PROCESO DE GESTIÓN DE FORMACIÓN PROFESIONAL INTEGRAL

FORMATO GUÍA DE APRENDIZAJE

IDENTIFICACIÓN DE LA GUIA DE APRENDIZAJE

- **Denominación del Programa de Formación:** Sistemas Teleinformáticos
- **Código del Programa de Formación:** 233108 V1
- **Ficha:** 3100110
- **Nombre del Proyecto (si es formación Titulada):**
  Implementación de Soluciones Tecnológicas para Empresas y Comunidad: Montaje de una mesa de Servicios Teleinformáticos
- **Fase del Proyecto (si es formación Titulada):** Planeación.
- **Actividad de Proyecto(si es formación Titulada):**
  AP02 - Elaborar el Portafolio de Servicios para Realizar un Óptimo Mantenimiento de los Equipos de Cómputo Según los Recursos Disponibles.
- **Competencia:** 220501121 - Operar Herramientas Informáticas y Digitales de Acuerdo con Protocolos y Manuales Técnicos.
- **Resultados de Aprendizaje Alcanzar:**
  - ✓ RAP 03 Planificar la Información Según Criterios de Ciberseguridad.
- **Duración de la Guía:** 56 Horas (28 Horas Presenciales – 28 Horas de Aprendizaje Autonomo)

2. PRESENTACIÓN

Cordial Saludo Aprendices,



En un mundo cada vez más digitalizado, la seguridad de la información se vuelve crucial. Las políticas de seguridad, la normativa, y la gestión adecuada de datos son pilares fundamentales para proteger la integridad y confidencialidad de la información.

En esta guía de aprendizaje, exploraremos estos aspectos clave, junto con los derechos de Habeas Data y de autor, así como los procesos de mejora continua y la importancia de las copias de seguridad. Únete a nosotros en este viaje de aprendizaje, donde adquirirás las habilidades necesarias para enfrentar los desafíos de seguridad informática y gestión de datos en el mundo actual. ¡Tu participación es vital para dominar estas competencias y proteger la información en un entorno digital en constante evolución!

3. FORMULACIÓN DE LAS ACTIVIDADES DE APRENDIZAJE

3.1 Actividades de Reflexión Inicial.



*La **seguridad de la información**, también conocida como InfoSec, es un conjunto de procedimientos y herramientas que protegen la información confidencial de una organización. Su objetivo es evitar que la información sea utilizada de forma indebida, acceda a ella alguien no autorizado, se interrumpa o se destruya.*



*La **gestión de datos** consiste en recopilar, mantener y utilizar datos de manera segura, eficiente y rentable. El objetivo de la gestión de datos es ayudar a las personas, las organizaciones y las cosas conectadas a optimizar el uso de los datos dentro de los límites de las políticas y normativas, para que puedan tomar decisiones y tomar medidas que maximicen el beneficio para la empresa. Contar con una estrategia de gestión datos sólida nunca ha sido tan importante, sobre todo ahora que las organizaciones recurren cada vez más a los activos intangibles para crear valor.*

Actividad de Reflexión Inicial:

En el vasto y siempre cambiante paisaje digital contemporáneo, la seguridad de la información y la gestión de datos son pilares fundamentales que influyen en cómo protegemos y gestionamos nuestra información en línea, tanto en contextos personales como profesionales. La seguridad de la información abarca medidas y prácticas diseñadas para salvaguardar los datos contra una amplia gama de amenazas, incluido el acceso no autorizado, el uso indebido y la alteración. Por otro lado, la gestión de datos se refiere al proceso estratégico de recopilación, almacenamiento, organización y análisis de datos para garantizar su integridad y utilidad. En este contexto, cada experiencia digital, desde transacciones financieras hasta interacciones en redes sociales, presenta riesgos potenciales que pueden comprometer nuestra privacidad y seguridad. Desde el robo de identidad hasta el phishing y el malware, estas amenazas son omnipresentes y requieren una vigilancia constante y la adopción de medidas proactivas. Es crucial comprender la importancia de adoptar prácticas de seguridad sólidas, como el uso de contraseñas seguras, la autenticación de dos factores y la educación en ciberseguridad, para mitigar estos riesgos. Además, en entornos laborales y académicos, la

seguridad de la información y la gestión de datos son igualmente vitales para proteger la confidencialidad de la información sensible y garantizar el cumplimiento de las regulaciones. La implementación de políticas de seguridad robustas, la capacitación del personal y el uso de herramientas de cifrado son aspectos clave en este sentido. Sin embargo, enfrentamos desafíos significativos en nuestra búsqueda de seguridad digital. La evolución constante de las tecnologías y la sofisticación de las amenazas cibernéticas requieren una constante adaptación y vigilancia. La falta de conciencia sobre seguridad y las lagunas en las regulaciones también representan obstáculos importantes en este camino. En resumen, en el laberinto digital de la era moderna, la seguridad de la información y la gestión de datos son nuestras brújulas indispensables. Al comprender los riesgos, adoptar medidas proactivas y trabajar juntos, podemos navegar de manera segura por este intrincado paisaje digital y proteger lo que más valoramos: nuestra información y nuestra privacidad en línea.

Dado que la seguridad de la información y la gestión de datos son aspectos críticos en el entorno digital actual, es fundamental comprender nuestras percepciones y experiencias previas en este ámbito. Te invito a reflexionar sobre las siguientes preguntas:

- ¿Que entendimiento tienes sobre el concepto de seguridad de la información y la gestión de datos?
- ¿Haz experimentado alguna situación en la que hallas sentido que tus datos personales estuvieran en riesgo?
- ¿Qué medidas crees que son importantes para proteger la información personal en línea?
- ¿Cómo crees que la seguridad de la información y la gestión de datos impactan en tu entorno laboral o académico?
- ¿haz tenido alguna experiencia relacionada con el manejo de datos en tu vida cotidiana o profesional?
- ¿Qué desafíos crees que enfrentamos en términos de seguridad de la información en la sociedad actual?

Ambiente Requerido: Casa SENA (Yondó – Antioquia).

Materiales: Computadores de Escritorio, Portátil, TV, Cable HDMI, Sonido, Internet, Microsoft Word, Hoja de Papel.

Duración: 1 Horas.

3.2 Actividades de Contextualización e Identificación de Conocimientos Necesarios para el Aprendizaje.



*Una C**opia de Seguridad (Backup**), respaldo, copia de respaldo, copia de reserva en ciencias de la información e informática es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.*

Actividad de Contextualización:

Descripción de la Actividad:

El señor Pedro García es el propietario de la mejor discoteca de la ciudad llamada la Rockola, la gente asiste con mucha frecuencia al sitio por la variedad de música que maneja el propietario. Pedro ha dedicado 10 años a guardar y coleccionar alrededor de 100.000 canciones en formato MP3, muy bien clasificados de todo tipo de música.

El computador personal de la discoteca donde se encuentra la colección musical sufre una avería o daño, el señor Pedro angustiado por que no quiere que se pierda su colección musical, decide llamar a un Técnico en sistemas que le recomendaron para que repare el daño.

El técnico efectivamente arregla el computador mediante un mantenimiento correctivo al hardware (Cambio de la memoria RAM), Pedro le dice al técnico que le realice una copia de seguridad de la música y otros archivos importante en un disco duro portable de 4TB, ya que no posee una copia de esta.

Los propietarios de las otras discotecas hablan con el técnico en sistemas, y le proponen que realice una copia de la colección musical del señor Pedro sin que este se dé cuenta, y ellos se la compran a un precio bastante elevado. Pero el técnico decide que no puede realizar esta acción porque la considera un robo, sabiendo que necesita el dinero para pagar deudas y comprar herramientas y equipos que necesita.

Resuelve los siguientes interrogantes:

- ¿Crees que el técnico actuó de la manera adecuada?
- ¿Qué hubieras hecho tú cómo técnico en esta situación, necesitando el dinero?
- ¿Qué es la ética profesional para ti?
- ¿Estás de acuerdo con la forma de actuar de los otros propietarios de discotecas?

Evidencia de Aprendizaje: Para evidenciar el proceso realizado usted debe realizar la evidencia mencionada, la cual debe ser enviada a través de la plataforma “ZAJUNA”.

Ambiente Requerido: Casa SENA (Yondó – Antioquia).

Materiales: Computadores de Escritorio, Portátil, TV, Cable HDMI, Sonido, Internet, Microsoft Word, Hoja de Papel.

Duración: 1 Horas.

3.3 Actividades de Apropiación del Conocimiento y Transferencia del Conocimiento.

Actividad de Aprendizaje 1: Protección de Datos y Derechos de Autor.

Descripción de la Actividad: Realice las siguientes acciones

1. En la era digital, la protección de datos y los derechos de autor son temas cruciales en proyectos que involucran la recopilación, manejo y uso de información personal y creativa.

Imagina que estás involucrado en un proyecto que requiere el manejo de datos personales y la utilización de material protegido por derechos de autor. La ley de Habeas Data garantiza el derecho a la privacidad y control de la información personal de los individuos, mientras que los derechos de autor protegen las obras creativas y sus derechos de propiedad.

El cumplimiento de estas leyes es fundamental para asegurar la ética y legalidad del proyecto. La ley de Habeas Data establece que las personas tienen derecho a conocer, actualizar y rectificar la información que se ha recopilado sobre ellos en bases de datos y archivos. Esto protege la privacidad y la seguridad de los datos de las personas, asegurando que se utilicen de manera adecuada y con consentimiento informado.

Por otro lado, los derechos de autor protegen las obras creativas, como textos, imágenes, música y software, otorgando a los creadores derechos exclusivos sobre su uso y distribución. Al utilizar material protegido por derechos de autor en un proyecto, es importante obtener los permisos necesarios y respetar los derechos de los autores.

El equilibrio entre la protección de datos y los derechos de autor es crucial en proyectos que involucran la recopilación y el uso de información personal y creativa. Cumplir con estas leyes no solo es una obligación legal, sino también ética, que garantiza el respeto y la privacidad de las personas, así como el reconocimiento y la protección del trabajo creativo.

- ¿Has escuchado alguna vez sobre la ley de Habeas Data? Si es así, ¿podrías describir en qué consiste?
- ¿Cómo crees que la ley de Habeas Data protege la privacidad de los datos de las personas?
- ¿Sabes qué son los derechos de autor y cómo se relacionan con la protección de la propiedad intelectual?
- ¿Qué medidas crees que son importantes para garantizar el cumplimiento de los derechos de autor al utilizar datos o información en un proyecto?
- ¿Cuál crees que es la importancia de respetar tanto la ley de Habeas Data como los derechos de autor en proyectos que involucran el manejo de datos e información personal.

2.Estimado aprendiz, en esta actividad te invito a profundizar en los conceptos de Habeas Data y Derechos de Autor mediante la creación de una tabla comparativa. Esta tabla deberá incluir una visión general de las similitudes y diferencias entre ambos temas, resaltando aspectos clave como definición, legislación aplicable, tipos de derechos, consentimiento y duración de la protección, entre otros

Cuadro Comparativo	
Habeas Data	**Derechaos de Autor**

Evidencia de Aprendizaje: Para evidenciar el proceso realizado usted debe realizar la evidencia mencionada, la cual debe ser enviada a través de la plataforma “ZAJUNA”.

Ambiente Requerido: Casa SENA (Yondó – Antioquia).

Materiales: Computadores de Escritorio, Portátil, TV, Cable HDMI, Sonido, Internet, Microsoft Word, Hoja de Papel.

Duración: 8 Horas.

Actividad de Aprendizaje 2: Leyes y Normativas de Seguridad de la Información en Colombia

En Colombia, las leyes y normativas que regulan la seguridad de la información son:

Ley 1581 de 2012

También conocida como Ley de Protección de Datos Personales, esta ley garantiza el derecho de las personas a conocer, actualizar y rectificar la información que se tenga sobre ellas en bases de datos.

Ley 1273 de 2009

Esta ley creó nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos.

Ley 23 de 1982

Ley que regula los derechos morales y patrimoniales que la Ley concede a los autores (los derechos de autor), por el solo hecho de la creación de una obra literaria, artística o científica, esté publicada o inédita.

Ley 599 de 2000

El artículo 269A del Código Penal Colombiano define el delito de acceso abusivo a un sistema informático:

- *Acceder a un sistema informático sin autorización o fuera de lo acordado.*
- *Permanecer en un sistema informático en contra de la voluntad de quien tenga derecho a excluirlo.*

Si alguien accede sin permiso a un sistema informático, como el correo electrónico, las redes sociales o los sistemas de información de una empresa, se debe denunciar ante la Fiscalía General de la Nación.

Decreto 620 de 2020

Este decreto establece los lineamientos para la implementación de medidas de seguridad de la información en el sector privado.

Decreto 338 de 2022

Este decreto adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, y crea el Modelo y las instancias de Gobernanza de Seguridad Digital.

Descripcion de la Actividad:

Es un placer invitarte a una emocionante misión para fortalecer tu comprensión sobre las leyes y normativas de seguridad de la información.

Esta actividad interactiva te brindará la oportunidad de explorar los fundamentos de la normatividad relacionada con este tema crucial. Para unirte a la actividad, simplemente haz clic en el siguiente enlace:

https://es.educaplay.com/recursos-educativos/18680613-seguridad_de_la_informacion_en_colombia.html

Nota: El objetivo principal de esta actividad es que adquieras conocimientos sobre las leyes y normativas de seguridad de la información mediante un juego interactivo. Te animo a participar y a profundizar tus habilidades en este campo tan relevante.

Evidencia de Aprendizaje: Para evidenciar el proceso realizado usted debe realizar la evidencia mencionada, la cual debe ser enviada a través de la plataforma “ZAJUNA”.

Ambiente Requerido: Casa SENA (Yondó – Antioquia).

Materiales: Computadores de Escritorio, Portátil, TV, Cable HDMI, Sonido, Internet, Educaplay.

Duración: 1 Horas.

Actividad de Aprendizaje 3: Desafio de Conocimiento sobre Copias de Seguridad

Existen varios tipos de copias de seguridad, entre ellos:

Copia de Seguridad Completa: *Crea una copia de todos los datos en cada ocasión, ya sea comprimida, cifrada o tal como están.*

Copia de Seguridad Incremental: *La copia de seguridad incremental, únicamente realiza copia de los datos que se hayan grabado desde la última copia de seguridad, bien sea completa o incremental. Esto ahorra tiempo y espacio al evitar duplicar datos no modificados. Sin embargo, la restauración puede ser más compleja al depender de varias copias.*



Copia de Seguridad Diferencial: *La copia diferencial se enfoca en copiar solo los datos que han sido modificados o añadidos desde la última copia completa. Ofrece mayor velocidad que la copia completa, pero requiere la copia completa para la restauración.*

Copia de Seguridad Espejo: *La copia en espejo replica exactamente el sistema original, incluyendo el sistema operativo, aplicaciones y todos los datos. Aunque permite una recuperación rápida y completa en caso de fallo del sistema, conlleva la necesidad de considerables recursos de almacenamiento debido a la duplicación de todos los datos. Crea una copia exacta de la información en tiempo real. Es decir, mientras trabajas.*

Descripción de la Actividad:

¡Estimado aprendiz, esta es la oportunidad de fortalecer tus conocimientos sobre copias de seguridad y su papel vital en la seguridad de la información!

Esta actividad interactiva te invita a sumergirte en los fundamentos de las copias de seguridad, explorando su importancia crítica en la protección de datos.

https://es.educaplay.com/recursos-educativos/18681295-desafio_de_conocimiento_sobre_copias_de_seguridad.html

Nota: Esta actividad tiene como objetivo identificar los conocimientos u experiencia frente a los diferentes tipos de copias de seguridad.

Evidencia de Aprendizaje: Para evidenciar el proceso realizado usted debe realizar la evidencia mencionada, la cual debe ser enviada a través de la plataforma “ZAJUNA”.

Ambiente Requerido: Casa SENA (Yondó – Antioquia).

Materiales: Computadores de Escritorio, Portátil, TV, Cable HDMI, Sonido, Internet, Educaplay.

Duración: 1 Horas.

Actividad de Aprendizaje 4: Estudio de Caso: Juliana y la Auditoria



*Una **Auditoria** es un revisión sistemática de una actividad o de una situación para evaluar el cumplimiento de las reglas o criterios objetivos a que aquellas deben someterse. Esta puede ser interna o externa, en función de si la realiza la propia empresa, o una entidad externa a la misma.*

Descripción de la Actividad:

Esta actividad presenta un caso particular en el que el aprendiz tomará partido. Después de leer el caso, pensará en las ventajas y las desventajas de realizar una auditoría interna, y el alcance de esta.

Juliana labora en una empresa de insumos médicos como contadora de la misma. En la entidad se han presentado dudas acerca de la veracidad de información contable.

Para este fin, encargan a Juliana la función de evaluar y exponer cuáles serían las ventajas y desventajas de realizar una auditoría interna en la empresa. Ella debe exponer su posición, teniendo en cuenta que en la empresa no se tiene un departamento de auditoría y no se piensa tener por el momento.

¿Qué debería argumentar Juliana?

Para realizar esta actividad debe:

- Desarrolle esta actividad con un informe en Microsoft Word, donde explique por lo menos cinco ventajas y desventajas acerca de la realización de la auditoría. De una conclusión si se debe o no realizar una auditoría. Si su respuesta es realizar una auditoría, ¿Cuál sería el alcance de esta?

Evidencia de Aprendizaje: Para evidenciar el proceso realizado usted debe realizar la evidencia mencionada, la cual debe ser enviada a través de la plataforma “ZAJUNA”.

Ambiente Requerido: Casa SENA (Yondó – Antioquia).

Materiales: Computadores de Escritorio, Portátil, TV, Cable HDMI, Sonido, Internet, Microsoft Word, Hoja de Papel.

Duración: 16 Horas.

Actividad de Aprendizaje 5: Realizar la Valuación de los Activos de la Organización

Reflexión!

Parte fundamental de la seguridad de la información y la ciberseguridad empieza por entender y reconocer el funcionamiento de las empresas y organizaciones; lo que implica hacer un análisis de los recursos tecnológicos y demás dispositivos que permiten que la empresa logre cumplir con los objetivos empresariales.

Es de suma importancia entender los lineamientos básicos que deben ser utilizados por los responsables de la seguridad de la información para poner en marcha la gestión y clasificación de activos que son manejados por la entidad, con el fin de determinar que activos posee, como deben ser utilizados, los roles y responsabilidades que tienen los usuarios sobre los mismos, y reconociendo adicionalmente el nivel de clasificación de la información que a cada activo debe darsele.

A partir de la reflexión descrita, elabore un informe detallado en el que describa:

- ¿Cuáles con las activos tangibles o intangibles informáticos con que cuenta su organización que están relacionados o requeridos para el cumplimento d ellos objetivos empresariales ?
- ¿Cómo debe ser la clasificación de la organización?
- ¿Qué metodología o estándares puede utilizar para realizar el proceso de valuación de activos?
- Por otro lado, teniendo en cuenta el caso de estudio definido en el material de formación, plantee la identificación y clasificación de los activos.
- Defina el estándar o el marco de referencia que mas se ajusta al estudio de caso.

Evidencia de Aprendizaje: Para evidenciar el proceso realizado usted debe realizar la evidencia mencionada, la cual debe ser enviada a través de la plataforma “ZAJUNA”.

Ambiente Requerido: Casa SENA (Yondó – Antioquia).

Materiales: Computadores de Escritorio, Portátil, TV, Cable HDMI, Sonido, Internet, Microsoft Word, Hoja de Papel.

Duración: 16 Horas.

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 : **Actividad de Aprendizaje 1:** Protección de Datos y Derechos de Autor. **Actividad de Aprendizaje 3:** Desafio de Conocimiento sobre Copias de Seguridad. **Evidencias de Desempeño:** **Actividad de Aprendizaje 2:** Leyes y Normativas de Seguridad de la Información en Colombia. **Evidencias de Producto:** **Actividad de Aprendizaje 4:** Estudio de Caso: Juliana y la Auditoria. **Actividad de Aprendizaje 5:** Realizar la Valuación de los Activos de la Organización	Aplica controles de seguridad según normativa, necesidades y restricciones de acceso a la información. Propone procesos de mejora en el manejo de la información con base a la normativa vigente. Gestiona las copias de seguridad y recuperación, según lineamientos establecidos por la empresa.	Observación Directa. Lista de Chequeo. Valoración del Producto.

5. GLOSARIO DE TÉRMINOS

0-day o Ataque de Día Cero: Ataque contra una aplicación o sistema que aprovecha vulnerabilidades desconocidas para ejecutar código malicioso.

Account Harvesting (Cosechar Cuentas): Recolectar cuentas y contraseñas para usarlas con fines malintencionados.

Activo: El término de activo de información se relaciona con todos esos elementos tecnológicos o relacionados con la tecnología que la organización utiliza para el cumplimiento de sus metas o core del negocio. Según la Norma ISO/IEC 27001 se entiende como activo todo aquello que es importante y que la organización valora, por lo tanto, debe de protegerse.

Adware: Programa que muestra publicidad durante la instalación o ejecución de otros programas.

Agujero de Seguridad: Falla en un sistema de información que puede ser explotada para violar su seguridad.

Amenaza: Cualquier evento que puede afectar los activos de información y se relaciona, principalmente, con recursos humanos, eventos naturales o fallas técnicas.

Ataque Man in The Middle: Atacante se introduce en la comunicación entre dos equipos para interceptar y desencriptar datos.

Bluesnarfing: Ataque informático mediante Bluetooth para tomar completo control de dispositivos móviles.

Bombas Lógicas o Temporales: Virus que se activa con ciertos eventos preestablecidos, permaneciendo oculto si no se dan estas condiciones.

Bot: Programa informático que realiza tareas automáticas a través de Internet.

Botnet: Conjunto o red de robots informáticos que se ejecutan automáticamente y pueden ser controlados remotamente.

CISO: Chief Information Security Officer (Oficial de seguridad de la información).

Clasificación de la Información: Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulados en la entidad. Tiene como objetivo asegurar que la información recibe el nivel de protección adecuado.

Clickjacking: Técnica para engañar usuarios y obtener información confidencial mediante la ocultación de acciones en páginas web.

Cracker: Persona con conocimientos avanzados que manipula software para obtener beneficio personal o afectar a otros.

Confidencialidad: Propiedad que determina que la información solo esté disponible y sea revelada a individuos, entidades o procesos autorizados.

Dark Web: Contenido de la web que existe en darknets, requiriendo software específico para acceder. Parte de la internet profunda.

Deep Web: Contenido de internet no indexado por los motores de búsqueda convencionales.

Denial of Service (DoS): Ataque que causa que un servicio o recurso sea inaccesible a usuarios legítimos.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando esta así lo requiera.

El Clicker: Troyano diseñado para aumentar el número de visitas a ciertos sitios web o realizar ataques de denegación de servicio (DoS) hacia servidores específicos.

El Backdoor: Troyano que deja una puerta trasera abierta en el sistema infectado, permitiendo al atacante acceder remotamente sin consentimiento del usuario.

El Keylogger: Troyano que registra las pulsaciones del teclado para capturar información valiosa como contraseñas o datos bancarios.

El Proxy: Troyano que convierte el equipo infectado en un servidor proxy para que el atacante pueda acceder a Internet ocultando su identidad.

El Password Stealer: Troyano que roba contraseñas y otra información introducida en formularios de páginas web, generalmente utilizando técnicas de keylogger.

El Dialer: Troyano que crea conexiones telefónicas en el equipo del usuario sin su conocimiento, generalmente para hacer llamadas de alto coste relacionadas con contenido adulto.

Exploit: Fragmento de software, datos o acciones que aprovechan vulnerabilidades de seguridad para obtener un comportamiento no deseado en un sistema.

Firewall: Sistema que protege una computadora o red de intrusiones externas.

Gusano Informático: Programa autorreplicante que se propaga por Internet sin necesidad de interacción humana.

Hacker: Persona experta en informática que busca violar límites de acceso por desafío o beneficio personal.

Hacking Ético: Uso de conocimientos de informática y seguridad para identificar y corregir vulnerabilidades en redes sin causar daño.

Heurística: Técnicas empleadas por los antivirus para reconocer códigos maliciosos no presentes en su base de datos.

Habeas Data: Derecho que garantiza a las personas el control y acceso a su información personal almacenada en bases de datos, así como la posibilidad de corregirla o eliminarla. Este derecho se enfoca en la protección de la privacidad y el manejo adecuado de los datos personales por parte de las organizaciones.

Hoax o Bulos: Correos electrónicos con información falsa que incita a los usuarios a reenviarlos, sin capacidad de replicación. Objetivo: sobrecargar el flujo de información o el sistema de correo.

Honeypot: Herramienta de seguridad informática que simula ser un objetivo atractivo para los ataques, permitiendo detectarlos, obtener información del atacante y proteger otros sistemas.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

Inyección de Código: Envío de datos inesperados a un intérprete, común en consultas SQL, LDAP, XPath, etc. Puede resultar en pérdida de datos, corrupción o toma de control del sistema.

IoT (Internet de las Cosas): Sistema de dispositivos interconectados que pueden transferir datos a través de una red, sin necesidad de interacción humana.

Iptables: Firewall integrado en el kernel de Linux, utilizado para configurar reglas de seguridad.

Joe Job: Truco en el que se envían correos spam a múltiples usuarios, alterando la dirección del remitente para hacer parecer que provienen de una víctima.

Keylogger: Software o dispositivo que registra las pulsaciones del teclado para capturar información como contraseñas o datos personales.

Malware: Programa o código informático malicioso diseñado para dañar un sistema o causar un mal funcionamiento, como virus, troyanos, gusanos, etc.

Newbie: Persona novata en hacking que busca aprender técnicas y puede llegar a convertirse en hacker.

Nube: Paradigma que ofrece servicios de computación a través de Internet, permitiendo acceder a recursos sin necesidad de gestionarlos localmente.

Lammer: Persona aficionada que presume habilidades de hacking pero carece de conocimientos profundos, siendo más propensa a generar daños.

P2P (Red de Pares): Red de ordenadores donde cada nodo actúa como cliente y servidor, permitiendo el intercambio directo de información.

Pentesting o Examen de Penetración: Ataque controlado a un sistema informático para encontrar debilidades de seguridad y evaluar su resistencia a ataques.

Pharming: Explotación de vulnerabilidades en servidores DNS o equipos de usuarios para redirigir nombres de dominio a máquinas diferentes.

Phishing: Engaño mediante correos, mensajes o llamadas falsas que imitan fuentes de confianza para obtener información confidencial.

Piggybacking: Conexión no autorizada a una red inalámbrica, generalmente sin daño directo pero potencialmente peligrosa.

Protocolo: Conjunto de reglas que rigen la comunicación entre dispositivos en una red, como el protocolo de internet (IP).

Familia de protocolos: Conjunto de protocolos que sustentan el funcionamiento de Internet, como TCP e IP.

Puerto: Valor utilizado en la capa de transporte para distinguir entre múltiples aplicaciones conectadas al mismo host.

Ransomware: Programa malicioso que restringe el acceso a partes del sistema y exige un rescate para restaurar el acceso.

Riesgo: Es la posibilidad de que una amenaza se produzca, dando lugar a un ataque sobre un recurso o servicio tecnológico. Esto no es otra cosa que la probabilidad de que ocurra el ataque por parte de la amenaza.

Rootkit: Conjunto de herramientas utilizadas para ocultar procesos y archivos de un sistema comprometido, permitiendo acceso no autorizado.

Sniffer: Aplicación para redes que captura y analiza paquetes de datos, como Wireshark y Ettercap.

Software de Copia de Seguridad: Aplicaciones que permiten realizar copias de seguridad de archivos y datos importantes.

Software de Firewall: Herramientas que controlan el tráfico de red y protegen una red informática de accesos no autorizados.

Sistema de Gestión de Bases de Datos (DBMS): Software que permite almacenar, gestionar y recuperar datosde una base de datos, como MySQL, Oracle o Microsoft SQL Server.

SPAM: Correos no solicitados que perjudican al receptor, enviados en grandes cantidades, también conocido como correo basura.

Spambot: Programa que genera y envía correos basura a una lista masiva de destinatarios.

Spoof/Spoofing: Suplantación de identidad en comunicaciones, donde un atacante finge ser otra entidad a través de la falsificación de datos.

Spyware: Programa que se instala sin consentimiento del usuario para recopilar información del equipo infectado, como hábitos de navegación o datos personales.

Tor: Proyecto que desarrolla una red de comunicaciones distribuida para garantizar el anonimato de los usuarios en Internet, formando parte de la "darknet" o "web profunda".

Troyano: Malware que proporciona una puerta trasera para que otros programas maliciosos o ciberdelincuentes puedan acceder al sistema y robar información sin conocimiento del usuario.

Virus: Programa informático diseñado para dañar un equipo o dispositivo y con capacidad de autorreplicarse.

Virus de Enlace: Virus que cambia los enlaces de los accesos directos de programas infectados, impidiendo el acceso a estos programas.

Vulnerabilidad: Es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información, en la que se permite que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma.

VPN (Red Privada Virtual): Tecnología que permite extender una red de área local sobre una red pública como Internet, proporcionando seguridad y privacidad en la comunicación.

Vulnerabilidad: Puntos débiles de un sistema informático que pueden ser explotados por un atacante para comprometer la integridad, disponibilidad o confidencialidad del sistema.

XSS (Cross-Site Scripting): Vulnerabilidad informática que permite inyectar código JavaScript u otro lenguaje similar en páginas web visitadas por el usuario, comprometiendo la seguridad del sistema.

Downloader: Troyano diseñado para descargar e instalar otros malware en equipos infectados, preparándolos para ejecutarse automáticamente.

6. REFERENTES BILBIOGRÁFICOS

Eee. (2024, January 10). Norma ISO 27001:2022: todo lo que debes saber sobre el nuevo estándar de Seguridad de la información. Escuela Europea de Excelencia.

https://www.escuelaeuropeaexcelencia.com/2022/12/norma-iso-270012022-todo-lo-que-debes-saber-sobre-el-nuevo-estandar-de-seguridad-de-la-informacion/

ISO/IEC 27001:2022.(n.d).ISO

https://www.iso.org/standard/27001#:~:text=ISO%2FIEC%2027001%20promotes%20a%20holistic%20approach%20to%20information,tool%20for%20risk%20management%2C%20cyber-resilience%20and%20operational%20excellence

Udearroba. (2018, April 4). Concepto de gestión de la información [Video]. YouTube.

https://www.youtube.com/watch?v=XgTA-TJJ8NQ

Narvaez, M. (2023, 19 junio). Levantamiento de información: Qué es y cómo realizarlo. QuestionPro.

https://www.questionpro.com/blog/es/levantamiento-de-informacion/

Sistemas de Gestión de la Seguridad de la Información (SGSI). Fortalecimiento TI.(s.f.).

https://www.mintic.gov.co/gestionti/615/w3-article-5482.html?_noredirect=1

7. CONTROL DEL DOCUMENTO

	Nombre	Cargo	Dependencia	Fecha
Autor (es)	**Jorge Luis Arias Maestre**	**Instructor Técnico**	**SENA/CTMAE**	**06 Noviembre de 2024**

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

	Nombre	Cargo	Dependencia	Fecha	Razón del Cambio
Autor (es)					