Curso:

Ciberseguridad: Phishing y Fraude Digital.

A lo largo de este curso, se abordarán tanto conceptos clave como principios y terminología necesaria, para profundizar en técnicas y metodologías actualmente empleadas en la protección de las infraestructuras de información de una organización.

Dirigido a	Personas funcionarias y servidores del sector público y municipal, que tengan un entendimiento básico de la ciberseguridad o que hayan completado el curso de Introducción a la Ciberseguridad (Nivel 1).
Objetivo de aprendizaje	Se espera que quienes participan del curso puedan profundizar sobre la protección de datos y la gestión de riesgos, para así dar respuesta ante posibles incidentes cibernéticos al interior de su organización.
Objetivo general	Entregar habilidades y conocimientos necesarios para gestionar y mitigar riesgos de ciberseguridad de manera efectiva.
Objetivos específicos	1. *Comprender* los conceptos clave, principios y terminología de la ciberseguridad. 2. *Aplicar* herramientas que permitan reconocer aquellas técnicas y principios de manipulación psicológica empleados por los ciberdelincuentes en la ingeniería social. 3. *Conocer* estrategias efectivas y prácticas recomendadas para para garantizar la seguridad de la información personal y de sus dispositivos.
Metodología	El curso se desarrollará en modalidad online asincrónico, a través de la plataforma dispuesta por el Centro de Estudios de la Administración del Estado. Los contenidos del curso tienen una carga académica equivalente a **3 horas cronológicas**, las que pueden ser desarrolladas de manera autónoma e individual durante las 24 horas del día, en el horario que estime pertinente.

Contenidos

1. Módulo 1: Entendimiento básico de la ciberseguridad.

- ¿Qué es la ciberseguridad?
- Estadísticas de ataques
- Actores del ciberespacio.
- Amenazas cibernéticas.
- La importancia personal y global de la ciberseguridad.
- Resumen del módulo.
- Actividad

2. Módulo 2: Ingeniería social y manipulación psicológica.

- ¿Qué es la ingeniería social?
- Ocasiones y/o Vulnerabilidades.
- Técnicas comunes de ingeniería social.
- ¿Cómo evitar ser víctima de la ingeniería social?
- ¿Cómo reconocer un ataque cibernético?

	• Resumen del módulo. • Actividad. **3. Módulo 3: Mejores prácticas para proteger tus datos y dispositivos.** • Protección contra malware y ransonware. • ¿Cómo actuar si tu dispositivo ha sido infectado? • Seguridad de contraseñas y gestión de credenciales. • Navegación segura en internet. • Protección de datos y privacidad en línea. • Seguridad en redes sociales y plataformas en línea. • Riesgos de compartir información en línea. • ¿Cómo reportar delitos cibernéticos? • ¿Cómo protegerte de las consecuencias legales de los delitos cibernéticos? • Resumen del módulo. • Actividad. **4. Cierre del curso:** • ¡No seas víctima del Hacking!: Consejos
Evaluación →	El curso contempla una Evaluación al Final luego de revisar todo el contenido del curso y de haber completado las actividades de cada módulo. La evaluación contempla **20 preguntas** de selección múltiple y se considerara está aprobada con el **65%** de las respuestas correctas (13 preguntas). Cada participante tendrá **1 hora** para resolver dicha evaluación, desde que accede a la realización del cuestionario. En caso de no lograr el porcentaje mínimo de aprobación (65%), las personas que participan del curso podrán rendir un segundo intento para intentar cumplir con el requisito mínimo de aprobación. Esta será la última instancia para aprobar el curso.
Certificación →	Se entregará un certificado al finalizar el curso a quienes hayan ejecutado de manera completa cada uno de los 3 módulos, y obtengan el puntaje necesario para aprobar el mismo. Es responsabilidad de quien realiza el curso descargar el certificado, directamente desde la plataforma, una vez respondida la encuesta de satisfacción.