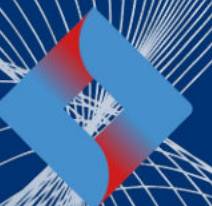




WORKSHOP

PRINCIPIOS DE CIBERSEGURIDAD BÁSICA EN EL SECTOR LOGÍSTICO



DIRIGIDO A:

Colaboradores que laboren en el área de tecnología en empresas del sector logístico.

Profesionales de logística: Encargados de la planificación y ejecución de las operaciones logísticas en la cadena de suministro.

Personas que laboren en el sector con interés en comprender y mitigar los riesgos cibernéticos en la cadena de suministro.



OBJETIVO GENERAL

Brindar conocimientos fundamentales sobre ciberseguridad, sus principios, herramientas básicas y buenas prácticas para proteger información y sistemas de amenazas cibernéticas.



CONTENIDO DEL PROGRAMA

MÓDULO

01



**1. Introducción a la
Ciberseguridad**

MÓDULO

02



**2. Fundamentos de
Redes y Seguridad en
Internet.**

MÓDULO

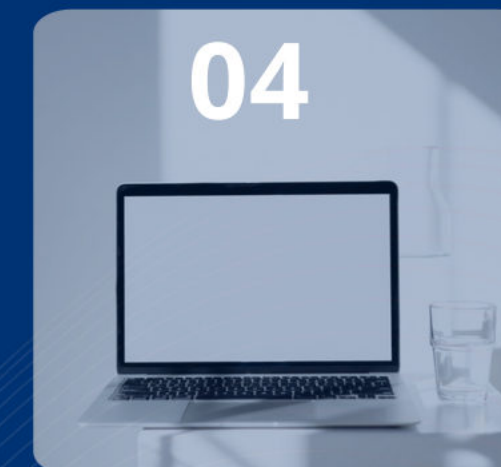
03



**3. Herramientas
Básicas de
Ciberseguridad**

MÓDULO

04



**4. Buenas Prácticas
y Planes de
Respuesta**



MÓDULO I

Introducción a la Ciberseguridad

Duración: 2 horas

Conceptos básicos de ciberseguridad.

- Definición e importancia.
- Diferencia entre seguridad informática y ciberseguridad.

Principales amenazas y riesgos cibernéticos:

- Malware (virus, ransomware, spyware, troyanos).
- Phishing y ataques de ingeniería social.
- Amenazas internas.

Confidencialidad, Integridad y Disponibilidad (CIA):

- Principios básicos de la seguridad.

Actividades:

- Discusión guiada: Ejemplos de ataques cibernéticos recientes.
- Ejercicio práctico:
Identificar amenazas en casos hipotéticos.

MÓDULO II

Fundamentos de Redes y Seguridad en Internet .

Duración: 2 horas

Cómo funcionan las redes:

- Conceptos básicos: IP, DNS, protocolos (HTTP, HTTPS, FTP, etc.).
- Puertos y su relevancia en la ciberseguridad

Seguridad en el uso de internet:

- Navegación segura.
- Importancia de las actualizaciones y los parches.

Amenazas comunes en redes:

- Ataques DDoS.
- Escucha clandestina (sniffing).

Actividades:

- Demo: Cómo un ataque de phishing puede capturar datos.
- Práctica: Configuración básica de un firewall personal.



MÓDULO III

Herramientas Básicas de Ciberseguridad

Duración: 2 horas

Software esencial para la seguridad:

- Antivirus y antimalware.
- VPNs y su uso.

Gestión de contraseñas:

- Herramientas de gestión de contraseñas (p. ej., LastPass, Bitwarden).
- Buenas prácticas para contraseñas seguras.

Introducción a análisis de vulnerabilidades:

- Escaneo básico con herramientas como Nessus o Nmap (demo).

Actividades:

- Práctica: Crear contraseñas seguras con gestores. Ejemplo guiado: Uso básico de Nmap para escaneo de puertos.

MÓDULO IV

Buenas Prácticas y Planes de Respuesta

Duración: 2 horas

Buenas prácticas de ciberseguridad:

- Buenas prácticas de ciberseguridad:
- Principios de seguridad por diseño. o Uso de doble autenticación (2FA).

Gestión de incidentes:

- Cómo identificar y responder a incidentes cibernéticos.
- Introducción a los planes de recuperación ante desastres (DRP).

Protección de datos personales:

- Cumplimiento de normativas básicas (GDPR, CCPA).

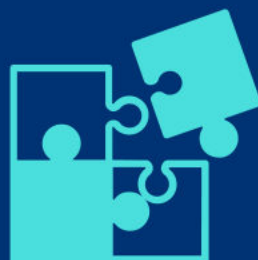
Actividades:

- Simulación: Respuesta a un incidente cibernético.
- Trabajo en grupo: Diseñar un esquema de buenas prácticas para un escenario ficticio.

Evaluación y Cierre



DURACIÓN: 30 MINUTOS



Evaluación y Cierre

- Resumen de conceptos claves.
- Cuestionario práctico de repaso.
- Sesión de preguntas y respuestas.



- Presentaciones y guías en PDF.
- Acceso a software gratuito (p. ej., Wireshark, Nmap).
- Lecturas recomendadas (blogs, artículos y manuales básicos).

