INSTRUCTOR:

No	NOMBRE	D.I	DD/MM/AA	DD/MM/AA	DD/MM/AA
1	Wendy Katherine Montoya Cano	1046912010	Wendy Montoya	Wendy Montoya	Wendy Montoya
2	Angie Vanessa Zapata Gutierrez	1046913171	Vanessa Z	Vanessa Z	Vanessa Z
3	Deisy Alejandra Cabano Vidales	1007363433	Firma 1	Firma 2	Firma 3
4	German Alberto David Usuga	1046911990	David Usuga G.	David Usuga G	David Usuga G.
5	Beatriz Giraldo Maruland a	1046902094	Betty G 1	Betty G	Betty G
6	Julieth Hernandez. Lopez	1037591420	Julieth H	Julieth H	Julieth H.
7	Miller Arley Perez Arenas	1046.904922	MPEREA	MPEREA	MPEREA
8	Luis Fernando Valencia Duque	1040047445	Firma 1	Firma 2	Firma 3
9	Mariana Patiño Serna	1046917471	Firma 1	Firma 2	Firma 3
10			Firma 1	Firma 2	Firma 3
11			Firma 1	Firma 2	Firma 3
12			Firma 1	Firma 2	Firma 3
13			Firma 1	Firma 2	Firma 3
14			Firma 1	Firma 2	Firma 3
15			Firma 1	Firma 2	Firma 3
16			Firma 1	Firma 2	Firma 3
17			Firma 1	Firma 2	Firma 3
18			Firma 1	Firma 2	Firma 3
19			Firma 1	Firma 2	Firma 3
20			Firma 1	Firma 2	Firma 3
21			Firma 1	Firma 2	Firma 3
22			Firma 1	Firma 2	Firma 3

PROCESO DE GESTIÓN DE FORMACIÓN PROFESIONAL INTEGRAL

FORMATOGUÍA DEAPRENDIZAJE

IDENTIFICACIÓN DE LA GUIA DE APRENDIZAJE

Denominación delPrograma de Formación: GESTION DE REDES DE DATOS

- Código del Programa de Formación: 228183

- Nombre del Proyecto: Implementar una red de datos para la interconexión de equipos, periféricos y dispositivos electrónicos en la multinacional GRAN COLOMBIA ubicada en el municipio de SEGOVIA, EN UN AMBIENTESIMULADO.

- Fase del Proyecto: EJECUCION

- Actividad de Proyecto: AP08 -aplicar buenas prácticas de calidad en la configuracion de dispositivos de computo de acuerdo con las especificaciones del diseño y los protocolos tecnicos, según las necesidades de la multinacional.

- Competencia: administración de hardware y software de seguridad en la red.

- Resultado de aprendizaje: verificar eventos en la infraestructura de red, mediante herramientas y técnicas de análisis de datos que permitan determinar incidentes de seguridad.

- Duración de la Guía: 90 Horas

2. PRESENTACIÓN

En los inicios las redes de datos no se cifraban porque no veían necesario realizar esta acción cuando empezaron a realizar ataques a la seguridad de dichas redes se vio la necesidad de implementar métodos para protegerlas, una de las soluciones fue implementar VPN (Virtual Prívate Network) en español Red privada Virtual es una tecnología de red que nos brinda una mejora sustancia la seguridad de una red LAN generalmente encaminada a una red WAN, esto se logra creando un túnel virtual que enlaza dos o más puntos con la característica que dicho túnel va cifrado lo cual impide que sea leído en claro por un atacante potencial. Las VPN más comunes son las de sitio a sitio en la cual se interconectan dos sedes y la de sitio remoto en la cual desde cualquier parte del mundo me conecto con un cliente VPN aun servidor VPN a través de su dirección pública y me permite accedera la red local como si estuviera en ella.

3. FORMULACIÓN DE LAS ACTIVIDADES DE APRENDIZAJE

Descripción de la(s) Actividad(es):

31 Responde los siguientes ítems, apoyándote en Internet y la bibliografía propuesta.
311 Liste los posibles problemasque tendría el comunicarme a través de internet sin ninguna seguridad.
312 Realice una descripción de que son las redes virtuales privadas y evolución.
313 Identifique los tipos más comunes de VPNs y realice unabreve descripción
314 ¿Cuáles son los puertos que utilizan las VPNs PPTP e IPSec?
315 Identifique 2 equipos activos que soporten la implementación de VPN y muestre su hoja de especificaciones.

4. ACTIVIDADES DE EVALUACIÓN

Tome como referencia la técnica e instrumentos de evaluación citados en la guía de Desarrollo Curricular

Evidencias de Aprendizaje	Criterios de Evaluación	Técnicas e Instrumentos de Evaluación
Evidencias de Conocimiento : Con el propósito de reflexionar y de hacer visible los conocimientos previos que tiene sobre el tema, establezca un análisis de las siguientes cuestiones: 1. ¿Conoce algún software de simulación de redes? 2. ¿Comprende la estructura de una dirección IPV4 y la de una dirección IPV6? 3. ¿Entiende algo de migración o cómo se implementa el protocolo IPV6?	Implementa el plan de seguridad diseñado, instalando el hardware y software, métodos y algoritmos de cifrado, asegurando las instalaciones físicas y eléctricas de la organización, configurando perfiles de usuario, configurando detectores de intrusos, estableciendo conexiones seguras, implementando mecanismos de control técnicos, operativos y administrativos, poniendo en marcha el plan de contingencia y recuperación de desastres, para la organización a nivel de equipos de seguridad, servidores, clientes y equipos	Técnica: Valoración de producto Instrumento: Listade chequeo

Evidencias de Desempeño Lea y analice el material de formación de la actividad 2 “Configuración de dispositivos activos y servicios para IPV6” que se encuentra en el botó “actividad 2” además, revise los materiales de apoyo o complementarios para realizar esta actividad. Uno de los objetivos de este programa de formación es que el aprendiz comprenda los servicios de red y algunos dispositivos activos con IPV6, así como la simulación de los dispositivos con Packet tracer. Para realizar la actividad de aprendizaje debe: - Realizar la lectura cuidadosa del Material de formación 2, en versión interactiva y descargable, seguidamente realizar las siguientes tareas: Ejecutar la	activos, siguiendo las normas internacionales vigentes	

actividad interactiva: “Actividad 2 – Evidencia 1 “Protocolo IPV6". Recuerde que: vidad interactiva “Actividad 2 – Evidencia 1” es evaluable. • En esta se debe identificar los componentes del encabezado de IPV6, en el primer ambiente debe identificar en el gráfico los componentes correctos, y en el segundo ambiente correlacionar la columna a con la columna b correspondiente al concepto y estructura del IPV6. Cuenta con el espacio de las sesiones en línea, en donde el instructor aborda el tema del material de formación, explica las actividades que contiene la guía de aprendizaje, resuelve dudas y da orientaciones generales para la próxima actividad.		

Evidencias de Producto: De acuerdo a los conocimientos adquiridos en el material de formación 2 y el material de apoyo, el aprendiz estará en capacidad de realizar el ejercicio, luego de instalar el software, debe realizar la simulación en packet tracert de 3 routers con el protocolo IPV6. Actividad práctica mediante software simulación packet tracer" configuración dispositivos activos para IPV6" "Actividad 2 – evidencia 2" Como evidencia debe crear en packet tracer la topología y configurar los routers de acuerdo a la simulación suministrada.		

5. GLOSARIO DE TÉRMINOS

Internet Engineering Task Force (IETF) (en español, Grupo de Trabajo de Ingeniería de Internet1): Es una organización internacional abierta de normalización, que tiene como objetivo el contribuir a la ingeniería de Internet, actuando en diversas áreas, como transporte, encaminamiento, seguridad. Se creó en los Estados Unidos, en 1986.

Dirección anycast: Es una dirección del rango reservado para las direcciones unicast que identifica múltiples interfaces y es empleada para la entrega de uno a uno-entre-varios. Con un rutado apropiado, los datagramas dirigidos a una dirección de tipo anycast serán entregados en un único interfaz, elmás cercano.

Dirección anycast de router de subred: Dirección anycast (prefijo de 64 bits::) que se asigna a las interfaces de los routers. Dirección de uso local: Dirección unicast IPV6 que no es alcanzable en la Internet IPV6. Las direcciones de uso local incluyen direcciones locales del enlace y direcciones locales del sitio.

Dirección MAC: Dirección de nivel de enlace de tecnologías típicas de redes locales como Ethernet, Token Ring y FDDI. También se conoce como dirección física, dirección del hardware o dirección deladaptador de red.

Dirección multicast: Es una dirección que identifica múltiples interfaces y que se emplea en entregas de datos uno-a-muchos. Mediante la topología de rutado multicast apropiada, los paquetes dirigidos a una dirección multicast se entregarán a todas las interfaces identificadas por ella.

Dirección unicast: Dirección que identifica a una única interfaz y que permite comunicaciones punto a punto a nivel de red. El alcance o ámbito de utilización de esa dirección es precisamente aquel en el que esa dirección es única.

DNS: (Domain Name System.) Servidor de nombre de dominio. DHCP (Dynamic Host Configuration Protocol): Un protocolo de configuración con estado ("stateful") que proporciona direcciones IP y otros parámetros de configuración para conexión a una red IP.

6. REFERENTES BILBIOGRÁFICOS

BIBLIOGRAFIA http://biblioteca.sena.edu.co Procesos y herramientas para la seguridad de redes. (2014). Retrieved from http://ebookcentral.proquest.com.bdigital.sena.edu.co Díaz, G., Mur, F., & Sancristóbal, E. (2004). Seguridad en las comunicaciones y en la información. Retrieved from http://ebookcentral.proquest.com.bdigital.sena.edu.co Baca, U. G. (2016). Introducción a la seguridad

informática. Retrieved from http://ebookcentral.proquest.com.bdigital.sena.edu.co J. C. (2014). Seguridad informática. Retrieved from http://ebookcentral.proquest.com.bdigital.sena.edu.co Carceller, C.
R., Campos, S. C., & García, M. C. J. (2013). Servicios en red. Retrieved from http://ebookcentral.proquest.com.bdigital.sena.edu.co

6. CONTROL DEL DOCUMENTO

	Nombre	Cargo	Dependencia	Fecha
Autor (es)	DIANA CAROLINA LOZANO DIAZ	INSTRUCTORA SISTEMAS	CTMAE	06-11-2020

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

	Nombre	Cargo	Dependencia	Fecha	Razón del Cambio
Autor (es)					




Smile


26/07/2022 19:43


Smile






Smile

LISTA DE CHEQUEO CUMPLIMIENTO INFRAESTRUCTURA TECNOLOGICA

No	REQUERIMIENTO	CUMPLE	NO CUMPLE	COMO LO CUMPLE	NÚMERO DE FOLIO
1	Normatividad aplicable Circular Externa No. 022 de 2010 antes Circular Externa No. 052 de 2007 de la Superintendencia Financiera de Colombia				
2	Aportes tecnológicos a cargo del proponente				
3	Requerimientos y especificaciones del software				
4	Software propio del proponente				
5	Requerimientos mínimos del sistema de información del proponente				
6	Módulo de generación de informes				
7	Módulo de supervisión en línea				
8	Modulo de evaluación de conocimientos				
9	Características mínimas del sistema de información del proponente				
10	Otros requerimientos tecnológicos				
11	Requerimientos mínimos de atención contact center				
12	Requerimientos mínimos de atención virtual				
13	IVR (Interactive Voice Response).				
14	ACD (Distribuidor inteligente de llamadas).				
15	Grabación de llamadas.				
16	Enrutamiento por habilidades.				
17	Enrutamiento por reglas de negocio.				
18	Retenedores de atención.				
19	Recuperación de abandonos.				
20	Notificación de tiempos en espera.				
21	Notificación de posición en espera.				
22	Priorización de nivel en cola.				
23	Transferencia inteligente con CTI (Pop-Up).				
24	Funciones para envío masivo de Email.				
25	Funciones para envío de fax.				
26	Reporte por disposiciones de IVR.				
27	Reportes por actividad de nodos IVR.				
28	Recuperación de abandonos en cola – ANI.				
29	Menús inteligentes por perfil del cliente, de tal manera que cuando un cliente llama se le presente los datos específicos de su interés.				
30	Balance de carga chat.				
31	Requerimientos mínimos de atención escrita				
32	Requerimientos mínimos de atención personalizada				
33	Requerimientos mínimos de atención PBX				
34	Requerimientos mínimos de atención de grandes clientes				
35	Requerimientos mínimos del software básico de los computadores personales provistos por el proponente				
36	Requerimientos referentes al hardware				
37	Hardware mínimo requerido para todos los canales de servicio				
38	Servidores de comunicaciones				
39	Computadores personales				
40	Multifuncionales e impresoras				
41	Digiturnos				
42	Soporte para la infraestructura tecnológica				
43	Requerimientos referentes a telecomunicaciones				
44	Requerimientos referentes a la continuidad de la operación del negocio				
45	Requerimientos referentes a seguridad de la información				
46	Plan actual de contingencia y continuidad del negocio				
47	Reserva y confidencialidad de la información				
48	Requerimientos especiales gobierno en línea				
49	Análisis y caracterización				
50	Interacción servicio al ciudadano				
51	Seguimiento a solicitudes, peticiones quejas, reclamos y denuncias				
52	Soporte en línea				
53	Certificaciones y constancias				
54	Priorización y planeación de cadenas de trámites y ventanillas únicas				
55	Retroalimentación del plan para la participación				
56	Especificaciones y obligaciones relacionadas con las interfaces del proyecto				