PROCESO DE GESTIÓN DE FORMACIÓN PROFESIONAL INTEGRAL

FORMATO GUÍA DE APRENDIZAJE

IDENTIFICACIÓN DE LA GUIA DE APRENDIZAJE

- Denominación del Programa de Formación: **Gestión de Redes de Datos**

- Código del Programa de Formación: **228183**
- Nombre del Proyecto (si es formación Titulada): **Diseño, implementación, configuración y gestión de infraestructuras tic para el ambiente de aprendizaje cloud computing del centro de tecnologías agroindustriales**

- Fase del Proyecto (si es formación Titulada): **Ejecución**

- Actividad de Proyecto (si es formación Titulada): **Implementar las políticas de administración de la infraestructura de conectividad.**

- Competencia

  - ✓ **Administración de hardware y software de seguridad en la red**
  - ✓ **Configuración de dispositivos activos de interconexión**
  - ✓ **Gestión de la infraestructura tecnológica de red.**
  - ✓ Configuración de equipos de cómputo

- **Resultados de Aprendizaje Alcanzar:**

✓ Gestionar el estado de la seguridad en la red de datos de la organización y su pertinencia según el plan de seguridad.

✓ Implementar el plan de seguridad en la organización aplicando estándares y normas internacionales de seguridad vigentes

✓ Implementar sistemas de gestión y monitoreo en la red, según estándares, políticas y recursos de la organización.

✓ implementar los servicios red necesarios para cumplir los requerimientos del portafolio de servicios de tecnologías de la información.

- Duración de la Guía: 120 Horas

2. PRESENTACIÓN

La seguridad informática o seguridad de la información es un conjunto de sistemas, métodos y herramientas destinados a proteger bienes, en este caso la información y todos aquellos elementos que participan en su ciclo de vida, estos bienes son también llamados activos, todo activo es un recurso que representa valor para la entidad, así los activos son todos aquellos recursos que facilitan en gran medida el funcionamiento mismo de la entidad, incluyendo las personas.

Cuando abordamos la temática de seguridad identificamos varios términos asociados a esta, si hacemos referencia al termino seguridad de la información, cobijamos todo el espectro de la información, o sea procesos, elementos, dispositivos, personas, entre otros; ahora bien si hablamos de seguridad informática esta solo cubre los aspectos tecnológicos que intervienen dentro del tratamiento y ciclo de vida de la información.

Cuando se habla de seguridad informática o seguridad de la información se distinguen tres componentes esenciales:

- Lo que se quiere proteger (Activos)
- Riesgos y amenazas que atentan contra lo que se quiere proteger.
- Políticas, mecanismos y procedimientos de protección.

Las nuevas prácticas de negocios empresariales han generado una necesidad de salvaguardar y proteger los bienes (activos) con buenas políticas, mecanismos de seguridad y procedimientos estructurados que permitan garantizar el dominio y control sobre ellos. Las redes modernas deben dar cabida a necesidades cada vez mayores para el acceso remoto, seguridad, gestión del ancho de banda, integridad, confidencialidad, no repudio y disponibilidad de la información, sobre estos principios se rige la seguridad informática o seguridad de la información.

En esta fase se debe realizar ciertos procedimientos basados en metodologías de análisis y normas internacionales de seguridad que ayuden a determinar los activos, las amenazas, los riesgos y las vulnerabilidades, para así crear y/o seleccionar las mejores políticas y mecanismos de protección para los bienes de cualquier entidad.

3. FORMULACIÓN DE LAS ACTIVIDADES DE APRENDIZAJE

3.1 Actividades de Reflexión Inicial:

Actividad 3.1.1

Analice y reflexione el siguiente caso:

"La empresa ABC.com dedicada a las ventas online posee una granja de servidores sobre los cuales se soporta no solo toda la infraestructura tecnológica para los procesos internos de la empresa, sino además el aplicativo de e-comerce , este servidor tiene ciertos componentes físicos (hardware) y ciertos componentes lógicos (software) que permiten un buen desempeño según la proyección de compras para sus clientes potenciales, además este servidor cuenta con ciertas configuraciones y elementos que permiten el acceso "seguro" a sus clientes para las compras en línea a través del portal web.

Como bien sabemos en ciertos países se celebran días de promociones (Black Friday), y la empresa tenía planeado ofertar ciertos productos con descuentos para esos días; llegado el día de las promociones, la plataforma presento una falla de seguridad porque en el portal se modificaron los precios de los productos sin autorización ni consentimiento de los responsables de las ventas en línea de la empresa, este inconveniente se debió a un ataque de manipulación de datos (tampering), el cual produjo que desde tempranas horas de la mañana el portal de ventas ofreciera la venta de productos a precios muy bajos lo que represento numerosas pérdidas financieras para la empresa, además de afectar negativamente la imagen corporativa."

La junta directiva de la entidad convoca a una reunión urgente para poder determinar qué área debió identificar, anticipar y mitigar este incidente, además de buscar mecanismos que impidan este tipo de incidentes en escenarios futuros. En el desarrollo de la reunión el área de seguridad, afirma que el problema del ataque se debió a problemas y malas prácticas en la programación y diseño del portal web por lo tanto argumenta que el área de desarrollo de software debe hacerse responsable del incidente argumentando que si se hubieran realizado buenas pruebas a la plataforma de compras se hubiese podido evitar el ataque; mientras que el área de desarrollo de software afirma que el área de seguridad es la responsable, pues es la encargada de proteger los elementos de infraestructura tecnológica ante cualquier posible ataque informático.

Tomando en cuenta los argumentos de ambas áreas, debata en grupos de trabajo (máximo 4 personas) y analicen:

- ¿Qué área tiene la razón respecto a la responsabilidad de anticipar y actuar ante el ataque informático?
- ¿Cree usted que el fallo de seguridad se pudo haber previsto y tomar medidas preventivas para evitar el ataque informático?
- ¿Cuáles fueron las razones principales por las cuales se produjo el ataque informático?
- ¿Cómo se puede mitigar este tipo de incidentes en situaciones futuras?

Comparta sus respuestas con los demás compañeros y discuta la importancia de la seguridad informática/información en las infraestructuras tecnológica, los aprendices participarán manifestando cuáles son los escenarios que conoce y considera viables para la implementación de políticas, mecanismos y procedimientos de seguridad en ambientes tecnológicos.

Actividad 3.1.2

Un Sistema Operativo es importante, ya que controla al computador y actúa como intermediario entre el usuario y la máquina.

El sistema operativo es un programa que al ejecutarse, controla la operación del computador. Por ejemplo, el sistema operativo realiza la tarea de administrar el uso del computador. Los complejos sistemas operativos aumentan la eficiencia y con ello disminuye el costo del uso del computador, puede permitir la operación simultánea al dejar que el programa de un usuario se ejecute mientras se termina la impresión de un usuario o tarea anterior.

Reconocer la importancia del sistema operativo y el software en el funcionamiento de un computar, mediante la observación de las imágenes que se presentan a continuación y posterior respuesta a los interrogantes que se plantean:







- Se ha preguntado en alguna ocasión: ¿Cómo funciona el software en un computador?

- ¿Qué pasaría si un computador no tiene sistema Operativo?
- ¿Qué puede dañar el sistema operativo o software de un computador?
- ¿Cómo se podría arreglar o restaurar el sistema Operativo?

Mencione sistemas operativos que conozcas y cuáles le gustaría aprender y por qué?

Se conforman grupos de trabajo (3-4 aprendices) para socializar las diversas opiniones que se generen frente a la observación de la imagen y las respuestas dada por los aprendices.

El instructor orientará la socialización, retroalimenta y despeja inquietudes.

Tiempo: 10 horas.
Modalidad: Individual y grupal

3.2 Actividades de Conocimientos Previos:

Actividad 3.2.1

En un entorno corporativo con múltiples plataformas tecnológicas, servidores, dispositivos activos de interconexión e información, es necesario la protección de estos bienes para garantizar el buen funcionamiento de los procesos de una empresa, además de salvaguardar la información propiamente sensible por no llamarla confidencial de la entidad. Que procesos, actividades, bienes y normas de seguridad de la información consideraría importante identificar y conocer para garantizar los principios de confidencialidad, integridad, disponibilidad y no repudio sobre ciertos activos de una empresa.?

Reunidos en los grupos de trabajo conformados, cada miembro con sus propias palabras definirá los siguientes términos:

- Análisis de riesgos.
- Análisis de Vulnerabilidades.
- Confidencialidad.
- Integridad.
- Disponibilidad.
- No repudio.
- Políticas de seguridad.

Socialice con el grupo de trabajo sus apreciaciones y compártalas con el instructor en un documento

Actividad 3.2.2

Cuando se identifican amenazas y riesgos para la seguridad de la información y la infraestructura informática, se debe crear un plan de seguridad para mitigar los riesgos y reducir dichas vulnerabilidades, políticas, líneas base de configuración, planes de continuidad y procedimientos para

respuesta a incidentes son necesarios para garantizar el óptimo funcionamiento de la infraestructura informática.

Las políticas de seguridad contemplan un aspecto importante en la protección y acceso a los activos de la entidad, los elementos de seguridad perimetral son considerados imprescindibles para cualquier infraestructura de datos en la protección de los activos frente a accesos no autorizados, ataques e intrusiones, uso inadecuado del canal de comunicaciones y accesos inseguros a los recursos corporativos. Se define perímetro como el espacio (no siempre delimitado físicamente) en el cual convergen redes confiables sobre las cuales tenemos control y gestión y las redes no confiables (normalmente redes externas). Entre los componentes internos y los componentes externos, que elementos perimetrales, procesos y buenas prácticas para la protección de la infraestructura consideraría importante identificar y conocer para garantizar los principios de confidencialidad, integridad, disponibilidad y no repudio sobre ciertos activos de una empresa?.

Reunidos en los grupos de trabajo conformados, cada miembro con sus propias palabras definirá los siguientes términos:

- Perímetro
- Zona desmilitarizada
- Niveles de Seguridad
- Firewall.
- Proxy
- VPN

Actividad 3.2.3

La funcionalidad ***"Propiedades del sistema"*** contiene información sobre las características de los componentes internos del computador. Por ejemplo, el tipo y velocidad del procesador, y de la cantidad de memoria RAM.

3.2.1 Describir las características de su computador y la función de cada componente por medio del siguiente ejercicio.

Para llevar a cabo la actividad es necesario revisar las especificaciones de la CPU y de la memoria RAM que se utiliza en las labores diarias.

En la siguiente figura se muestra un ejemplo de esta información



1. Cada aprendiz debe revisar y conocer las especificaciones completas de un equipo (la información del sistema), luego debe comparar las características de los componentes con los otros equipos (PC). Para ello deben utilizar el siguiente cuadro

2. Componente	Tipo/Descripción	Función
Procesador		
Memoria RAM		
Tamaño de disco Duro		
Sistema Operativo		

Se conformarán grupos de 5 aprendices y por medio de una mímica se socializan las experiencias del ejercicio

El instructor complementará y aclarará dudas de la actividad guiada.

Tiempo: 10 horas.
Evidencia: Tabla diligenciada

Modalidad: Individual y grupal.

3.3 Actividades de Apropiación:

Lea detenidamente el siguiente material de apoyo, para dar desarrollo a la actividad propuesta más adelante:

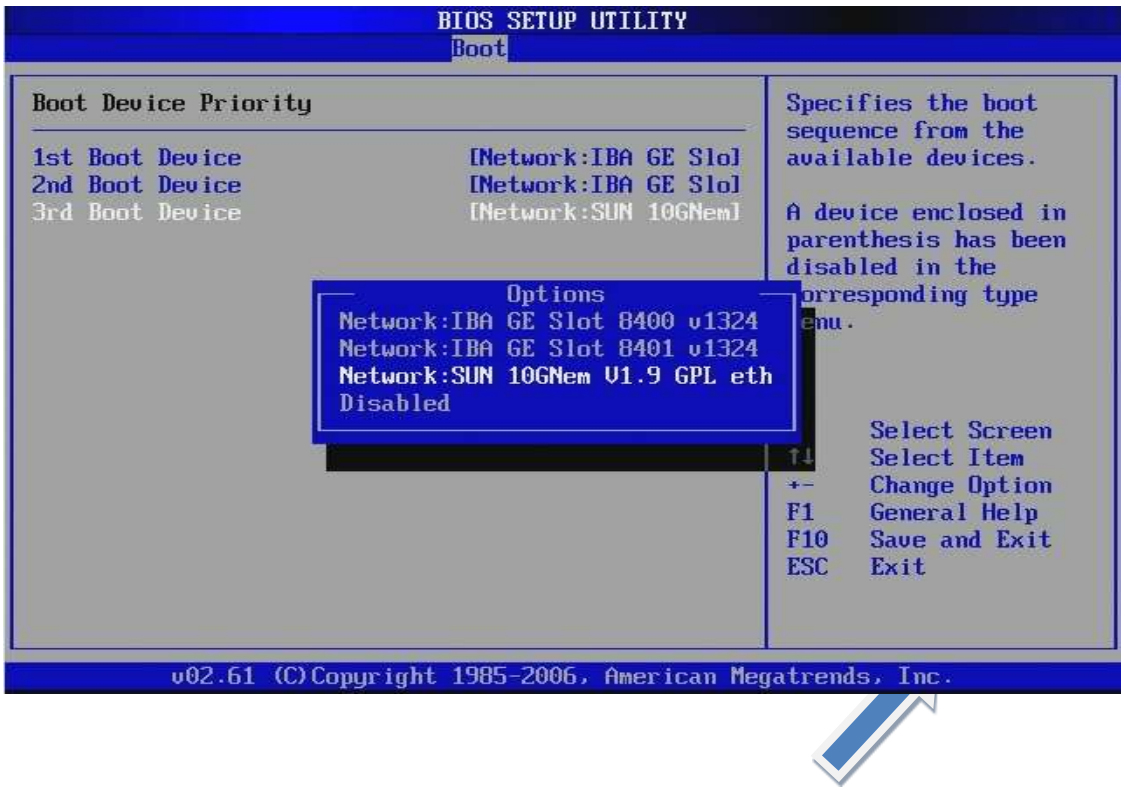
*El **Sistema Básico de Entrada/Salida (Basic Input-Output System)**, conocido simplemente con el nombre de **BIOS**, es un programa informático inscrito en componentes electrónicos de memoria Flash existentes en la placa base. Este programa controla el funcionamiento de la placa base y de dichos componentes.1 Se encarga de realizar las funciones básicas de manejo y configuración del ordenador2*

Después de un reset o del encendido, el procesador ejecuta la instrucción que encuentra en el llamado vector de reset (16 bytes antes de la instrucción máxima direccionable en el caso de los procesadores x86), ahí se encuentra la primera línea de código del BIOS: es una instrucción de salto incondicional, que remite a una dirección más baja en la BIOS. En los PC más antiguos el procesador continuaba leyendo directamente en la memoria RAM las instrucciones (dado que esa memoria era de la misma velocidad de la RAM), ejecutando las rutinas POST para verificar el funcionamiento del sistema y posteriormente cargando un sistema operativo (de 16 bits) en la RAM, que compartiría funcionalidades de la BIOS.

De acuerdo a cada fabricante del BIOS, realizará procedimientos diferentes, pero en general se carga una copia del firmware hacia la memoria RAM, dado que esta última es más rápida. Desde allí se realiza la detección y la configuración de los diversos dispositivos que pueden contener un sistema operativo. Mientras se realiza el proceso de búsqueda de un SO, el programa del BIOS ofrece la opción de acceder a la RAM-CMOS del sistema donde el usuario puede configurar varias características del sistema, por ejemplo, el reloj de tiempo real. La información contenida en la RAM-CMOS e

utilizada durante la ejecución del BIOS para configurar dispositivos como ventiladores, buses y controladores.

Los controladores de hardware del BIOS están escritos en 16 bits siendo incompatibles con los SO de 32 y 64 bits, estos cargan sus propias versiones durante su arranque que reemplazan a los utilizados en las primeras etapas.



Actividad 3.3.1

identificar los conceptos técnicos asociados al entorno de la BIOS, para ello con la ayuda del instructor el aprendiz ingresará a la BIOS del computador y Navegará por el entorno de la BIOS y se apropiara de cada uno de los conceptos.

El aprendiz deberá encender la torre y cuando cargue la primera imagen mantener presionada la tecla **F2** para ingresar a la BIOS, luego navegar por el Menú (indicado por la flecha de la imagen de arriba)

En el siguiente cuadro consignar cada uno de los componentes de la Bios y su descripción:

COMPONENTE	TRADUCION (Deberá traducir al español cada componente)	FUNCION

Actividad 3.3.2

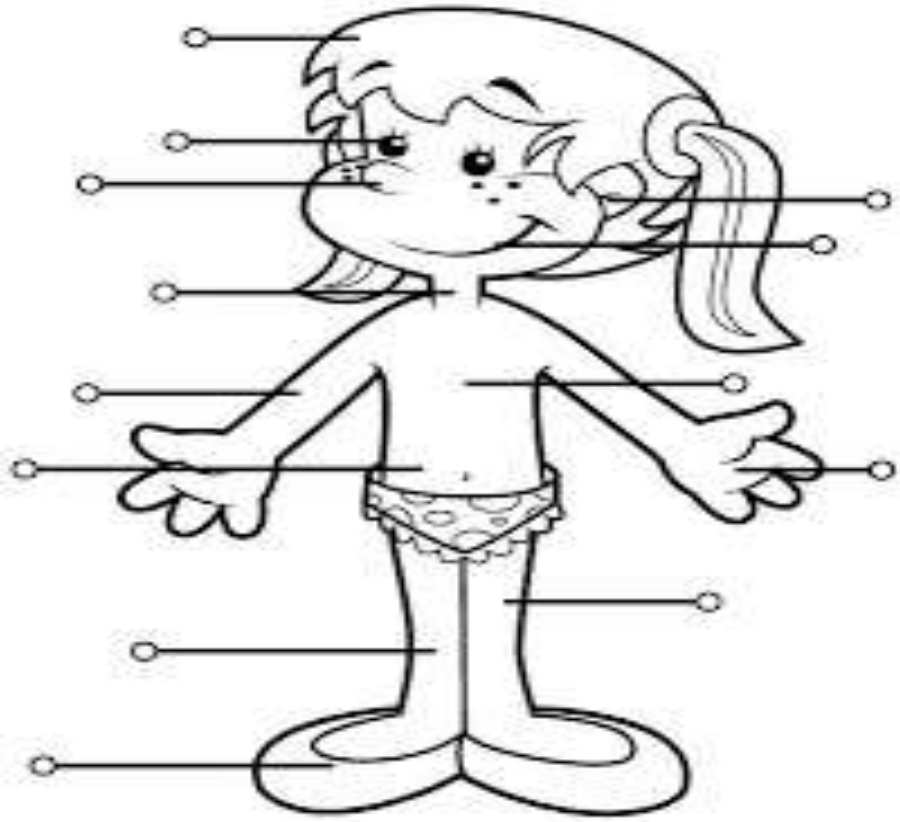
Ingresar a la Cmos-setup del equipo de cómputo tomar pantallazos de cada uno de los siguientes procedimientos y en el siguiente cuadro pegar el pantallazo y realizar la descripción del procedimiento realizado.

- ✓ Como se Ingresa al Setup
- ✓ Boot cd-DVD-USB-RED
- ✓ Deshabilitar puertos USB- LAN-AUDIO
- ✓ Virtualización
- ✓ Guardar y Salir
- ✓ Información del sistema

PANTALLAZOS	DESCRIPCION

De acuerdo con las actividades anteriores en la siguiente figura humana equiparar los componentes de la BIOS con las partes del cuerpo humano utilizando la figura que se encuentra a continuación al terminar en

grupo de tres aprendices deberán representarlo gráficamente y realizar la respectiva sustentación en clases. El instructor resolverá las inquietudes de los aprendices y ampliará los conceptos visto



Tiempo: 30 horas.

Evidencia: Tabla diligenciada y Documento en Word

Modalidad: grupal

Actividad 3.3.3

Análisis de Riesgos, Vulnerabilidades, Auditorias de Seguridad y Normatividad ISO 27000

Descripción de la actividad: Actividad creada para apropiar conceptos de normatividad en seguridad informática, así como la identificación amenazas y vulnerabilidades sobre plataformas tecnológicas, lo que permitirá determinar que políticas y procedimientos pueden mitigar las amenazas y reducirán los riesgos sobre estos activos.

Actividad 3.3.4

Implementación del plan de Seguridad de la Información y soluciones de seguridad perimetral

Descripción de la actividad: Actividad creada para apropiar conceptos de seguridad perimetral, firewalls, VPNS, PROXY, sistemas de prevención de intrusiones y sistemas de detección de intrusiones.

Por comodidad de lectura podrá encontrar la actividad adjunta en el documento con nombre: **Actividad-Implementación del plan de Seguridad de la Información y soluciones de seguridad perimetral** que se encuentra en formato pdf. Cada actividad planteada en dicho documento se validara con una evidencia de conocimiento, producto o desempeño.

3.4 Actividades de Transferencia:

Actividad 3.4.1

Especificar los pasos a seguir para realizar una futura instalación de un sistema operativo a partir de la resolución de las situaciones planteadas en los siguientes estudios de Casos:

Caso 1

Un cliente solicita la revisión de un equipo, con base en las características de su equipo de cómputo, es decir teniendo en cuenta la capacidad de almacenamiento en disco duro, velocidad del procesador (CPU) y la

capacidad de la memoria RAM, Realizar la instalación de un sistemas operativo Windows Capturar el procedimiento y justificar en el siguiente Cuadro:

PASO	JUSTIFICACIÓN DEL PASO
Paso1:	Porque:
Paso1:	Porque:
Paso1:	Porque:
…	
Paso N:	Porque:

Caso 2

Una empresa de tecnología Nueva en el mercado requiere de la instalación de sistemas operativos de 50 equipos de cómputo. La organización necesita ahorrar en la compra de

sus licencias por ello solicita la instalación de software free. Por lo tanto deberá recomendar y especificar los pasos que debe seguir para instalar otro Sistema Operativo diferente a las versiones de Windows (por ejemplo Linux Ubuntu, Mac Os, Chrome OS).

PASO	JUSTIFICACIÓN DEL PASO
Paso1:	Porque:
Paso1:	Porque:
Paso1:	Porque:
…	
Paso N:	Porque:

Los aprendices presentarán en un video los pasos de la instalación de los diferentes sistemas operativos El instructor complementará y aclarará dudas de la actividad guiada.

Tiempo: 31 horas.
Evidencia: Documento en Word y tabla diligenciada
Modalidad: grupal

Actividad 3.4.2

Con base en el conocimiento adquirido en el caso de estudio anterior analice la siguiente situación y plantee una solución tecnológica:

Una empresa que comercializa productos tecnológicos, quiere ampliar sus medios de ventas y plataformas tecnológicas, dentro del crecimiento que ha tenido la empresa no solo ha comprado dos servidores para potenciar su portal web, sino que también ha creado una sucursal en otra ciudad. En los últimos dos meses se ha presentado ciertos ataques al potal web, lo que ha generado pérdidas económicas para la empresa, además han sido víctimas de secuestro de datos y robo de información financiera, los dueños de la empresa solicitan una consultoría con un administrador de red, para que le oriente y le ayude a determinar qué mecanismos de seguridad pueden implementar en la empresa para evitar ser víctimas de más ataques informáticos, además de establecer un canal seguro de comunicación con la sede ubicada en otra ciudad

Tiempo: 10 horas.
Evidencia: Documento en Word y tabla diligenciada
Modalidad: grupal

- Ambiente Requerido

AMBIENTES DE APRENDIZAJE TIPIFICADOS
ESCENARIO (Aula, Laboratorio, taller, unidad productiva) y elementos y condiciones de seguridad industrial, salud ocupacional y medio ambiente
Ambiente de aproximadamente 48 mts2 con capacidad para 35 aprendices, dotado de sillas, mesas, conexiones eléctricas, pantalla para proyectar, buena iluminación y aire acondicionado.

- Materiales

Materiales de formación devolutivos: (Equipos/Herramientas)		**Materiales de formación (consumibles)**	
Descripción	**Cantidad**	**Descripción**	**Cantidad**
Computadores portátiles o de escritorio, con las siguientes características mínimas: • 32 GB de RAM • 500 GB de disco duro • Procesador cuatro núcleos de 2 GHz en adelante	18	• Software de Análisis de Vulnerabilidades y pruebas de Intrusión. • Software para análisis y gestión de riesgos	15
• Switch 24 puertos administrables y con soporte de VLANs • Router con sistema operativo que cumpla con características de seguridad. • Servidor para virtualizar hasta 3 sistemas 5 sistemas operativos tipo server o acceso a nube privada.	5 5 5		

4. ACTIVIDADES DE EVALUACIÓN

Evidencias de Aprendizaje	Criterios de Evaluación	Técnicas e Instrumentos de Evaluación
Evidencias de Conocimiento : Foro grupal con la temática "Planes de contingencia y recuperación de desastres", después de terminar la actividad (A5) ***Evidencias de Desempeño:*** (A1) Verificación del proceso de desarrollo del taller Firewalls. (A2) Verificación del proceso de desarrollo del taller VPNs. (A3) Verificación del proceso de desarrollo del taller PROXY (A4) Verificación del proceso de desarrollo del taller IDS. ***Evidencias de Producto*:** (A5). Verificación de la elaboración de la presentación "planes de contingencia y recuperación de desastres	Implementa las políticas, controles y procedimientos de acuerdo con el plan de seguridad. Implementa los componentes de hardware y software, según políticas y procedimientos técnicos para la organización. Asegura las comunicaciones entre sedes utilizando estrategias de conexión segura como vpn. Instala software de protección de redes como antimalware, antispam y de seguridad perimetral según requerimientos del plan de seguridad. Implementa planes de recuperación de desastres y de continuidad del negocio para los servicios críticos de la organización. Verifica el impacto de la aplicación del plan de seguridad en la reducción del riesgo (plan de tratamiento del riesgo) tomando como referencia la matriz de riesgo. Verifica la aplicación de los controles de seguridad de acuerdo con las políticas establecidas y a los manuales de buenas prácticas definidos en estándares inter	Técnica: Intercambios escritos Instrumento: Registro descriptivo. Técnica: Análisis de producción de alumnos Instrumento: Lista de chequeo Técnica: Análisis de producción de alumnos Instrumento: Lista de chequeo

5. GLOSARIO DE TÉRMINOS

Appliance: Dispositivo o software diseñado con un fin específico para ofrecer servicios determinados en una red de datos. Existen dos tipos de appliances, appliance por hardware que son dispositivos de computo con hardware y firmware diseñado para un fin específico, y appliance por software que es un sistema operativo la mayoría de las veces, el cual se puede desplegar en diferentes arquitecturas de hardware.

Firewall: Appliance de Seguridad que permite el control del tráfico, realizando tareas de filtrado de paquetes y redirección de direcciones y de puertos con base en reglas o listas de control de acceso.

VPN: Red Privada Virtual, es un servicio de red que permite la creación de túneles de comunicaciones seguros, a través de medios inseguros. Existen dos tipos de VPN: VPN punto a punto y VPN de Acceso Remoto.

IDS: Sistema de detección de intrusiones, Sistema informático que alerta de posible ataques de red, con base en patrones de ataque y firmas de ataque.

ANSI (American National Standards Institute), es una organización sin ánimo de lucro que supervisa el de sarrollo de estándares para productos, servicios, procesos y sistemas en los Estados Unidos. ANSI es miembro de la Organización Internacional para la Estandarización (ISO) y de la Comisión Electrotécnica Internacional (International Electrotechnical Commission, IEC).

EIA (Electronic Industries Alliance), es una organización formada por la asociación de las compañías electrónicas y de alta tecnología de los Estados Unidos, cuya misión es promover el desarrollo de mercado y la competitividad de la industria de alta tecnología de los Estados Unidos con esfuerzos locales e internacionales de la política.

•**IEEE (Instituto de Ingenieros Eléctricos y de Electrónica),** principalmente responsable por las especificaciones de redes de área local como 802.3 Ethernet, 802.5 TokenRing, ATM y las normas de GigabitEthernet.

•**ISO (International Standards Organization**), es una organización no gubernamental creada en 1947 a nivel mundial, de cuerpos de normas nacionales, con más de 140 países.

•**OSI:** Modelo de interconexión de sistemas abiertos, es un modelo de referencia para los protocolos de la red de arquitectura en capas, creado en el año 1980 por la ISO.

•**TIA** (TelecommunicationsIndustryAssociation), fundada en 1985 después del rompimiento del monopolio de AT&T. Desarrolla normas de cableado industrial voluntario para muchos productos de las telecomunicaciones y tiene más de 70 normas preestablecidas.

•**1000BASE-LX:** Ethernet para 1000 Mb/s (1 Gb/s) que opera en base a fibra multi-modo con láser de onda larga (1300 nm).
•**1000BASE-SX:** Ethernet para 1000 Mb/s (1 Gb/s) que opera en base a fibra multi-modo con láser de onda corta (850 nm).
•**1000BASE-T:** Ethernet para 1000 Mb/s (1 Gb/s) que usa 4 pares de cables de la categoría 5

•**1000BASE-TX:** Una alternativa de bajo costo frente a la 1000BASE-T que está desarrollando la TIA para el cableado de la categoría 6.

•**100BASE-T4:** Ethernet rápida para 100 Mb/s que usa cable de la categoría 3 formado por 4 pares.

•**100BASE-TX**: Ethernet rápida para 100 Mb/s que usa cable de la categoría 5 formado por 2 pares.

•**100VG-AnyLAN**: LAN para 100 Mb/s LAN que utiliza el Protocolo de Prioridad en la demanda, desarrollado originalmente por la Hewlett Packard y la AT&T para el cable de la categoría 3.

6. REFERENTES BILBIOGRÁFICOS

Saavedra Lopez, Esteban. Seguridad Perimetral en Redes GNU/Linux. Esteban Saavedra Slideshare. Fecha de Consulta: 1 de Febrero de 2017.URL: https://es.slideshare.net/estebansaavedra/introduccin-a-la-seguridad-perimetral-presentation

Título: Ampliar, reparar y configurar su PC
Autor: Durán Rodríguez, Luis
Editor: Marcombo
eisbn: 9788426716491
Año: 2006
Páginas: 608
Idioma: Español

7. CONTROL DEL DOCUMENTO

	Nombre	Cargo	Dependencia	Fecha
Autor (es)	**Walker Johnnier Tobar Pascuas** **Edinson de de Jesus Durando**	**Instructor Redes Cableadas de Telecomunicaciones** **Instructor Electronica y Autimatizacion**	**CTA** **CTA**	**15/01/2020**

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

	Nombre	Cargo	Dependencia	Fecha	Razón del Cambio
Autor (es)					