

Curso virtual - sincrónico

Ciberseguridad: Fundamentos, Riesgos, IA y Práctica Aplicada

Descripción

Este curso ha sido diseñado y estructurado en coherencia con las buenas prácticas internacionales de gestión de la ciberseguridad, manteniendo una alineación conceptual con la familia de normas ISO/IEC 27000, en particular ISO/IEC 27001, así como con el NIST Cybersecurity Framework (NIST CSF).

Los contenidos, actividades prácticas y herramientas propuestas refuerzan principios de concientización, protección de la información, control de accesos, detección de amenazas y respuesta a incidentes, desde la perspectiva del rol del colaborador, sin pretender sustituir ni certificar un Sistema de Gestión de Seguridad de la Información.

Perfil de ingreso

Colaboradores no técnicos con acceso a sistemas de información.

Inversión

¢170 000 (ciento setenta mil colones) + 2% IVA.
(realizable en dos tractos)

Periodo lectivo

Por definir de 6:00 a 9:00 pm

Duración: 7 sesiones de 3 horas cada una,
para un total de 21 horas lectivas.

Cantidad de estudiantes

Máximo: 18

Profesor

Por definir

- ✓ Inversión realizable en dos tractos.
- ✓ Posterior a la 2da. semana no se realiza reintegro.

DETALLE DEL CURSO

1

Fundamentos de ciberseguridad y superficie de ataque:

- Conceptos básicos: Confidencialidad, Integridad, Disponibilidad (CIA).
- Inventario de activos: qué es un activo de información; clasificación simple (documentos, credenciales, dispositivos).
- Superficie de ataque: definición; ejemplos desde el puesto de trabajo (correo, USB, aplicaciones SaaS, entre otras).
- Amenazas actuales: tipos generales (phishing, ransomware, fuga de datos) y cómo impactan al negocio.
- Factor humano: errores comunes; vectores que aprovechan la psicología; responsabilidad del colaborador.
- Actividad práctica: mapeo de activos e identificación de puntos de exposición.

2

Identidades, contraseñas y control de accesos:

- Identidad digital corporativa: cuentas corporativas vs personales; responsabilidad en su uso.
- Contraseñas seguras: principios (longitud, entropía, gestión segura, entre otras).
- Autenticación multifactor (MFA): qué es, tipos (SMS, app, token), beneficios y limitaciones.
- Principio de mínimo privilegio: ejemplos prácticos; cómo solicitar/revisar accesos.
- Gestión de credenciales: ciclo de vida (creación, rotación, revocación).
- Actividad práctica: evaluación de fortaleza de contraseñas y buenas prácticas de creación.

3

Phishing, ingeniería social y fraude digital:

- Ingeniería social: técnicas comunes (pretexting, baiting, tailgating) y señales de alerta.
- Tipos de phishing: correo, SMS (smishing), voz (vishing), spear-phishing; ejemplos reales adaptados al sector.
- Fraude empresarial: suplantación de proveedores, fraude en pagos, compromiso de correo empresarial (BEC).
- Detección y verificación: cómo analizar remitente, cabeceras, enlaces y adjuntos; indicadores de compromiso.
- Reporte y escalamiento: cuándo y cómo reportar sospechas; qué información aportar.
- Actividad: análisis guiado de correos sospechosos y evaluación de enlaces.

4

Protección de información, nube y uso seguro de IA

- Clasificación de la información: niveles prácticos (público, interno, confidencial); etiquetado y manejo.
- Riesgos de compartición en la nube: control de acceso, enlaces compartidos, sincronización automática.
- Uso de IA generativa: riesgos de fuga de datos, veracidad de resultados, privacidad y propiedad intelectual.
- Shadow AI: qué es, ejemplos de riesgo cuando empleados usan herramientas no autorizadas.
- Prompts y APIs: buenas prácticas para no exponer datos sensibles en prompts; revisión antes de compartir.
- Actividad: ejercicios de clasificación y reformulación segura de prompts.

DETALLE DEL CURSO

5

Dispositivos, malware y seguridad del endpoint:

- Tipos de malware: virus, troyanos, ransomware, spyware; cómo se comportan.
- Vectores de infección: correo, descargas, dispositivos extraíbles, vulnerabilidades sin parchear.
- Seguridad básica del endpoint: actualizaciones, antivirus/EDR, configuración mínima segura, backups.
- Higiene digital: separación de cuentas, cifrado de disco, bloqueo automático.
- Respuesta inicial ante sospecha: pasos inmediatos para aislar y reportar.
- Actividad práctica: revisión de configuraciones y análisis básico de archivos sospechosos.

6

Trabajo remoto, redes y seguridad operativa:

- Riesgos del trabajo remoto: dispositivos personales, redes domésticas, exposición de datos.
- Wi-Fi seguro: diferencias entre redes públicas y privadas; configuración WPA2/WPA3; SSID y contraseñas.
- VPN y acceso remoto: cuándo usar VPN; riesgos de VPN mal configurada; alternativas seguras.
- Seguridad operativa: actualizaciones, separación de entornos, políticas de teletrabajo.
- Checklist de teletrabajo seguro: pasos prácticos para el día a día.
- Actividad práctica: evaluación simple de seguridad de red Wi-Fi y checklist aplicado.

7

Gestión de incidentes y simulación integral:

- Qué es un incidente: Diferenciar eventos de incidentes de seguridad y su impacto real.
- Marco NIST SP 800-61: Las 4 fases de respuesta ante incidentes (detección, análisis, contención y recuperación).
- Detección y análisis: Herramientas y técnicas para identificar y investigar incidentes.
- Contención y recuperación: Estrategias para aislar el problema y restaurar sistemas.
- Comunicación legal: Protocolos de comunicación durante incidentes y cumplimiento de Ley 8968 CR.
- Post-mortem: Análisis de lecciones aprendidas sin culpas para mejorar futuras respuestas.