PROCESO DE GESTIÓN DE FORMACIÓN PROFESIONAL INTEGRAL

FORMATO GUÍA DE APRENDIZAJE

IDENTIFICACIÓN DE LA GUIA DE APRENDIZAJE

- **Denominación del Programa de Formación:** Técnico en sistemas teleinformáticos.
- **Código del Programa de Formación:** 233108 V1.0
- **Nombre del Proyecto:** Fortalecimiento de los servicios teleinformáticos de equipos y redes en las MiPymes de la región.
- **Fase del Proyecto:** Planeación
- **Actividad de Proyecto:** Planificar procesos físicos y lógicos de soporte y el mantenimiento de sistemas teleinformáticos.
  Competencia: 220501121 - Operación de herramientas informáticas

- **Resultados de Aprendizaje Alcanzar:**

  RAP2 - Planificar la información según criterios de ciberseguridad.

  RAP4 - Documentar la gestión de la información acuerdo a protocolos establecidos.

- **Duración de la Guía:** 78 horas Directas y 18 Horas Autónomas

2. PRESENTACIÓN

Cordial saludo Aprendices

Es de tener en cuenta que la información y los datos son el "**bien más preciado**" para la empresa o las personas, debido a que mientras las empresas pueden tramitar información financiera, económica, documentación confidencial y mucho más, las personas equivalentemente tramitan información financiera llegando inclusive a tramitar las fotos familiares que son de mucha importancia para ellas.

Teniendo en cuenta lo anterior, la seguridad informática posee vital importancia al buscar proteger los datos personales, empresariales y financieros que garantizan la tranquilidad de las empresas y las personas al reducir la vulnerabilidad y aumentar la confianza; para ello se tienen en cuenta tres (3) Principios de Seguridad de la Información como lo son la Disponibilidad, la Privacidad o confidencialidad y la Integridad de la Información.

La información es un bien que se involucra en todos los niveles económicos, operativos e intelectuales de una compañía, ocupando un lugar preponderante en la toma de decisiones y la solución de problemas, convirtiéndose en clave para el desarrollo legal, organizacional y financiero.

Existen amenazas y vulnerabilidades tanto en el mundo FISICO como INFORMATICO que ponen en peligro los activos y disposición de la data.

La norma ISO 27001 nos aportan las pautas, los requerimientos y los controles para poder tener un **S**istema de **G**estión de la **S**eguridad de la **I**nformación **(SGSI),** en las organizaciones, este SGSI, consistente en medidas orientadas a **proteger la información**, indistintamente del formato de esta, contra cualquier amenaza, de forma que garanticemos en todo momento la continuidad de las actividades de la empresa, teniendo como objetivos principales:

- La confidencialidad
- La integridad
- y La disponibilidad de la Información.

En la siguiente gráfica, se describen de una manera rápida las fases necesarias para la implementación del “Sistema de Gestión de la Seguridad Informática - SGSI”:



https://www.normas-iso.com/iso-27001/

3. FORMULACIÓN DE LAS ACTIVIDADES DE APRENDIZAJE

3.1 Actividad de Reflexión: Lo invitamos a leer el siguiente artículo.

Ciberataques en Colombia en el 2023 siguen en aumento

by Diana Gonzalez | Mar 14, 2023 | Ciberseguridad, Protección de la información | 0 comments



Colombia y Brasil son los 2 países de Latinoamérica que aparecen en el listado de los 10 países del mundo con más ataques de ransomware en el 2022, según el informe “Amenazas Cibernéticas 2023” de la empresa SonicWall, llamando la atención sobre la importancia de la ciberseguridad para las organizaciones colombianas de todas las industrias en el 2023.

El alza de los ciberataques es una tendencia mundial, como lo señala el reporte de SonicWall, con un aumento del 28% de ataques cibernéticos en todos los sectores económicos a nivel mundial en el tercer trimestre de 2022, por lo que se espera que esta tendencia continúe en el 2023 en todo el mundo,

impulsada por innovaciones en las vulnerabilidades de ransomware y en el “hacktivismo” de estado impulsado por conflictos internacionales.

A la par que los entornos de trabajo, comercio y comunicación se digitalizan, los ciberdelincuentes encuentran más campo de acción para operar, explotando las vulnerabilidades en las prácticas de trabajo híbridas de las organizaciones, por lo que se prevé que los ataques ya no se realizarán en su mayoría por “Phishing” o correo electrónico con archivos infectados, sino los delincuentes ampliarán su objetivo para apuntar a herramientas de trabajo colaborativo como Slack, Teams, OneDrive y Google Drive, según el informe “Amenazas cibernéticas 2023”.

Por favor, busque tres (3) casos recientes de Ciberataques en Colombia y analice:

- ✓ Nombre de la Empresa.
- ✓ Tipo de ciberataque.
- ✓ Tiempo de recuperación.

Con la información encontrada los aprendices en grupos de Tres (3) personas, deben preparar una exposición de 15 minutos En power point o prezi donde nos cuente los tipos de ataques y como fue el proceso de recuperación.

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

Apropiar los conceptos básicos sobre seguridad en informática para lo cual se propone se estudie:

- Amenazas de seguridad.
- Procedimientos de seguridad.
- Técnicas de mantenimiento preventivo comunes para propósitos de seguridad.
- Procesos básicos de solución de problemas de seguridad.

En grupos de trabajo colaborativo de 3 aprendices se debe realizar un mapa conceptual de los siguientes temas, y prepárese para exponer 3 aspectos que serán seleccionados al azar.

- Malware: Que es, tipos, cómo se identifican y controlan.
- Suplantación de identidad tipos de phishing, correo no deseado, cómo identificarlos y buenas prácticas.
- Ataques TCP: Que son, cómo identificarlos.

- Ataques de Dia cero e ingeniería social.
- Directiva de seguridad local de Windows.
- Protección de acceso a datos y Protección contra malware.
- Técnicas de seguridad
- Protección de equipos físicos.
- Técnicas de mantenimiento preventivo comunes para propósitos de seguridad.
- Procedimientos mínimos de solución de problemas de seguridad.

Nota: Se recomienda el uso del material de apoyo: IT Essentials de Cisco (Aspectos de seguridad).

3.3. **Actividades de apropiación del conocimiento**

Descripción de las Actividades:

3.3.1. Realizar la parametrización de Seguridad en Windows 10 o 11 según procedimiento técnicos

Implantación de seguridad de sistemas operativo Windows tiene aspectos importantes y particulares de seguridad o endurecimiento (hardening).

Realizar las prácticas de configuración:

Aplique la Guía de Seguridad con Windows 10 y 11:
https://youtube.com/playlist?list=PLT0koQYMKV1ioayNc02Wnjv5X2wwBEzqf

- Firewall de Windows.
- Windows defender.
- Windows Update
- Navegador seguro SmartScreen
- Windows defender Offline Scanner.
- Configuración de información en redes sociales

En grupos de trabajo colaborativo de 3 aprendices se debe realizar video del procedimiento aplicado para la parametrización de Seguridad en Windows.

Ambiente Requerido: Mínimo 60 metros cuadrados, materiales y herramientas requeridas

Materiales: Computador funcionales de escritorio o portátiles con memoria RAM 16 GB, procesador 3.0 GHz o Superior, Disco Duro de 1 TB, Software ofimático, Red internet operativa para consultas

3.3.2. Planificar copias de seguridad según procedimientos técnicos y criterios de seguridad.

Se recomienda que en Grupo de Tres (3) personas, los aprendices expongan las características necesarias para la realización copias de seguridad:

- Tipos de copias de seguridad.
- Discusión de ventajas y desventajas de cada tipo.
- Estrategia 3-2-1 de copias de seguridad
- Preparación de disponibilidad de recursos.
- Retención de copias y periodos.
- Controles de cifrado y protección de datos.
- Puede usar el material: Copias de Seguridad “Una guía de aproximación para el empresario” disponible en:

  https://www.incibe.es/sites/default/files/contenidos/guias/guia-copias-de-seguridad.pdf

Ambiente Requerido: Mínimo 60 metros cuadrados, materiales y herramientas requeridas.

Materiales: Computador funcionales de escritorio o portátiles con memoria RAM 16 GB, procesador 3.0 GHz o Superior, Disco Duro de 1 TB, Software ofimático, Red internet operativa para consultas

Lineamientos para la entrega del producto

- **Producto para entregar:** En los mismos grupos anteriores que expusieron, deben por favor:
  A. Crear una Carpeta en el Sistema Operativo Windows y nombrarla “Backup”.
  B. Una vez creada la anterior Carpeta deben guardar en esta Carpeta al menos cinco (5) Archivos que sean diferentes y de tipos diferentes.
  C. Con la herramienta de Copia de Seguridad del Sistema Operativo Windows o cualquier otra herramienta de Copia de Seguridad, deben realizar dos (2) Procesos de Copias de Seguridad. Un (1) Backup Incremental que tenga registros de mínimo Dos (2) Horas diferentes y un (1) Backup Total de la Carpeta con sus archivos.

     Nota: Para efectos de ver las versiones y los cambios de la copia incremental, se deben por favor modificar los archivos antes de hacer cada copia de seguridad (Diferentes Horas).

  D. Etiquetar las copias de Seguridad creadas, con las fechas y Hora de Creación y un nombre seleccionado por ustedes, donde se debe diferenciar si la copia es Total o Incremental.

- Contenido: Archivos de las Copias de Seguridad realizados.

- Para hacer el envío de la evidencia remítase al área de la actividad correspondiente y acceda al espacio en el sistema LMS de la entidad.

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
Conocimiento: **Exposición**: En 15 minutos presente los 3 casos de Ciberseguridad que investigó, planteando tipo de ataque y como fue el proceso de recuperación **Mapa conceptual**: Recomendaciones para el HARDENING (Endurecimiento). **Desempeño:** **Informe técnico:** Planificar copias de seguridad según procedimientos técnicos y criterios de seguridad. (configuración del firewall, antivirus, reglas de conexión). **Producto:** **Archivos de las Copias de Seguridad creadas y etiquetadas.** **Video y Sistema Operativo (EndPoint) protegido:** Implementación de Herramientas del Sistema Operativo para Endurecer la Seguridad del Equipo	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. Gestiona las copias de seguridad y recuperación, según lineamientos establecidos por la empresa Implementa herramientas para endurecer la Seguridad en los equipos de cómputo con SO Windows.	**Conocimiento**: ✓ **Lista de chequeo: IE-01-Guia_6** Exposición Casos de Ciberseguridad ✓ **Lista de chequeo IE-02-Guia_6** Exposición del Mapa conceptual. **Evidencias de Desempeño:** ✓ Rubrica **IE-03-Guia_6** **Evidencias de Producto:** ✓ **Lista de Chequeo IE-04-Guia_6:** Copias de seguridad.docx

5. GLOSARIO DE TÉRMINOS

CIBERSEGURIDAD: La seguridad informática, también conocida como ciberseguridad, es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo vinculado con la misma, y especialmente la información contenida en una computadora o circulante a través de las redes de computadoras.

CONFIDENCIALIDAD: Consiste en que la información no debe llegar a personas u organizaciones que no estén autorizadas.

CONTROLES DE SEGURIDAD: La virtualización utiliza el software para imitar las características del hardware y crear un sistema informático virtual. Esto permite a las organizaciones de TI ejecutar más de un sistema virtual, y múltiples sistemas operativos y aplicaciones, en un solo servidor.

DISPONIBILIDAD: La información debe poder ser accedida en cualquier momento que se requiera, por las personas autorizadas

INTEGRIDAD: La información debe mantenerse íntegra y sin modificaciones por parte de personas no autorizadas.

MALWARE: Se relaciona con software dañino que afecta los dispositivos, de lograrse materializar se podría generar perdida de información, incluso monitorear las acciones que se estén haciendo en el dispositivo de forma silenciosa sin que el usuario se entere.

PHISHING: Consiste en suplantar la identidad de una persona o una entidad, la principal vía de ataque es el envío de emails, por eso la importancia de verificar los remitentes, enlaces y archivos adjuntos que parezcan sospechosos o de dudosa procedencia.

6. REFERENTES BILBIOGRÁFICOS

- Del Poder Judicial, A. V. (2017, April 07). Análisis e Interpretación de los Controles - Anexo "A" ISO 27001. Youtube. Retrieved from https://www.youtube.com/watch?v=YIMxx-LbUWM
- Guía para la implementación del Principio de Responsabilidad Demostrada (Accountability) | Superintendencia de Industria y Comercio. (2022, December 07). Retrieved from https://www.sic.gov.co/noticias/guia-para-la-implementacion-del-principio-de-responsabilidad-demostrada
- Informática pa novatos. (2022, December 07). Curso de seguridad doméstica con Windows 10. Youtube. Retrieved from https://www.youtube.com/playlist?list=PLT0koQYMKV1ioayNc02Wnjv5X2wwBEzqf

- Instituto nacional de ciberseguridad. (2018). Copias de Seguridad. “Una guía de aproximación para el empresario”. Retrive from https://www.incibe.es/sites/default/files/contenidos/guias/guia-copias-de-seguridad.pdf
- Incibe. Protege tu empresa – Blog - (2008, Agosto) – «Como Pedro por su casa»: ¿a quién dejas acceder a tus sistemas? (1/2) https://www.incibe.es/protege-tuempresa/blog/como-pedro-por-su-casa-01
- Incibe. Protege tu empresa – Blog - (2008, Agosto) – «Como Pedro por su casa»: ¿a quién dejas acceder a tus sistemas? (2/2) https://www.incibe.es/protege-tuempresa/blog/como-pedro-por-su-casa-02
- Quanti Media Group. (2021, November 04). ¿Qué es la norma ISO 27001? | Quanti Lightboard Series. Youtube. Retrieved from https://www.youtube.com/watch?v=iZNUDnf7QgQ
- Quanti Media Group. (2021, November 04). ¿Qué es la norma ISO 27001? | Quanti Lightboard Series. Youtube. Retrieved from https://www.youtube.com/watch?v=iZNUDnf7QgQ
- Ti, L. C. (2020, October 12). ESTRUCTURA DE LA NORMA ISO 27001 2013. Youtube. Retrieved from https://www.youtube.com/watch?v=NoFccA90D7E

7. CONTROL DEL DOCUMENTO

	Nombre	Cargo	Dependencia	Fecha
Autor (es)	**Peter Emerson Pinchao**	**Experto Temático**	**CTPI**	**2/11/2022**

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

	Nombre	Cargo	Dependencia	Fecha	Razón del Cambio
Autor (es)	**Peter Emerson Pinchao**	**Experto Temático**	**CTPI**	**2/11/2022**	
Autor	**Gilberto González Medina**	**Experto técnico**	**CTPI Cauca**	**14-06-2023**	**Actualización**