PROCESO DE GESTIÓN DE FORMACIÓN PROFESIONAL INTEGRAL
FORMATO GUÍA DE APRENDIZAJE

IDENTIFICACIÓN DE LA GUIA DE APRENDIZAJE

- **Denominación del Programa de Formación:** Tecnólogo en Gestión de Redes de Datos.
- **Código del Programa de Formación:** 538201.
- **Nombre del Proyecto (si es formación Titulada):** Implementación y Administración de la Infraestructura de Red Convergente y en la Nube de Acuerdo al Diseño, Tecnologías Disponibles y Necesidades Del Cliente.
- **Fase del Proyecto (si es formación Titulada):** Fase III. Gestión de la Infraestructura Informática.
- **Actividad de Proyecto(si es formación Titulada):** Implementación de las Soluciones de Gestión Informatica.
- **Competencia:** Gestión de la Infraestructura Tecnológica de Red.
- **Resultados de Aprendizaje Alcanzar:** Planificar la Implementación de Plataformas de Gestión y Monitoreo Según Parámetros Definidos en la Solución.
- **Duración de la Guía**: 60 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.

Desde hace años existe una mayor conciencia acerca de la importancia de asegurar los procesos de transmisión de datos en internet, ya que esto podría poner en riesgo nuestras contraseñas personales, cuentas de banco, la base de datos de los clientes de un negocio o incluso información altamente confidencial que causaría enormes pérdidas y daños si se hiciera pública de forma indebida. Es aquí donde el SENA, enfocará a lo largo de este resultado de aprendizaje, los conceptos y las implementaciones necesarias, para que los Tecnólogos en Gestión de Redes de Datos puedan implementar soluciones de servicios (protocolos) seguros en el sector empresarial e Internet.

3. FORMULACIÓN DE LAS ACTIVIDADES DE APRENDIZAJE

✧ **Actividades de Reflexión Inicial.**

Actividad: Reflexionar acerca de cómo las telecomunicaciones influyen en el diario vivir de la sociedad según el uso dado a las mismas.
Duración: 60 minutos.

Los Aprendices en mesa redonda reflexionarán acerca de cómo las *comunicaciones/telecomunicaciones* afectan la sociedad en la que viven y el impacto de la misma en su desarrollo como individuo. Una vez finalizada se hará la retroalimentación del tema y los aprendices responderán la siguiente pregunta:

¿Cómo impactan las tecnologías de comunicación/telecomunicación su proceso de formación?

¿Qué importancia tiene la confidencialidad en sus transacciones web diarias?

¿Usaría usted un servicio sabiendo que sus datos personales pueden ser facilmente vistos o interceptados por un delincuente en la red?

Ambiente Requerido: Ambiente de aproximadamente 48 mts2 con capacidad para 30 aprendices, dotado de sillas, mesas, conexiones eléctricas y de datos, pantalla para proyectar, buena iluminación y aire acondicionado.

Materiales: Lápices, lapiceros, hojas de block, computadores portátiles o de escritorio, con las estas características mínimas: 8 GB de RAM 500 GB de disco duro, procesador cuatro núcleos de 2 GHz en adelante; y licencias de Sistemas Operativos .

✧ **Actividad de contextualización e identificación de conocimientos necesarios para el aprendizaje.**

Actividad: Relacionar los principales conceptos de seguridad en redes con las amenazas presentes en las mismas, según el tipo de amenaza.
Duración: 120 minutos.

El instructor presentará a los aprendices los siguientes videos: *Seguridad en redes de datos* https://www.youtube.com/watch?v=7qjNJxH-0fU y *Qué y cómo funciona un certificado de seguridad SSL/TLS* https://www.youtube.com/watch?v=tHhFQaurGAg y una vez terminados los aprendices harán un cuadro conceptual sobre las principales amenazas a la seguridad informática.

El aprendiz hará un análisis de la imagen presentada a continuación "*Pilares de la seguridad*" y definirá con base en ésta y su opinión personal (sin buscar ni consultar ninguna bibliografía/webgrafía) los diferentes elementos que conforman dicha imagen; después responderá la siguiente pregunta: *¿Cual pilar cree que es más importante y porqué?*.



Figura 1. Pilares de la seguridad. Imagen tomada de http://normasdeseguridada1.blogspot.com/2016/10/objetivos-de-la-seguridad-informatica.html

Mediante un sondeo o lluvia de ideas los aprendices hablarán acerca de los conceptos de seguridad y criptografía más relevantes de los cuales tengan conocimiento. El instructor puede guiar la actividad para que los aprendices hablen acerca de los siguientes tópicos:

- ✓ *Protocolos inseguros.*
- ✓ *Protocolos seguros.*
- ✓ *Puertos de conexión seguros.*
- ✓ *Encriptado de datos.*
- ✓ *HTTPS.*
- ✓ *Amenazas y riesgos (informática e información).*

Ambiente Requerido: Ambiente de aproximadamente 48 mts2 con capacidad para 30 aprendices, dotado de sillas, mesas, conexiones eléctricas y de datos, pantalla para proyectar, buena iluminación y aire acondicionado.

Materiales: Lápices, lapiceros, hojas de block, computadores portátiles o de escritorio, con las estas características mínimas: 8 GB de RAM 500 GB de disco duro, procesador cuatro núcleos de 2 GHz en adelante; y licencias de Sistemas Operativos.

✧ **Actividades de apropiación del conocimiento (Conceptualización y Teorización).**

Actividad: Identificar los elementos principales del cifrado de conexiones de extremo a extremo utilizando SSL/TLS, mediante el desarrollo de conceptos según estudio de caso.
Duración: 6 horas.

El aprendiz mediante la revisión del material de apoyo provisto por el instructor (*Seguridad Informática - Criptografía*) en la Plataforma Territorium y mediante búsquedas en Internet desarrollará la sección de consulta de conceptos de la actividad "Taller Configuración de Servicios de Red Seguros" disponible en la plataforma Territorium.

Una vez realizada la actividad el aprendiz construirá un mapa conceptual de los elementos más representativos y que considere más importante acerca de lo aprendido. El instructor hará retroalimentación del tema.

Ambiente Requerido: Ambiente de aproximadamente 48 mts2 con capacidad para 30 aprendices, dotado de sillas, mesas, conexiones eléctricas y de datos, pantalla para proyectar, buena iluminación y aire acondicionado.

Materiales: Lápices, lapiceros, hojas de block, computadores portátiles o de escritorio, con las estas características mínimas: 8 GB de RAM 500 GB de disco duro, procesador cuatro núcleos de 2 GHz en adelante; programas de virtualización de Sistemas Operativos y licencias de Sistemas Operativos.

✧ **Actividades de transferencia del conocimiento.**

Actividad: Implementar los servicios de una Infraestructura de Clave Pública (*PKI*) para asegurar los servicios de red utilizando Certificados SSL/TLS, según caso de estudio.
Duración: 20 horas.

El aprendiz desarrollará la sección de implementación de la actividad "*Actividad Configuración de Servicios de Red Seguros*" disponible en la plataforma Territorium, donde implementará una solución que resuelva las necesidades de una empresa por medio del aseguramiento de los servicios de red ofrecidos por la misma.

Cuando termine la implementación subirá las evidencias solicitadas de la misma a la plataforma Territorium mediante el enlace dispuesto para tal fin. Una vez revisada la actividad, se darán las conclusiones de la misma y se hará la retroalimentación respectiva.

Ambiente Requerido: Ambiente de aproximadamente 48 mts2 con capacidad para 30 aprendices, dotado de sillas, mesas, conexiones eléctricas y de datos, pantalla para proyectar, buena iluminación y aire acondicionado.

Materiales: Lápices, lapiceros, hojas de block, computadores portátiles o de escritorio, con las estas características mínimas: 8 GB de RAM 500 GB de disco duro, procesador cuatro núcleos de 2 GHz en adelante; programas de virtualización de Sistemas Operativos y licencias de Sistemas Operativos.

4. ACTIVIDADES DE EVALUACIÓN

Evidencias de Aprendizaje	Criterios de Evaluación	Técnicas e Instrumentos de Evaluación
Evidencias de Conocimiento: *Evaluación de conocimientos de conceptos y principios teóricos sobre criptografía y aseguramiento de servicios de red.* **Evidencias de Desempeño:** *Cumplimiento de la lista de chequeo en habilidades donde el aprendiz demuestre sus destrezas y habilidades sobre criptografía y aseguramiento de servicios de red.*	*Caracteriza el entorno y los recursos a ser gestionados y monitoreados de acuerdo con marcos de referencia, criterios técnicos y necesidades de la organización.* *Planea la implementación de las estrategias de gestión y monitoreo según caracterización de la empresa.* *Apropia las plataformas y recursos tecnológicos necesarios para la gestión y monitoreo de la infraestructura presente en la organización.* *Reconoce los estándares y líneas base de configuración de las plataformas de monitoreo y gestión elegidas según necesidades de la organización.*	**Técnica**: Pregunta **Instrumento**: Cuestionario **Técnica**: Observación **Instrumento**: Lista de Chequeo

Verificación de las máquinas virtuales y las configuraciones realizadas en las mismas para el aseguramiento de los servicios de red. **Evidencias de Producto:** *Talleres de conocimiento y Presentación de informes con los manuales en formato digital de la implementación aseguramiento de servicios de red.*	*Define las estrategias y métodos de recolección de datos de monitoreo.* *Valida que las especificaciones técnicas del software de gestión y monitoreo se ajusten a los requerimientos y necesidades de la organización.* *Comprueba que los mecanismos de recolección de datos de monitoreo se ajustan a las plataformas, acorde con criterios técnicos y requerimientos definidos.* *Verifica que el software de gestión y monitoreo cumple con criterios técnicos y de funcionamiento requeridos por la organización.*	**Técnica**: Observación **Instrumento**: Lista de Chequeo

5. GLOSARIO DE TÉRMINOS

ACTIVO: Recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente.

AMENAZA: Es un evento que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

ATAQUE: Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

AUTORIDAD CERTIFICADORA: a veces abreviadas como AC o CA (por las siglas del término inglés Certification Authority), son entidades de confianza que emiten certificados digitales.

CERTIFICADO DIGITAL: es un vínculo entre una clave pública y una identidad de usuario, que se consigue mediante una firma digital por una tercera parte o autoridad de certificación (AC) que publica su clave pública en la que TODOS confían.

CRIPTOANÁLISIS: Técnica consistente en comprometer la seguridad de un criptosistema. Esto se puede hacer descifrando un mensaje sin conocer la clave, o bien obteniendo a partir de uno o más criptogramas la clave que ha sido empleada para su codificación.

CRIPTOGRAFÍA: Rama inicial de las Matemáticas y en la actualidad de la Informática y la Telemática, que hace uso de métodos y técnicas con el objeto principal de cifrar y/o proteger un mensaje o archivo por medio

de un algoritmo, usando una o más claves. Funciona a través de la utilización de cifras o códigos para escribir algo secreto en documentos y datos confidenciales que circulan en redes locales o en internet.

HTTPS: El Protocolo seguro de transferencia de hipertexto (en inglés: Hypertext Transfer Protocol Secure o HTTPS), es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de Hipertexto, es decir, es la versión segura de HTTP.

PKI: Una infraestructura de clave pública (*en inglés: Public Key Infrastructure –PKI–*) es una combinación de hardware, software, y políticas y procedimientos de seguridad, que permiten la ejecución con garantías de operaciones criptográficas, como el cifrado, la firma digital, y el no repudio de transacciones electrónicas. El término PKI se utiliza para referirse tanto a la autoridad de certificación y al resto de componentes, como para señalar, de manera más amplia y a veces confusa, al uso de algoritmos de clave pública en comunicaciones electrónicas. Este último significado es incorrecto, ya que no se requieren métodos específicos de PKI para usar algoritmos de clave pública.

RIESGO: Posibilidad de que se produzca un impacto determinado en un activo o en toda la Organización.

SEGURIDAD INFORMÁTICA: es un conjunto de sistemas, métodos y herramientas destinados a proteger un bien, el mas importante de ellos la información, en este proceso participan además personas.

SSL: es el acrónimo de Secure Sockets Layer (capa de sockets seguros), la tecnología estándar para mantener segura una conexión a Internet, así como para proteger cualquier información confidencial que se envía entre dos sistemas e impedir que los delincuentes lean y modifiquen cualquier dato que se transfiera, incluida información que pudiera considerarse personal.

TLS: (Transport Layer Security, seguridad de la capa de transporte) es solo una versión actualizada y más segura de SSL. Si bien aún denominamos a nuestros certificados de seguridad SSL porque es un término más común, al comprar certificados SSL en Symantec, en realidad se compran los certificados TLS más actualizados con la opción de cifrado ECC, RSA o DSA.

VULNERABILIDAD: Posibilidad de ocurrencia de la materialización de una amenaza sobre un activo.

6. REFERENTES BILBIOGRÁFICOS

- http://www.dma.fi.upm.es/recursos/aplicaciones/matematica_discreta/web/aritmetica_modular/criptografia.html
- https://www.pabloyglesias.com/mundohacker-esteganografia/
- https://www.escueladeinternet.com/funcionan-las-autoridades-certifican-los-ssl/
- https://www.upv.es/contenidos/CD/info/711545normalc.html
- https://tecnologia-informatica.com/que-es-la-criptografia/

- https://www.redalia.es/ssl/protocolo-ssl/
- https://es.wikipedia.org/wiki/Protocolo_seguro_de_transferencia_de_hipertexto
- https://revista.seguridad.unam.mx/numero-10/el-cifrado-web-ssltls
- https://windowserver.wordpress.com/2011/02/26/criptografa-e-infraestructura-de-clave-pblica-pki/
- https://www.digitalocean.com/community/tutorials/how-to-create-a-self-signed-ssl-certificate-for-apache-on-centos-8
- https://techexpert.tips/es/iis-es/habilitar-https-en-iis/

7. CONTROL DEL DOCUMENTO

	Nombre	Cargo	Dependencia	Fecha
Autor (es)	Rodrigo Ebrat Carr	Instructor	CESGE	05/10/2021

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

	Nombre	Cargo	Dependencia	Fecha	Razón del Cambio
Autor (es)					