FAT no permiten directivas de seguridad, garantizando el acceso a todos los archivos de una partición por cualquier usuario del sistema operativo.

FAT32: es una versión del sistema de archivos FAT que maneja en teoría hasta 4.294.967.296 unidades de asignación (direccionables con 32 bits, de ahí el nombre) de hasta 32 KB cada una. De estos 32 bits de direccionamiento solo se usan 28 (268.435.456 unidades de asignación) y 18 de éstas están reservadas para el sistema. Por lo tanto, el tamaño máximo teórico de una partición que use FAT32 es de unos 8 TB (268.435.456-18 x 32 KB).

Dominio: es cada nodo que desciende del dominio raíz ".", y representa a una subred nominal (clasificada por nombres, diferente de una subred protocolar clasificada por direcciones IP) dentro del Sistema de Nombres de Dominio (DNS, por sus siglas en inglés).

Dentro de cada dominio puede haber subdominios, dentro de los cuales puede haber otros subdominios, formándose así los nombres de dominio, que generan una estructura de árbol de dominios. La notación textual de los nombres de dominio consiste en una serie ordenada de etiquetas separadas por puntos, y al final el dominio raíz ".", aunque este último no suele escribirse. Por ejemplo, el nombre de dominio www.ejemplo.com consta de cuatro etiquetas, a saber: www.dominio.com, y ".", teniendo como dominio de nivel superior (TLD) a com.

Protocolo de Internet: (IP, de sus siglas en inglés Internet Protocol) es un protocolo no orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados.

TCP/IP: protocolo base de Internet, y sirve para enlazar computadoras que utilizan diferentes sistemas operativos, incluyendo PC, computadoras centrales sobre redes de área local (LAN) y área extensa (WAN).

Firewall: es un elemento de hardware o software utilizado en una red de computadoras para prevenir algunos tipos de comunicaciones prohibidas por las políticas de red, las cuales se fundamentan en las necesidades del usuario.
Confidencialidad: Dado que los datos viajan a través de un medio potencialmente hostil como Internet, los mismos son susceptibles de interceptación, por lo que es fundamental el cifrado de los mismos. De este modo, la información no debe poder ser interpretada por nadie más que los destinatarios de esta.

RPV o VPN: es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

El ejemplo más común es la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo un hotel. Todo esto utilizando la infraestructura de Internet.

Para hacerlo posible de manera segura es necesario proveer los medios para garantizar la autenticación, integridad y confidencialidad de toda la comunicación:

6. REFERENTES BIBLIOGRAFICOS

Infografía:

Microsoft. Glosario (2014). Recuperado el 4 de abril de 2018, de http://www.microsoft.com/latam/technet/recursos/howto/glosario/default.mspx

Luis Pérez. Servicios de Red en Windows (2009). Recuperado el 4 de abril de 2018, de http://www.youtube.com/watch?v=bS9KxsavjRQ&feature=share&list=PLD8234B9EC8FB7DB3

Pablo Martínez. Curso Windows Server 2003 (2010). Recuperado el 4 de abril de 2018, de http://www.youtube.com/watch?v=fzik_HKIFtA&feature=share&list=PLDCAF016C56877B37

Pablo Martínez. Curso Windows Server 2008 (2013). Recuperado el 4 de abril de 2018, de http://www.youtube.com/watch?v=R88q6596pz0&feature=share&list=PLBBC993A6895D054B

Pablo Martínez. Curso Windows Server 2012 (2013). Recuperado el 4 de abril de 2018, de ttp://www.youtube.com/watch?v=agxIxJKpYus&feature=share&list=PLEmsMMOSNtyqGsnjxx-YkPWo1xqu7YyXR

Bibliografía SENA: Recuerde que las credenciales de ingreso son el documento identidad.

Gómez, López, Julio, and López, Oscar David Gómez. Administración de sistema operativos, RA-MA Editorial, 2014. ProQuest Ebook Central
http://ebookcentral.proquest.com.bdigital.sena.edu.co/lib/senavirtualsp/detail.action?docID=3228996

Matthews, Marty. Windows Server 2008: guía del administrador, McGraw-Hill Interamericana, 2009. ProQuest Ebook Central,
http://ebookcentral.proquest.com.bdigital.sena.edu.co/lib/senavirtualsp/detail.action?docID=3191885

Raya, Cabrera, José Luis, and González, Manuel Santos. Sistemas operativos en red, RA-MA Editorial, 2014. ProQuest Ebook Central
http://ebookcentral.proquest.com.bdigital.sena.edu.co/lib/senavirtualsp/detail.action?docID=3229158

7. CONTROL DEL DOCUMENTO

	Nombre	Cargo	Dependencia	Fecha
Autor (es)	**Gustavo Rodríguez Salinas**	Instructor	CEAI	**Abril 15 de 2018**

8. CONTROL DE CAMBIOS (diligenciar únicamente si realiza ajustes a la guía)

	Nombre	Cargo	Dependencia	Fecha	Razón del Cambio
Autor (es)	Diego Fernando Rodríguez Mapallo	Instructor	CEAI	Abril 14-26 de 2021	Actualización de formato y horas
	Luz Dary López R.	Formadora de Instructores	CEAI	21/04/2021	Guía revisada y enviada para ajustes.
	Luz Dary López R.	Formadora de Instructores	CEAI	26/04/2021	Guía revisada y **APROBADA.**

	Sandra Patricia Galíndez	Formadora de Instructores	CEAI	8/11/2023	Guía revisada y **APROBADA.**
Autor (es)	Diego Fernando Rodríguez Mapallo	Instructor	CEAI	29/06/2024	Actualización de formato y horas
	Sandra Patricia Galíndez	Instructor	CEAI		