FICHA TÉCNICA DE INICIATIVAS DE CAPACITACIÓN

PLAN DE CAPACITACIÓN CCC 2025 – 2026

El Comité de Creación de Capacidades (CCC) de la OLACEFS está llevando a cabo un mapeo de iniciativas de formación en virtud del Plan de Capacitación 2025 – 2026, cuya finalidad es fortalecer las capacidades institucionales y profesionales de las EFS en materias atingentes como Transformación Digital y Gobernanza de TI, Medio Ambiente y Cambio Climático, Prevención y Lucha contra la Corrupción, Compras y Contratación Pública, como así también aquellas que se han venido trabajando como habilidades transversales y en materia de auditoría.

FICHA TÉCNICA	
Institución: Corte de Cuentas de la República de El Salvador	**Nombre de la iniciativa de capacitación:** Seguridad de la Información y Ciberseguridad
Modalidad: Virtual	**Duración (horas cronológicas/pedagógicas): 60**
Tipo de actividad: Curso	**Nivel de la actividad[1]:** Intermedio

Objetivo General

Proporcionar a los participantes los conocimientos y habilidades necesarias para implementar y gestionar estrategias efectivas de seguridad de la información y ciberseguridad en el sector público, con el fin de proteger los datos sensibles, prevenir amenazas cibernéticas y garantizar la integridad, confidencialidad y disponibilidad de la información gubernamental.

Objetivos de aprendizaje

- Comprender los principios fundamentales de la Seguridad de la Información, incluyendo la confidencialidad, integridad y disponibilidad (modelo CIA), y su aplicabilidad en el sector público.
- Analizar las amenazas, vulnerabilidades y riesgos cibernéticos que afectan a las instituciones públicas y cómo estas pueden comprometer la protección de datos sensibles y sistemas tecnológicos.
- Identificar y aplicar las normativas y marcos internacionales de ciberseguridad y protección de datos, como la ISO/IEC 27001 y NIST.

[1] **Nivel Básico:** Cursos que tienen por objetivo introducir: Introducir los conceptos y los términos básicos del tema. Se centra en la comprensión general y en la adquisición de habilidades elementales. Ideal para principiantes sin experiencia previa en la materia. No se requieren conocimientos previos ni habilidades técnicas específicas.
Nivel Intermedio: Cursos que tengan por objetivo profundizar en los temas, aumentar la comprensión técnica y aplicar conocimientos en proyectos o situaciones específicas. Dirigido a quienes cuentan con conocimientos básicos del tema o experiencia práctica (validad por la EFS). Se asume familiaridad con los conceptos esenciales y la terminología.
Nivel Avanzado: Cursos que tengan por objetivo explorar temas complejos, desarrollar habilidades especializadas y resolver problemas avanzados. Enfocado en personas con una sólida base de conocimientos o experiencia significativa en el área. Ideal para quienes buscan perfeccionar habilidades o alcanzar un nivel experto (validado por la EFS).

▪ Implementar controles y medidas de seguridad en la infraestructura tecnológica, incluyendo redes, aplicaciones y sistemas, para mitigar riesgos de ciberataques y proteger la información institucional.

Pilares de capacitación:	**Requiere de tutor:**
Transformación Digital y Gobernanza de TI	NO

PERFILES

Perfil de ingreso[2]:	**Perfil de egreso:**
▪ Cargos en áreas relacionadas con: Tecnologías de la Información (TI), Gestión de datos y protección de la información, Administración pública y gestión de servicios gubernamentales, Seguridad informática y ciberseguridad, Gestión de riesgos tecnológicos en instituciones públicas. ▪ Conocimientos previos básicos en el uso de tecnologías digitales y su aplicabilidad en los procesos de la administración pública. ▪ Interés en fortalecer la protección de la información y los sistemas tecnológicos dentro de la institución, con especial atención a la prevención de ciberataques y la implementación de estrategias de ciberseguridad. ▪ Disponibilidad para aprender sobre las principales normativas y marcos de seguridad en el ámbito de la ciberseguridad, como ISO 27001, y cómo aplicarlos en la práctica dentro de su entorno institucional. ▪ Capacidad para trabajar con herramientas informáticas básicas, así como un compromiso por desarrollar habilidades técnicas relacionadas con la gestión de la seguridad digital. ▪ Disposición para implementar políticas de seguridad y fomentar una cultura de protección de datos y privacidad en su institución pública.	▪ Capacidad para diseñar, implementar y mantener un sistema de gestión de seguridad de la información (SGSI) basado en marcos y normas internacionales, como ISO 27001, para garantizar la protección de los datos institucionales. ▪ Habilidad para identificar vulnerabilidades en la infraestructura tecnológica de la institución pública y aplicar medidas correctivas para mitigar riesgos y prevenir ciberataques. ▪ Competencia para desarrollar políticas de ciberseguridad robustas y alineadas con los marcos normativos nacionales e internacionales, promoviendo la protección de la información y la resiliencia ante incidentes cibernéticos. ▪ Capacidad para gestionar incidentes de seguridad cibernética, desde la detección hasta la resolución, implementando procedimientos de respuesta y recuperación adecuados. ▪ Habilidad para diseñar e implementar programas de formación y concientización para el personal de la institución, promoviendo prácticas seguras y reduciendo el riesgo de ataques cibernéticos a través de la capacitación. ▪ Competencia para garantizar el cumplimiento de normativas y regulaciones nacionales e internacionales en materia de seguridad de la información, como el GDPR y la Ley de Protección de Datos Personales, adaptándolas a las necesidades del sector público. ▪ Habilidad para implementar medidas de protección de datos personales y garantizar la privacidad de la información en el ámbito de la administración pública.

REQUISITOS

Requisitos de postulación[3]:	**Requisitos de aprobación:**
▪ Desempeñar funciones en áreas relacionadas con las tecnologías de la información o control institucional. ▪ Contar con al menos un año de experiencia profesional en el uso, administración o supervisión de herramientas tecnológicas, sistemas de	Alcanzar el porcentaje mínimo de aprobación (Nota mínima 80%)

[2] Características generales, habilidades o conocimientos previos que se espera que los participantes tengan para aprovechar mejor la capacitación. Es una descripción de un "perfil ideal" para quien asiste al curso, pero no necesariamente es obligatorio.

[3] Criterios obligatorios que deben cumplir los participantes para poder inscribirse o asistir al curso.

información o procesos de control institucional. ▪ Poseer conocimientos básicos sobre entornos digitales, sistemas informáticos y/o gestión de la información en el ámbito institucional. ▪ Disponer de los recursos técnicos necesarios para participar en modalidad virtual, como equipo con acceso a internet estable (si aplica). ▪ Contar con el aval o respaldo institucional para su participación en el curso.	
EVALUACIONES	
Tipos de evaluación: Test de evaluación de conocimiento	**Posee encuesta de satisfacción:** **SI**
CONTENIDO	
Temario/programa: 1. Gestión de la seguridad de la información. 2. Protección de datos personales y normativas internacionales. 3. Concientización y cultura de seguridad.	

***Se solicita adjuntar el programa o silabo de la iniciativa de capacitación.**

CORTE DE CUENTAS DE LA REPÚBLICA
DIRECCIÓN
CENTRO DE INSTRUCCIÓN Y CAPACITACIÓN
EL SALVADOR, C.A.