Cielito Home
EXPERIENCIAS A LA CARTA

CURSO DE CYBERSEGURIDAD

CAPACITACIÓN ANUAL SOBRE CONCIENTIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN.

Introducción al curso

- Objetivos del curso

Módulo 1: Conciencia sobre la Seguridad de la Información

- Lección 1: Introducción a la ciberseguridad
- Preguntas del módulo

Módulo 2: Reconociendo y Respondiendo a Incidentes

- Lección 2: Señales de un incidente de ciberseguridad
- Lección 3: Cómo responder a un incidente
- Preguntas del módulo

Módulo 3: Amenazas Digitales y Cómo Protegerte

- Lección 4: Tipos de malware
- Lección 5: Ingeniería social
- Preguntas del módulo

Módulo 4: Seguridad en Herramientas y Tecnología

- Lección 6: Inteligencia artificial en el trabajo
- Lección 7: Redes sociales
- Preguntas del módulo

 Módulo 5: Manejo de Datos Sensibles

- Lección 8: Protección de datos
- Lección 9: Gestión y destrucción de datos
- Preguntas del módulo

 Módulo 6: Seguridad en la Navegación y Dispositivos

- Lección 10: Navegación segura
- Lección 11: Protección de dispositivos móviles
- Preguntas del módulo

 Módulo 7: Colaboración en la Nube

- Lección 12: Buenas prácticas en la nube
- Preguntas del módulo

 Conclusión

Curso: Fundamentos de la Seguridad de la Información

Introducción al curso

Bienvenido al curso sobre Fundamentos de la Seguridad de la Información. Este curso está diseñado para capacitarte en los conceptos clave de ciberseguridad, las amenazas más comunes y las mejores prácticas para proteger datos sensibles, tanto personales como laborales.

Objetivos del curso:

1. Reconocer las amenazas más comunes en el ámbito digital.
2. Aprender las mejores prácticas para proteger datos y sistemas.
3. Desarrollar habilidades para identificar, responder y prevenir incidentes de ciberseguridad.

Módulo 1: Conciencia sobre la Seguridad de la Información

Lección 1: Introducción a la ciberseguridad

La ciberseguridad tiene como propósito principal proteger los datos corporativos, de clientes y empleados. Para lograrlo, cada persona dentro de una organización debe:

- Cumplir con las políticas y estándares de seguridad.
- Detectar posibles amenazas y actuar rápidamente.
- Usar tecnologías como la inteligencia artificial de manera responsable.

Preguntas:

1. ¿Qué es la ciberseguridad y por qué es importante en una organización?
   a) Un conjunto de políticas que solo aplican a sistemas operativos.
   b) Medidas para proteger información y sistemas digitales.
   c) Una herramienta que solo usan expertos en tecnología.

2. ¿Cuáles son las responsabilidades individuales en la ciberseguridad?
   a) Identificar amenazas y notificarlas.
   b) Ignorar mensajes sospechosos.
   c) Usar cualquier dispositivo para manejar información sensible.

3. ¿Qué deberías hacer si detectas una actividad sospechosa en tu sistema?
   a) Intentar resolverlo por tu cuenta.
   b) Notificar inmediatamente al equipo de seguridad.
   c) Reiniciar tu computadora.

Módulo 2: Reconociendo y Respondiendo a Incidentes

Lección 2: Señales de un incidente de ciberseguridad

Reconocer las señales de un sistema comprometido es crucial. Algunas señales comunes son:
- Alarmas del antivirus indicando infección.
- Mensajes emergentes solicitando rescates o soporte técnico falso.
- Navegación redirigida a sitios no deseados.
- Pérdida de acceso a contraseñas o cuentas.
- Instalación accidental de software sospechoso.
- Pérdida o robo de dispositivos laborales.

Lección 3: Cómo responder a un incidente

Para responder correctamente a un incidente:
1. No intentes solucionar el problema por tu cuenta.
2. Notifica de inmediato al equipo de seguridad para minimizar el impacto.

Preguntas:

1. ¿Cuáles son algunas señales comunes de un incidente de ciberseguridad?
   a) Alarmas del antivirus y pérdida de contraseñas.
   b) Documentos desorganizados en la computadora.
   c) Lentitud en la red.

2. ¿Por qué es importante notificar los incidentes rápidamente?
   a) Para minimizar el impacto del incidente.
   b) Porque es una regla opcional.
   c) Para reportarlo a redes sociales.

3. ¿Qué pasos incluirías en un plan de respuesta a incidentes?
   a) Ignorar el problema.
   b) Documentar, notificar y aislar el sistema afectado.
   c) Formatear el sistema sin consultar al equipo de seguridad.

Módulo 3: Amenazas Digitales y Cómo Protegerte

Lección 4: Tipos de malware

Los software maliciosos son herramientas comunes que usan los ciberatacantes. Algunos tipos son:
- Keyloggers: Capturan pulsaciones de teclado para robar información confidencial.
- Ransomware: Bloquea tus archivos y exige rescate para recuperarlos.
- Spyware: Espía tus actividades, incluso utilizando tu cámara o micrófono.

Lección 5: Ingeniería social

La ingeniería social es una técnica de manipulación psicológica para obtener información confidencial. Ejemplos:
- Llamadas falsas: Simulando ser de instituciones oficiales.
- Correos electrónicos falsos: Que aparentan ser de colegas o superiores.

Preguntas:

1. ¿Qué es un ransomware y cómo afecta a los sistemas?
   a) Un virus que ralentiza la computadora.
   b) Un software que cifra archivos y exige un pago para desbloquearlos.
   c) Una herramienta para proteger información.

2. ¿Cómo puedes prevenir los ataques de ingeniería social?
   a) Verificando la identidad de quien solicita información.
   b) Ignorando correos electrónicos.
   c) Compartiendo contraseñas solo con personas confiables.

3. ¿Qué acciones debes tomar ante un mensaje sospechoso de phishing?
   a) Abrir el enlace para verificarlo.
   b) Ignorarlo completamente.
   c) No abrir el enlace y reportarlo al equipo de seguridad.

Módulo 4: Seguridad en Herramientas y Tecnología

Lección 6: Inteligencia artificial en el trabajo

Aunque la inteligencia artificial (IA) puede ser una herramienta poderosa, también presenta riesgos como:
- **Sesgos:** Los datos de entrenamiento pueden contener información parcial.
- **Privacidad:** Evita enviar datos confidenciales a herramientas de IA.
- **Sobredependencia:** Revisa siempre los resultados generados por la IA.

Lección 7: Redes sociales

Las redes sociales pueden ser una fuente de riesgos para la seguridad si no se usan de manera adecuada. Para proteger tu información:
- Usa contraseñas únicas y activa la autenticación en dos pasos.
- Sé cauteloso con la información que compartes.
- Desconfía de mensajes urgentes o "demasiado buenos para ser verdad".

Preguntas del módulo

1. ¿Qué riesgos presenta la inteligencia artificial en el trabajo?
   - a) Ayuda en la toma de decisiones.
   - b) Posible sesgo en los resultados y comprometer datos sensibles.
   - c) Mejora la productividad.

2. ¿Por qué es importante ajustar la configuración de privacidad en redes sociales?
   - a) Para proteger la información personal y evitar accesos no autorizados.
   - b) Para compartir datos con amigos.
   - c) Para sincronizar cuentas laborales y personales.

3. ¿Cómo puedes validar la información generada por la IA?
   - a) Revisándola con un criterio humano y confirmándola con fuentes confiables.
   - b) Usándola sin revisión adicional.
   - c) Asumiendo que siempre es correcta.

Módulo 5: Manejo de Datos Sensibles

Lección 8: Protección de datos

El manejo adecuado de datos sensibles es fundamental para garantizar la privacidad y la seguridad de la información. Para proteger los datos sensibles:
- Usa sistemas y dispositivos autorizados.
- Cifra toda la información que envíes o almacenes.
- Evita copiar o guardar datos en servicios no autorizados.

Lección 9: Gestión y destrucción de datos

Además de proteger los datos, es esencial eliminarlos de manera segura cuando ya no sean necesarios. Algunas prácticas clave incluyen:
- Mantener los registros de datos organizados y actualizados.
- Usar métodos seguros para eliminar documentos físicos (triturado) y digitales (software especializado).

Preguntas del módulo:

1. ¿Qué medidas debes tomar para proteger datos sensibles?
   - a) Usar dispositivos no autorizados.
   - b) Cifrar la información y usar sistemas aprobados.
   - c) Guardar datos en servicios personales para mayor accesibilidad.

2. ¿Cómo se deben eliminar los datos digitales de manera segura?
   - a) Enviándolos a la papelera y vaciándola.
   - b) Usando software especializado para su eliminación.
   - c) Dejándolos almacenados indefinidamente.

3. ¿Por qué es importante mantener un registro organizado de los datos?
   - a) Para garantizar el cumplimiento de políticas y evitar fraudes.
   - b) Para compartir información con facilidad.
   - c) Para simplificar el acceso de cualquier usuario.

Módulo 6: Seguridad en la Navegación y Dispositivos

Lección 10: Navegación segura

La navegación en internet puede exponer tus datos a riesgos si no tomas las precauciones necesarias. Para navegar de manera segura:
- Usa navegadores actualizados y elimina extensiones innecesarias.
- Nunca sincronices navegadores laborales con personales.
- Cierra sesión al finalizar actividades en línea y evita sitios no confiables.

Lección 11: Protección de dispositivos móviles

Tus dispositivos móviles almacenan gran cantidad de información sensible. Para protegerlos:
- Configura bloqueos de pantalla como contraseñas o biometría.
- Descarga aplicaciones únicamente de fuentes confiables.
- Desactiva Wi-Fi y Bluetooth cuando no los uses para evitar conexiones automáticas a redes no seguras.

Preguntas del módulo:

1. ¿Qué prácticas mejoran la seguridad al navegar por internet?
   - a) Sincronizar navegadores para mayor comodidad.
   - b) Actualizar navegadores y evitar extensiones innecesarias.
   - c) Usar navegadores desactualizados para evitar problemas de compatibilidad.

2. ¿Cómo puedes proteger tu dispositivo móvil contra amenazas?
   - a) Configurando bloqueos de pantalla y descargando aplicaciones confiables.
   - b) Dejando Wi-Fi y Bluetooth siempre activos para mayor conectividad.
   - c) No configurando contraseñas para evitar olvidarlas.

3. ¿Por qué es importante cerrar sesión después de usar un navegador?
   - a) Para proteger tus credenciales y evitar usos indebidos.
   - b) Para ahorrar batería.
   - c) Para compartir fácilmente las credenciales con otros.

Módulo 7: Colaboración en la Nube

Lección 12: Buenas prácticas en la nube

Las herramientas de colaboración en la nube facilitan el trabajo en equipo, pero también presentan riesgos si no se utilizan adecuadamente. Para proteger tus datos:
- Usa soluciones autorizadas por tu organización y evita accesos públicos o anónimos.
- Protege videoconferencias con contraseñas y salas de espera.
- Activa la autenticación multifactor (MFA) en todas tus cuentas.

Preguntas del módulo:

1. ¿Qué medidas de seguridad puedes implementar al usar herramientas en la nube?
   - a) Usar autenticación multifactor (MFA) y evitar accesos públicos.
   - b) Compartir enlaces sin restricciones para mayor accesibilidad.
   - c) Permitir accesos anónimos para simplificar procesos.

2. ¿Cómo puedes proteger una videoconferencia contra accesos no autorizados?
   - a) Configurándola con contraseñas y habilitando salas de espera.
   - b) Compartiendo el enlace en redes sociales.
   - c) Permitiendo que cualquiera entre sin verificación previa.

3. ¿Qué puedes aprender de los riesgos de compartir enlaces públicos?
   - a) Los enlaces públicos pueden exponer información confidencial a usuarios no autorizados.
   - b) Los enlaces públicos siempre son seguros si se generan desde la nube.
   - c) No hay riesgos asociados a compartir enlaces públicos.

Conclusión

Este curso te ha proporcionado herramientas prácticas para identificar, responder y prevenir amenazas digitales. Recuerda que la seguridad de la información es una responsabilidad compartida.

Respuestas del Curso: Fundamentos de la Seguridad de la Información

Módulo 1

1. b) Medidas para proteger información y sistemas digitales.

2. a) Identificar amenazas y notificarlas.

3. b) Notificar inmediatamente al equipo de seguridad.

Módulo 2

1. a) Alarmas del antivirus y pérdida de contraseñas.

2. a) Para minimizar el impacto del incidente.

3. b) Documentar, notificar y aislar el sistema afectado.

Módulo 3

1. b) Un software que cifra archivos y exige un pago para desbloquearlos.

2. a) Verificando la identidad de quien solicita información.

3. c) No abrir el enlace y reportarlo al equipo de seguridad.

Módulo 4

1. b) Posible sesgo en los resultados y comprometer datos sensibles.

2. a) Para proteger la información personal y evitar accesos no autorizados.

3. a) Revisándola con un criterio humano y confirmándola con fuentes confiables.

Módulo 5

1. b) Cifrar la información y usar sistemas aprobados.

2. b) Usando software especializado para su eliminación.

3. a) Para garantizar el cumplimiento de políticas y evitar fraudes.

Módulo 6

1. b) Actualizar navegadores y evitar extensiones innecesarias.

2. a) Configurando bloqueos de pantalla y descargando aplicaciones confiables.

3. a) Para proteger tus credenciales y evitar usos indebidos.

Módulo 7

1. a) Usar autenticación multifactor (MFA) y evitar accesos públicos.

2. a) Configurándola con contraseñas y habilitando salas de espera.

3. a) Los enlaces públicos pueden exponer información confidencial a usuarios no autorizados.