INSTITUCIÓN BADRA

OPERADOR EN CIBERSEGURIDAD Y RIESGO DIGITAL

Programa de la Capacitación

PROGRAMA DE LA CAPACITACIÓN
OPERADOR DE CIBERSEGURIDAD Y RIESGO DIGITAL

Este curso te permitirá ingresar al mundo de la **ciberseguridad operativa** sin necesidad de experiencia técnica avanzada. Aprenderás a realizar tareas reales como **monitoreo de alertas, gestión de accesos, verificación de respaldos y reporte de incidentes**, utilizando herramientas aplicadas en empresas y fintechs.

La formación está orientada al **aprendizaje práctico**, incorporando además el uso de **Inteligencia Artificial** para analizar alertas y agilizar procesos operativos. Como cierre, participarás de **simulacros intensivos** donde pondrás en práctica la detección de riesgos, la toma de decisiones y la documentación de incidentes en escenarios similares a un entorno laboral real.

OBJETIVOS DE LA CAPACITACIÓN

- Aprender a interpretar alertas, registros básicos y comportamientos anómalos para reconocer cuándo una situación requiere escalamiento o intervención inmediata.
- Conocer el ciclo de vida de usuarios dentro de una organización, realizando altas, bajas y modificaciones de accesos, junto con la actualización de inventarios y activos críticos.
- Implementar medidas esenciales de seguridad como autenticación multifactor, uso de bóvedas de contraseñas y auditorías visuales sobre estaciones de trabajo y entornos corporativos.
- Trabajar con tableros básicos de seguridad, herramientas de monitoreo y sistemas de detección de anomalías para fortalecer la capacidad de respuesta ante riesgos.
- Desarrollar criterios para escalar incidentes, preservar evidencia y generar reportes claros y organizados siguiendo normativas y buenas prácticas utilizadas en el sector.
- Participar en simulaciones prácticas donde se pondrán en juego habilidades de análisis, comunicación y toma de decisiones frente a incidentes y alertas ficticias.

El Factor Humano y la Identidad

1. Panorama del Riesgo Moderno

- **El Triángulo de la Seguridad (CID):** Confidencialidad, integridad y disponibilidad explicadas con ejemplos de la vida cotidiana (Ej.: el Home Banking).
- **Definición de Riesgo para Operadores:** La fórmula simple de riesgo (Amenaza vs Ocurrencia - Vulnerabilidad vs Ocurrencia). Concepto de impacto.
- **Motivaciones del Atacante:** Del activismo al cibercrimen profesional y el Ransomware como modelo de negocio.

Actividad Práctica - Análisis de Activos:

- El cursante debe listar los 5 activos más valiosos de una "PYME ficticia" (Ej.: una pañalera con venta online) y qué pasaría si se pierden por un día.
- **OSINT Básico:** Buscar qué información pública hay de una empresa en internet que un atacante podría usar.

2. Psicología de la Amenaza (Ingeniería Social)

- **Sesgos Cognitivos:** Por qué caemos en el engaño (sentido de urgencia, autoridad, miedo).
- **Anatomía del Phishing:** Smishing (SMS), Vishing (Voz) y Spear Phishing (dirigido).
- **El "Cuento del Tío" Digital:** Cómo se adaptan las estafas tradicionales al entorno Fintech.

Actividad Práctica - Laboratorio de Detección:

- Analizar 10 correos reales y marcar las "banderas rojas" (red flags): remitentes extraños, links acortados, lenguaje urgente.
- **Simulacro de Respuesta:** Redactar un aviso preventivo para los empleados de una oficina tras detectar una campaña de phishing activa.

3. Gestión de Identidades (IAM)

- **El Ciclo de Vida del Usuario:** Onboarding (ingreso), Movimiento (cambio de rol) y Offboarding (egreso).
- **Principio de Mínimo Privilegio:** Dar solo el acceso necesario para el trabajo que realizará el usuario.
- **Autenticación vs. Autorización:** La diferencia entre decir "soy yo" y tener permiso para "abrir la caja fuerte".

Actividad Práctica - Diseño de Matriz de Accesos:

- Crear una tabla simple para una Fintech: ¿Qué carpetas debe ver el de Ventas vs Cuáles el de Legales?
- **Checklist de Egreso:** Crear una lista de pasos obligatorios para dar de baja a un empleado que se va en malos términos (evitar el "usuario fantasma").

4. Taller Práctico I (Manos a la Obra)

- **Blindaje de Cuentas:** Instalación y configuración de una Bóveda de Contraseñas (ej. Bitwarden) para uso corporativo.
- **MFA para todos:** Configuración paso a paso de factores de autenticación (Google Authenticator, llaves físicas) en herramientas comunes como Gmail o Slack.
- **Auditoría de "Escritorio Limpio":** Ejercicio visual de detección de riesgos en una oficina física (postits con claves, routers expuestos, documentos en la impresora).

Entregable: Un mini-manual de "Primeros Pasos de Seguridad" que el cursante podría entregar a un nuevo empleado en su primer día de trabajo.

Operativa, Vigilancia y Herramientas (El "Cómo")

1. Infraestructura para no-técnicos (El Escenario)

- **¿Dónde viven los datos?:** Diferencia práctica entre Servidor Local, Nube (Cloud) e Infraestructura Híbrida.

- **El camino de la información:** ¿Qué es una IP, un Dominio y un Certificado SSL? (Explicado como dirección postal y sello de autenticidad).
- **Sistemas Operativos en la Empresa:** Breve repaso de Windows Server vs. Linux (enfocado en qué buscar en cada uno).

Actividad Práctica:

- **Mapeo de Red Simple:** Utilizar herramientas gratuitas (como ping o whois) para entender de dónde viene un servicio web.
- **Identificación de "Puntos de Dolor":** En un diagrama de red simple, marcar dónde están los datos más sensibles.

2. Gestión de Activos y "Shadow IT" (El Mapa)

- **Gestión de Activos (Asset Management):** Por qué una notebook perdida o un celular personal con datos de la empresa son riesgos críticos.
- **Shadow IT:** El peligro de las herramientas que los empleados usan sin avisar (ej. un Dropbox personal para archivos del trabajo).
- **Ciclo de vida del hardware:** Desde la compra hasta la destrucción segura de discos duros.

Actividad Práctica:

- **Creación de un Inventario Crítico:** Ejercicio de registro de activos utilizando una plantilla profesional, incluyendo fechas de parches y responsables.
- **Escaneo de Red Básico:** Uso de herramientas tipo *Advanced IP Scanner* para ver qué dispositivos están conectados a la red de la oficina.

3. Monitoreo y Detección de Anomalías (La Torre de Vigilancia)

- **Eventos vs. Incidentes:** Por qué un login fallido es un evento, pero 100 logins fallidos en un minuto es un incidente.
- **Introducción al SOC y SIEM:** Conceptos básicos de centralización de alertas (sin entrar en configuraciones complejas).
- **Lectura de Dashboards:** Cómo interpretar los gráficos de un Antivirus Corporativo (EDR).

Actividad Práctica:

- **Simulación de Triaje:** Se le presentan al cursante 5 alertas de seguridad y debe clasificarlas por prioridad (Baja, Media, Alta, Crítica) justificando su decisión.
- **Lectura de Logs con "Ojos Humanos":** Revisar un archivo de registro de accesos y encontrar el "intruso" basándose en horarios inusuales.

4. Taller Práctico II (IA y Documentación)

- **Prompt Engineering para Seguridad:** Cómo usar ChatGPT o Gemini para que nos explique qué significa una línea de código sospechosa o un error de sistema extraño.
- **Sistemas de Tickets:** Práctica de apertura, seguimiento y cierre de un ticket de seguridad (uso de herramientas tipo Trello o Jira simplificado).
- **Redacción Técnica para Humanos:** Cómo informar a un jefe que "algo anda mal" sin causar pánico pero con la urgencia necesaria.

Entregable: Un "Informe Semanal de Salud Digital" que resuma lo que el operador "vio" durante su guardia simulada.

Cumplimiento, Respuesta y Resiliencia

1. El Marco Legal y Regulatorio (Las Reglas del Juego)

- **Introducción a Normativas Locales:** Qué piden reguladores como el **BCRA** (para Fintechs) o la **Ley de Protección de Datos Personales** en Argentina/Región.
- **Estándares Internacionales (en lenguaje simple):** Qué es la ISO 27001 y por qué a las empresas les importa tanto "certificar".
- **Ética Profesional:** La importancia de la confidencialidad y el manejo de información sensible por parte del operador.

Actividad Práctica - Checklist de Cumplimiento:

- Tomar una normativa simplificada y verificar si una oficina ficticia la cumple (Ej. "¿Los datos de los clientes están cifrados?").

- **Búsqueda de Brechas:** Analizar una noticia reciente de una filtración de datos y ver qué ley se incumplió.

2. Respuesta a Incidentes (Primeros Auxilios Digitales)

- **Ciclo de Vida del Incidente:** Detección, contención, erradicación y recuperación.
- **El Rol del Operador en la Crisis:** No es "arreglarlo todo", sino ser el cronista y el apoyo (tomar tiempos, documentar qué se hizo).
- **Protocolos de Escalamiento:** ¿Cuándo un problema de soporte se convierte en una emergencia de seguridad?

Actividad Práctica - Simulacro de "Botón de Pánico"

- Recibir una alerta de Ransomware y ejecutar un "Playbook" (manual de pasos) de emergencia: aislar la máquina, avisar al CISO, documentar el estado.
- **Redacción de Reporte:** Escribir un informe post-incidente para que la gerencia entienda qué pasó sin tecnicismos.

3. Continuidad del Negocio y Resiliencia (El Seguro de Vida)

- **Estrategia de Backups (3-2-1):** 3 copias, 2 medios distintos, 1 fuera de línea.
- **Resiliencia vs. Seguridad:** Por qué no basta con ser "fuertes", sino que hay que ser "elásticos" (saber volver a la normalidad rápido).
- **Puntos Críticos de Recuperación (RTO y RPO):** ¿Cuánto tiempo puede estar la empresa sin sistema?

Actividad Práctica - Plan de Recuperación Casero:

- Diseñar un plan de respaldo para una pequeña oficina contable.
- **Prueba de Restauración:** Verificar si una copia de seguridad realmente funciona (simulacro de "vuelta a la vida").

4. Proyecto Final y Salida Laboral

Examen de Certificación (Práctico) - "Un día en la vida del Operador": El cursante debe gestionar una consola simulada durante 2 horas, detectando 3 incidentes, documentándolos y reportándolos correctamente.

Taller de Empleabilidad:

- **LinkedIn para Ciberseguridad:** Cómo destacar las "Skills" aprendidas, aunque no se tenga experiencia previa.
- **El CV del Asistente de Riesgos:** Qué palabras clave buscan los reclutadores (IAM, EDR, Phishing, Compliance).
- **Role-Play de Entrevista:** Cómo explicar el valor de un "Operador" en una PYME que aún no sabe que lo necesita.