**PROCESO DIRECCIÓN DE FORMACIÓN PROFESIONAL INTEGRAL**

**FORMATO GUÍA DE APRENDIZAJE**

## 1. IDENTIFICACIÓN DE LA GUIA DE APRENDIZAJE

- Denominación del Programa de Formación: CONTROL DE LA SEGURIDAD DIGITAL.
- Código del Programa de Formación: 233103
- Nombre del Proyecto: Asegurar los procesos de seguridad de la información tanto lógicos y físicos en las instituciones y empresas del departamento del cauca
- Fase del Proyecto: Análisis
- Actividad de Proyecto: interpretar los requerimientos necesarios para monitorizar, controlar y documentar procesos de seguridad digital según tecnológicas y modelo de seguridad digital de la empresa.
- Competencia Diagnosticar la seguridad de la información de acuerdo con métodos de análisis y normativa técnica
- Resultado de aprendizaje: Documentar el proceso de realización de inventario según procedimientos establecidos por la organización.
- Duración de la Guía (20 horas)

## 2. PRESENTACION

Imagen tomada de https://www.itbusiness-solutions.com.mx/hubfs/IMG-ITBS-BLOG/ITBS-Seguridad-CIberseguridad.jpg?t=1536232942813

Debido a la globalización, a los grandes avances tecnológicos, las empresas u organizaciones deben estar a la vanguardia en sus procesos informáticos, por lo cual deben asegurar su infraestructura computacional a través de todo su sistema de procesamiento y almacenamiento de datos de tal manera que se garantice la confidencialidad, integridad y disponibilidad de los mismos en el momento en que se requiera. La seguridad física y lógica de la información cada vez más está siendo amenazada por el incremento en los delitos informáticos y el terrorismo computacional, es por eso que las organizaciones se deben encontrar preparadas para no dejar ninguna vulnerabilidad en su sistemas y utilizar todos los recursos a su alcance para proteger todos los recursos computacionales y de información estratégicos para el negocio.

.

## 3. FORMULACION DE LAS ACTIVIDADES DE APRENDIZAJE

### 3.1 Actividades de Reflexión inicial.

Una de las técnicas más usada por los delincuentes informáticos para el robo de información es la ingeniería social, por este motivo es de vital importancia conocer y entender esta técnica para proteger nuestra información de una manera adecuada ante estas intrusiones.

**Actividad No 1. Identificar el alcance que tiene el uso de la ingeniería social por medio de la película "Hacker, ningún sistema es seguro", en la seguridad tecnológica en la actualidad.**

**Enlace de la película:** https://youtu.be/2cCCCx_nRvU

Los aprendices observaran la película "Hacker, ningún sistema es seguro", posteriormente de forma individual o en grupo responderán las siguientes preguntas.

**1.** Cree usted que Benjamín y sus amigos manejaron con Confidencialidad, integridad y disponibilidad de la información a la que accedieron? Explique su respuesta.
**2.** Piensa que es cierto que ningún sistema es seguro? Justifique su opinión.
**3.** Qué opina sobre la frase usada en la película "Internet es un hoyo legal"?
**4.** Que entiende por Ingeniería Social, está de acuerdo con el uso de esta técnica, para obtener información sobre algo o alguien cuando se requiera.
**5.** como considera la seguridad de informacion en su institución educativa

**Duración de la Actividad:** 2 horas.
**Tipo de Actividad:** Individual-Grupal.

**3.2 Actividades de contextualización e identificación de conocimientos necesarios para el aprendizaje.**
Con el avance de las tecnologías se incrementan los peligros y vulnerabilidades en los sistemas de información. **La ingeniería social** es la extracción de manera engañosa de datos personales del usuario, se ha visto fortalecida desde la aparición de Internet, sustentando su principio básico que dice: "los usuarios son el eslabón débil del sistema", porque para una atacante resulta, en primera instancia, más sencillo y rápido buscar y encontrar vulnerabilidades y debilidades en los seres humanos que en las herramientas tecnológicas. Existen gran variedad de prácticas que permiten utilizar esta técnica que debemos conocer y prepararnos para evitar ser víctimas de estas trampas.

**Actividad No 1** Identificar los elementos que conforman la seguridad informática de acuerdo a las características, contramedidas y ataques de la información.

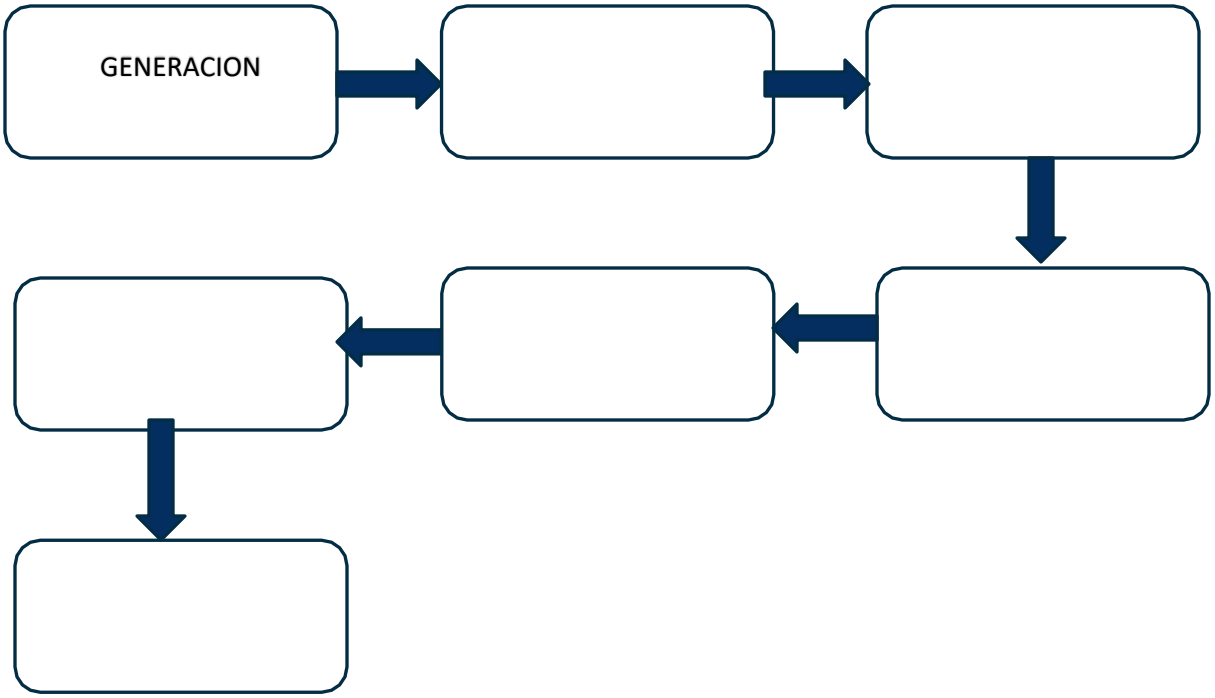
Para realizar las siguientes actividades debe recurrir al material de apoyo 1. Y al glosario de términos de la guía

### 3.1 Relaciona los términos con su definición

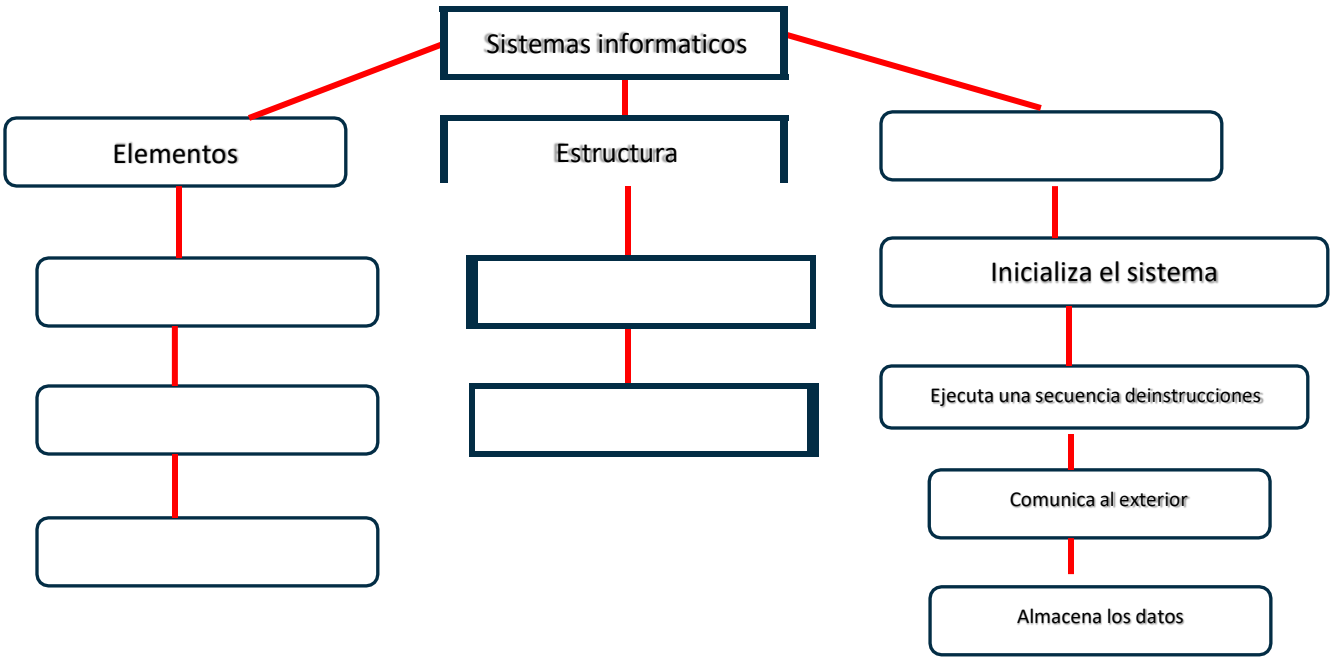
| | |
|---|---|
| **a . APT** | Entidad de diferentes miembros nacionales encargada de establecer modelos unificados. |
| **b. DoS** | Procedimiento de aseguramiento y habilitación del uso de celulares por los empleados |
| **c. EMM** | Adversario con habilidad sofisticada y recursos que le permiten múltiples ataques |
| **d. OSI** | Negativa de la solicitud de usar un servicio de cómputo por un usuario legítimo |
| **e. ISO.** | Estandarización de la comunicación de los sistemas computacionales de distintas tecnologías |

**3.2** Completa el siguiente diagrama con el documento **gestión de la informacion.PDF**

**Ciclo de vida de la información**



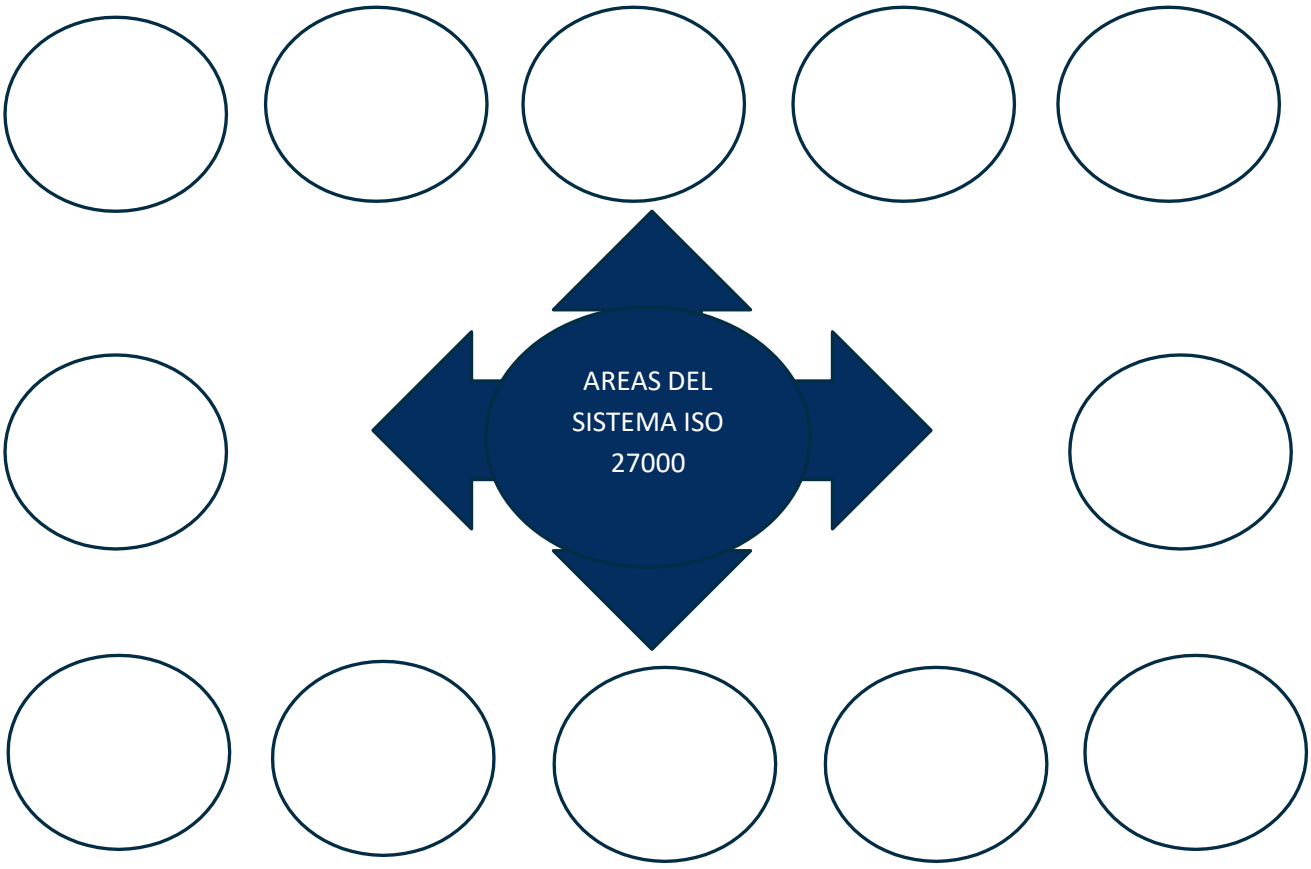

**3.3** Completa el siguiente mapa conceptual con el documento **sistemas informáticos.pdf**



**3.4** observa el video **Seguridad de la información .**Escribe la información faltante sobre los principios de la seguridad informática.

| **Características de la seguridad** | **Estados de los datos** | **Contramedidas** |
|---|---|---|
| Confidencialidad | | |
| | Almacenamiento | |
| | | Capacitación |

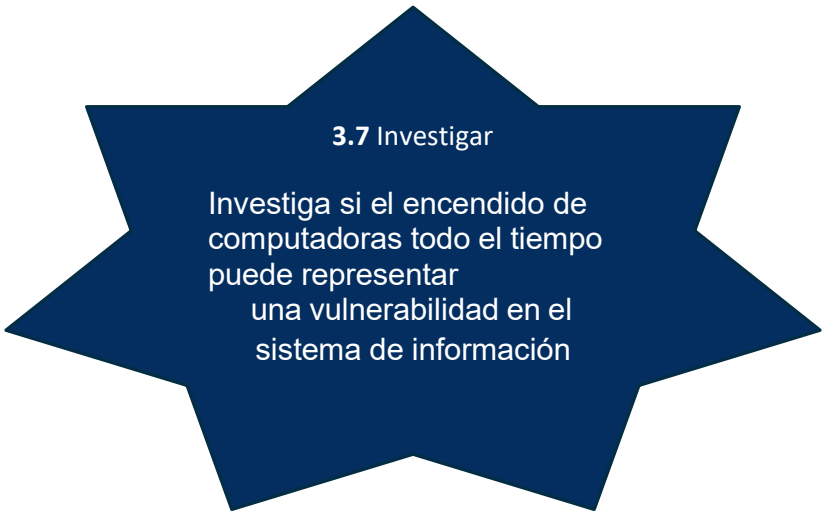
**3.5** Escribe la información faltante en el siguiente diagrama. Con el documento **Administración de la seguridad de la información.pdf**



**3.6** Completa las oraciones.

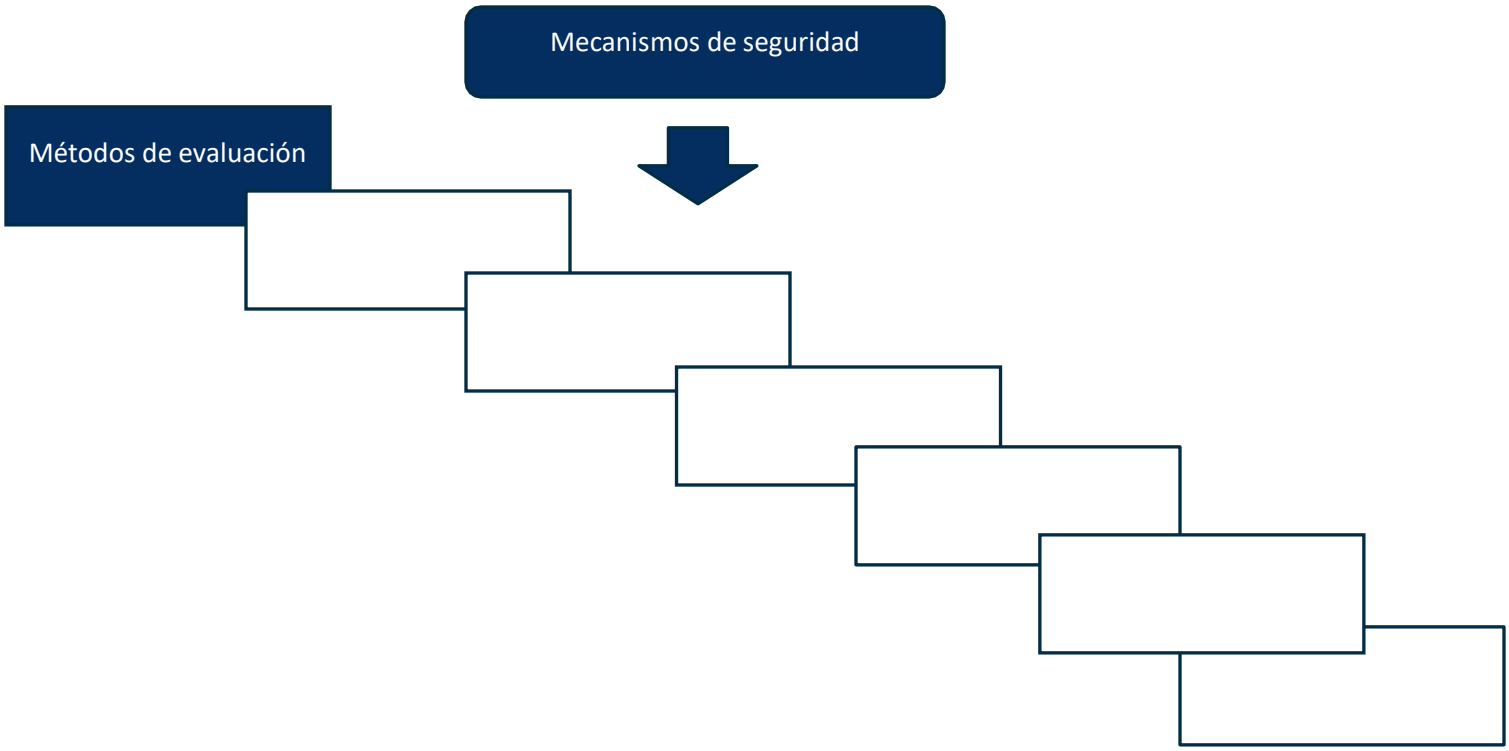
| |
|---|
| reglas ISP adaptable práctica usuarios aplicaciones establecer detectar prevenir |

**a.** Las políticas de seguridad de la información o_____son un conjunto de _____ promulgadas por una organización.
**b.** Las razones por las que las instituciones crean políticas son:_____un proceso general para la seguridad de la información,_____y_____los datos comprometidos, entre otras.
**c.** Las características con las que deben contar las políticas de seguridad son: completa, _____, amplia y_____.
**d.** Las políticas deben abordar todos los datos,_____, sistemas, infraestructura, _____y terceros involucrados con la organización, sin excepción.

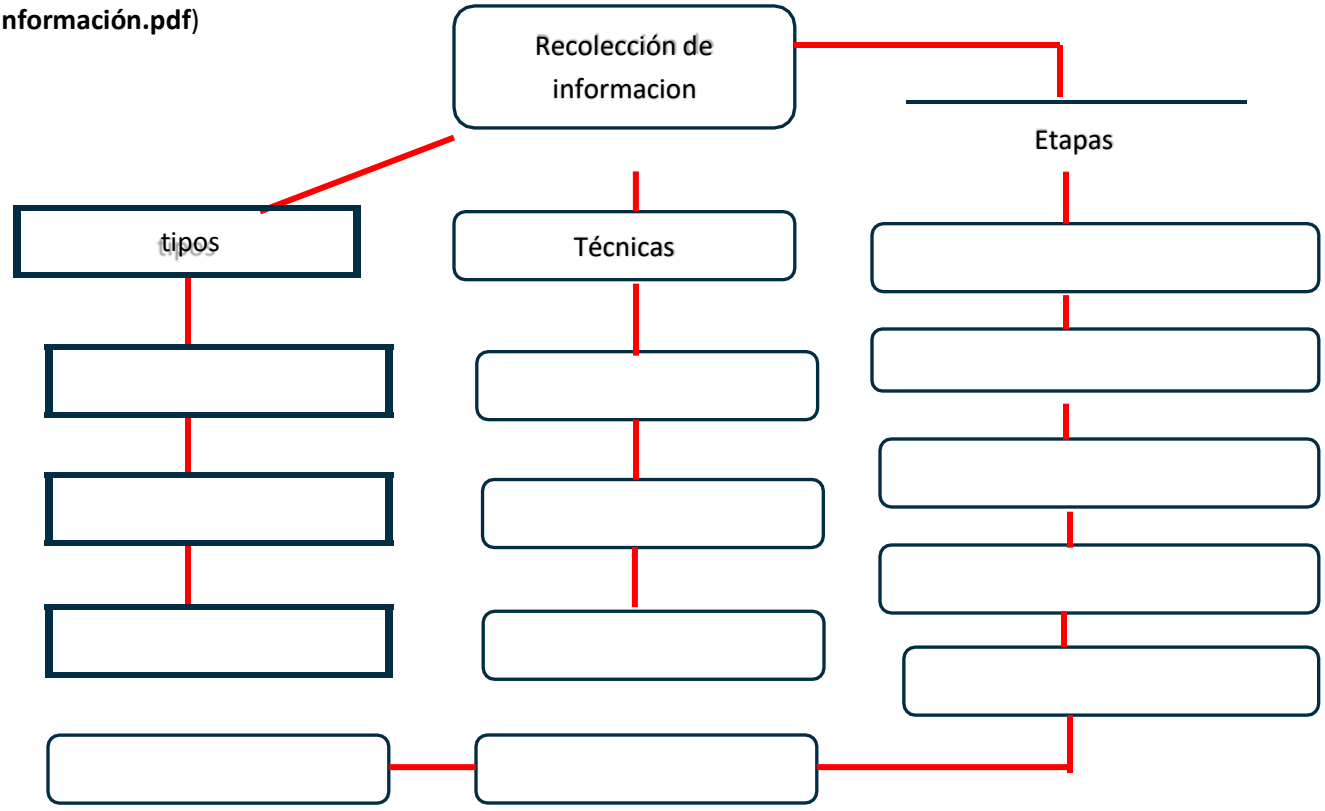



**Las siguientes actividades realizar con el material de apoyo 2.**

**3.8** completar el siguiente diagrama con el video **Mecanismos de la seguridad informática.mp4**




**3.9** completa el siguiente mapa conceptual con el material de apoyo (documento **Recopilación de información.pdf**)



**3.10** Ordenar las actividades que comprenden el procedimiento. Material de apoyo ( video **administracion del riesgo.mp4** )

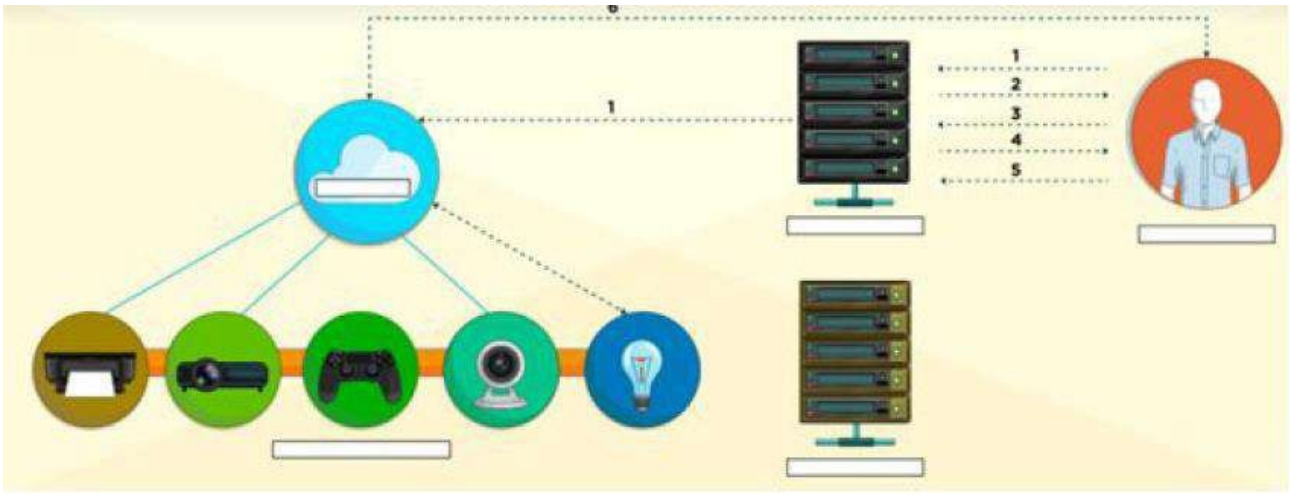
| |
|---|
| Analiza el costo-beneficio. |
| Implementa los controles seleccionados dada tu responsabilidad. |
| Selecciona los controles a implementar dependiendo del presupuesto. |
| Elabora una lista de acciones para resolver un riesgo reconocido. |
| Examina todas las acciones posibles para mitigar los riesgos. |
| Asigna responsabilidades claras y bien delimitadas a tu equipo técnico. |

**MITIGACION DEL RIESGO**

**3.11** Indica el nombre de los elementos del diagrama de un sistema de autenticación, (material de apoyo, **video autenticación de los usuario.mp4**)

| | | |
|---|---|---|
| **Dueño de los recursos** | | **Servidor de autorización** |
| **Servidor de recursos** | **Empleado** | **Dispositivos** |

NOTA: editar esta imagen y en cada rectángulo colocar su respectivo texto




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

**Primera caso de estudio.** **(**Material de apoyo documento **Amenazas, ataques y vulnerabilidades.pdf ).**

Los empleados de una compañía encuentran que no pueden utilizar sus computadoras debido a que aparece un mensaje en el arranque de sistema operativo, el cual solicita un depósito de dinero por medio de criptomonedas para poder desbloquear el acceso.

**Contesta las siguientes preguntas**.

¿Contra qué tipo de hacker se enfrenta la organización?

¿Cuáles pueden ser las amenazas que producen este tipo de consecuencias?

**Segundo Caso de Estudio** (material de apoyo **Metodologías de evaluación de la seguridad.mp4** )

El equipo de TI de una empresa quiere evaluar el nivel de seguridad de presenta la red en la oficina central. Entre los datos que requieren recabar están:

- ✓ Servicios de red
- ✓ Sistemas operativos

**Responde la siguiente pregunta**

¿Cual de los métodos de evaluación de la seguridad es el más idóneo para este caso? ¿Por qué?

**Tercer caso de Estudio (material de apoyo Control de acceso.pdf )**

De acuerdo con la siguiente lista de control:

Carpeta 1: Usuario 1 (lectura y escritura), usuario 2 (lectura)
Carpeta 2: Usuario 1(escritura), usario 2(administración)
Equipo 1: Usuario 1(ejecución), usuario 2 (administración y ejecución)

**Completar la siguiente matriz de control:**

| | C1 | C2 | E1 |
|---|---|---|---|
| U1 | | | |
| U2 | | | |

I

**3.4. Actividades de transferencia del conocimiento.**

Para determinar estrategias de seguridad informática e implementar algunas medidas, es necesario identificar las amenazas y vulnerabilidades a las que se encuentran expuestos los sistemas de información; la seguridad de la información que se implementa en un software proporcionan un grado de calidad mayor al producto.

**Actividad No 1 Aplicar funcionales de seguridad en el entorno laboral**

Realizar ejercicios practicos y documentativos del proceso en el ambiente de formación con el instructor :

- ✓ Etiquetado de documentos
- ✓ Accesso sopechosos
- ✓ Buen uso de mecanismos de acceso
- ✓ Politica de contraseñas

**4. ACTIVIDADES DE EVALUACIÓN**

La evaluación es un proceso realizado durante toda la dinámica de aprendizaje-enseñanza y se llevará a cabo en cada uno de los espacios y momento de la formación. Como actividad de cierre se realizará un cuestionario de transferencia de conocimiento en cuanto al proceso formativo teniendo en cuenta los conocimientos alcanzados y aspectos actitudinales, acompañamiento del instructor en el proceso de formación.

**Duración de la actividad**: 2 horas.
**Tipo de actividad**: Individual

| Evidencias de Aprendizaje | Criterios de Evaluación | Técnicas e Instrumentos de Evaluación |
|---|---|---|
| **Evidencias de Conocimiento**<br><br>Respuesta a preguntas sobre Métricas mediante evaluación escrita.<br><br>**Evidencias de Desempeño:**<br><br>Aplicación de herramientas de los diferentes tipos de pruebas de Software.<br><br>**Evidencias de Producto:**<br><br>Informe Plan de pruebas del proyecto.<br><br>**Evidencias de Conocimiento :** | Elabora y diligencia instrumentos e instructivos, para documentar y evaluar los procesos de desarrollo de software, de acuerdo a las pautas de aseguramiento de la calidad de la organización.<br><br>Define el plan de evaluación de la calidad de procesos de desarrollo de software, aplicando principios de aseguramiento de calidad y de gestión de proyectos, de acuerdo con el procedimiento establecido.<br><br>Define y establece criterios para medir procesos asignados, aplicando fundamentos de | Formulación de preguntas /Cuestionario.<br><br>Juego de roles, socialización, estudio de casos (lista de chequeo,)<br><br>Observación del trabajo desarrollado en el ambiente formativo implementando pruebas (Lista de chequeo).<br><br>1. Talleres prácticos desarrollados en grupo en el proceso formativo |

| | | |
|---|---|---|
| 1. Evaluación teórica de conocimientos.<br><br>2. Talleres de investigación<br><br>**Evidencias de Desempeño:** Prácticas y manejo de herramientas de seguridad informática<br><br>**Evidencias de Producto:**<br>Informe amenazas y vulnerabilidades que pueden afectar el proyecto formativo | medición, de acuerdo con los objetivos organizacionales.<br><br>Realiza la evaluación de calidad, a partir de la medición de los procesos y productos, de acuerdo con las necesidades de información de los diferentes niveles administrativos, de los objetivos organizacionales y de los criterios de medición establecidos.<br><br>Mejora y adecua procesos asignados, de acuerdo con los resultados de las mediciones, evaluaciones y recomendaciones de resolución, de no conformidades. | 2. Pruebas individuales de conocimientos teóricos<br><br>3. Pruebas prácticas individuales<br><br>4. Observación del trabajo desarrollado en el ambiente formativo |

**5. GLOSARIO DE TERMINOS**

**Activo (Asset):**Un recurso, procedimiento, sistema u otra cosa que tenga un valor para una organización y por lo tanto deba de ser protegida, los Activos pueden ser bienes físicos tales como equipos de cómputo y maquinaria, también puede ser la Información y propiedad intelectual.

**Adware:** Software legitimo pero molesto, es una característica que tienen algunos programas gratuitos o en fase de prueba que muestran publicidad, mensajes de activación o de compra, comúnmente el creador cobra por la publicidad que se muestra, los mensajes se muestran cuando esta en funcionamiento el software asociado.
**Antivirus:** Software diseñado para la detección, prevención y eliminación de Software mal intencionado o dañino para los sistemas.

**Ataques de Diccionario:** Es un tipo de ataque de fuerza bruta enfocado en el que se utiliza una lista predefinida de palabras.

**Ataque de Fuerza Bruta:** Es un tipo de ataque que consiste en que el atacante intenta con todas las posibles combinaciones de letras, números y caracteres para acertar la contraseña, PIN o phassphrace.

**Auditoría:** La verificación independiente de cualquier actividad o proceso.

**Autenticación:** El procedimiento de verificar la identidad que reclama un sujeto mediante una validación en un sistema de control de acceso**.**

**Autorización:** Es el proceso de definir los derechos o permisos asignados a un sujeto (que puede hacer).

**Baja de Voltaje (Brownout):** Voltaje bajo de manera prolongada de una fuente de energía eléctrica, tal como la energía eléctrica del servicio público.

**Biometría:** Cualquiera de varios métodos utilizados como parte de un mecanismo de autenticación, para verificar la identidad de una persona. Los tipos de biometría utilizada incluye las huellas dactilares, impresiones de la palma de la mano, firmas, escaneos de retina, escaneos de voz y patrones de escritura en teclados.

**Certificado Digital:** Es un certificado que liga una identidad a una llave de cifrado pública.

**Cifrado:** El proceso de transformar texto plano a texto cifrado**.**

**Cifrar:** Una transformación criptográfica de texto claro a mensaje cifrado.

**Confidencialidad:** Previene del uso no autorizado o revelación de información, asegurándose que la información es accesible únicamente para aquellos que tengan autorizado su uso**.**

**Controles Detectivos:** Controles que identifican violaciones e incidentes.

**Controles Disuasivos:** Controles que desalientas la realización de violaciones.

**Criptoanálisis:** Es la ciencia de descifrar texto cifrado sin el uso de la llave criptográfica.

**Criptografía:** La ciencia de cifrar o descifrar información, tal como puede ser un mensaje privado para proteger su confidencialidad, integridad y / o autenticidad.

**Criptología:** La ciencia que abarca Criptografía y Criptoanálisis.

**DDoS (Ataque distribuido de negación de Servicios):** Es un tipo de ataque en el que el atacante inicia ataques de negación de servicio simultáneamente desde muchos sistemas.

**Defensa en profundidad (o en capas):**Es el principio de proteger los activos (información, bienes físicos de la empresa, etc) por medio de utilizar varias capas de protección diferentes.

**Descifrado:**Es el proceso de transformar texto cifrado en texto plano.
**Directrices (Guidelines):** Documentos similares a Estándares, pero considerados recomendaciones, en lugar de un requisito forzosos.

**Disponibilidad**: El proceso de asegurar que los sistemas e información sean accesibles para usuarios autorizados cuando ellos lo requieran.

**Due Care (Cuidado Necesario):** Los pasos que toma una organización para implementar mejores prácticas de seguridad.

**Due Diligence (Diligencia Debida):** La prudente administración y ejecución de "Due Care".

**Dumpster Diving (Buceo de Contenedores):** El proceso de examinar basura con la intención de encontrar bienes valiosos o información.

**Espionaje:** La práctica de espiar o utilizar espías para obtener información propietaria o confidencial.

**Firewall:** Dispositivo o programa que controla el flujo de tráfico entre redes.

**Firewall de Aplicaciones:** Un Firewall que inspecciona la capa 7 del Modelo OSI (aplicación) con el objetivo de bloquear contenido malicioso antes de que alcancé o abandoné el Servidor de Aplicaciones (portal web, base de datos, etc).

**Forense (Informática Forense):** La ciencia de conducir una investigación criminal computacional para poder determinar que sucedió o quien es el responsable por lo ocurrido.

**Función Hash**: Una función matemática que crea una representación única de un grupo grande de datos. Las funciones Hash son frecuentemente utilizadas en algoritmos criptográficos y para producir resúmenes de mensajes (Checksums and message digest).
**Gateway:** Un sistema conectado a una red de computadoras, el cual ejecuta cualquier traducción en tiempo real o funcionalidad de interfaz.

**Honeypot:** Un sistema señuelo instalado por un administrador de seguridad para descubrir los métodos de ataque de hackers potenciales.

**Hot Site**: Una ubicación alterna a la de uso diario, con recursos computacionales totalmente funcionales que tiene servicios de electricidad, aire acondicionado, servidores de impresión, servidores de archivos y estaciones de trabajo, en resumen todos los servicios brindados en la ubicación primaria.

**Identificación:** Los medios por los cuales un usuario reclama una identidad especifica sin validación a un sistema.

**Integridad:** Garantiza la exactitud y completitud de la información y los métodos de procesamiento.

**Negación de Servicios (DoS):**Es un ataque a sistemas o redes con la intención de hacer que el sistema o red no este disponible para su uso.

**Propiedad Intelectual**: Incluye patentes, marcas registradas, derechos de autor y secretos comerciales.

**Pruebas de Caja Negra**:Es un tipo de prueba de seguridad donde el sujeto que realiza la prueba no tiene ningún conocimiento previo de los sistemas que están siendo puestos a prueba.

**Texto Cifrado (Ciphertext):** Es un texto plano que ha sido transformado (cifrado) en un mensaje mezclado que es ininteligible.

## 6. REFERENTES BILBIOGRAFICOS


Pruebas de penetración en Ingenieria social: https://searchdatacenter.techtarget.com/es/consejo/Pruebas-de-penetracion-en-ingenieria-social-cuatro-tecnicas-efectivas

Qué es Kali linx y qué puedo hacer con el?: https://computerhoy.com/paso-a-paso/software/que-es-kali-linux-que-puedes-hacer-41671

Instalar Kali Linux en Virtual box: http://www.cursodehackers.com/VirtualBox.html

25 ataques informáticos y como prevenirlos: https://ciberseguridad.blog/25-tipos-de-ataques-informaticos-y-como-prevenirlos/

Ciberataques: https://www.eitb.eus/es/tag/ciberataques/

Glosario de tecnología: https://www.onasystems.net/glosario-terminos-seguridad/

**7. CONTROL DEL DOCUMENTO**

| | Nombre | Cargo | Dependencia | Fecha |
|---|---|---|---|---|
| **Autor (es)** | **EDGAR VERNAZA ARBOLEDA** | **INSTRUCTOR** | **COMERCIO Y SERVICIOS** | **JUNIO 2023** |

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

| | Nombre | Cargo | Dependencia | Fecha | Razón del Cambio |
|---|---|---|---|---|---|
| **Autor (es)** | **JORGE ENRIQUE SANCHEZ PINO** | **INSTRUCTOR** | **CENTRO DE COMERCIO Y SERVICIOS** | **07/07/2024** | **ACTUALIZACION** |
| | | | | | |