

PROTOCOLO ■■■
PROVINCIAL DE CIBERSEGURIDAD

Políticas de Concientización y Entrenamiento en Seguridad

07
CAPÍTULO



Políticas de Concientización y Entrenamiento en Seguridad

1.0 OBJETIVO

Garantizar que se brinde el nivel adecuado de capacitación en concientización sobre seguridad de la información a todos los usuarios de Tecnología de la Información (TI).

2.0 REFERENCIAS

Publicaciones especiales del Instituto Nacional de Estándares y Tecnología (NIST): NIST SP 800-53: Concientización y capacitación (AT), NIST SP 800-12, NIST SP 800-16, NIST SP 800-50, NIST SP 800-100; Código Electrónico de Regulaciones Federales (CFR): 5 CFR 930.301

3.0 POLÍTICA

Esta política es aplicable a todos los departamentos y usuarios de recursos y activos de TI.

1. FORMACIÓN DE CONCIENTIZACIÓN EN SEGURIDAD

El Ministerio de Planificación Estratégica y Modernización - MPEyM deberá:

- a. Programar capacitación en concientización sobre seguridad como parte de la capacitación inicial para nuevos usuarios.
- b. Programar capacitación en concientización sobre seguridad cuando lo requieran los cambios en el sistema de información y periódicamente con la frecuencia necesaria en cada Unidad de Organización.
- c. La oficina de TI determinará el contenido adecuado de la formación en materia de concienciación sobre la seguridad y las técnicas de concienciación sobre la seguridad en función de los requisitos organizativos específicos y los sistemas de información a los que el personal tiene acceso autorizado. El contenido deberá:
 - i. Incluir una comprensión básica de la necesidad de seguridad de la información y acciones de los usuarios para mantener la seguridad y responder a incidentes de seguridad sospechosos.

- ii. Abordar la concientización sobre la necesidad de seguridad en las operaciones. Las técnicas de concientización sobre la seguridad pueden incluir, por ejemplo, exhibir carteles, ofrecer suministros con recordatorios de seguridad, generar avisos por correo electrónico de altos funcionarios de la organización, mostrar mensajes en la pantalla de inicio de sesión y realizar eventos de concientización sobre la seguridad de la información.

2. CONCIENCIA EN SEGURIDAD | AMENAZA INTERNA

El Departamento de TI deberá:

- a. Incluir capacitación en concientización sobre seguridad para reconocer e informar indicadores potenciales de amenazas internas.

3. FORMACIÓN EN SEGURIDAD BASADA EN FUNCIONES

El Departamento de TI deberá:

- a. Proporcionar capacitación en seguridad basada en roles al personal con roles y responsabilidades de seguridad asignados:
 - i. Antes de autorizar el acceso al sistema de información o realizar las funciones asignadas.
 - ii. Cuando lo requieran cambios en el sistema de información y una frecuencia periódica definida por MPEyM, después de eso.
- b. Designar personal para recibir capacitación inicial y continua en el empleo y operación de controles ambientales que incluyan, por ejemplo, dispositivos/sistemas de detección y extinción de incendios, sistemas de rociadores, extintores de incendios portátiles, mangueras fijas contra incendios, detectores de humo, temperatura/humedad, HVAC, y energía dentro de la instalación.

4. CONTROLES DE SEGURIDAD FÍSICA

El Departamento de TI deberá:

- a. Proporcionar capacitación inicial y continua en el empleo y operación de controles de seguridad física; Los controles de seguridad física incluyen, por ejemplo, dispositivos de control de acceso físico, alarmas de intrusión física, equipos de monitoreo/vigilancia y guardias de seguridad (procedimientos operativos y de implementación).

- b. Identificar personal con roles y responsabilidades específicas asociadas con los controles de seguridad física que requieren capacitación especializada.

5. EJERCICIOS PRACTICOS

La oficina de TI deberá:

- a. Proporcionar ejercicios prácticos de formación en seguridad que refuercen los objetivos de la formación; Los ejercicios prácticos pueden incluir, por ejemplo, capacitación en seguridad para desarrolladores de software que incluya ataques cibernéticos simulados que exploten vulnerabilidades comunes del software (por ejemplo, desbordamientos de buffer), o ataques de phishing dirigidos a líderes/ejecutivos de alto nivel. Este tipo de ejercicios prácticos ayudan a los desarrolladores a comprender mejor los efectos de dichas vulnerabilidades y a apreciar la necesidad de estándares y procesos de codificación segura.

6. COMUNICACIONES SOSPECHOSAS Y COMPORTAMIENTO ANÓMALO DEL SISTEMA

La oficina de TI deberá:

- a. Proporcionar capacitación a su personal específico sobre cómo reconocer comunicaciones sospechosas y comportamientos anómalos en los sistemas de información organizacionales.

7. REGISTROS DE ENTRENAMIENTO EN SEGURIDAD

El MPEyM deberá:

- a. Designar personal para documentar y monitorear las actividades individuales de capacitación en seguridad de sistemas de información, incluida la capacitación básica en concientización sobre seguridad y la capacitación específica en seguridad de sistemas de información.
- b. Conservar registros de capacitación individuales por una periodicidad de cinco años.

4.0 CUMPLIMIENTO

Los empleados que incumplan esta política pueden estar sujetos a medidas disciplinarias, así como sanciones penales, civiles y/o administrativas si correspon-

dieren. Los terceros/proveedores, incluidos, entre otros, los contratistas, pueden estar sujetos a la rescisión de acuerdos contractuales, a la denegación de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

5.0 EXCEPCIONES DE POLÍTICA

Las solicitudes de excepciones a esta política serán revisadas por la Dirección de Ciberseguridad (DC), la Secretaría de Innovación Pública (SIP) y/o Encargado de Seguridad de la Información. Los departamentos que soliciten excepciones deberán proporcionar dichas solicitudes al DC/SIP. La solicitud debe indicar específicamente el alcance de la excepción junto con la justificación para otorgar la excepción, el posible impacto o riesgo asociado al otorgar la excepción, las medidas de mitigación de riesgos que debe tomar el Departamento de TI, iniciativas, acciones y un cronograma para lograrlo, el nivel mínimo de cumplimiento de las políticas aquí establecidas. El DC/SIP revisará dichas solicitudes; consultar con el departamento solicitante.

6.0 FECHA DE EMISIÓN / FECHA DE REVISIÓN

Fecha	Descripción de Cambio	Crítico
26-06-2024	Draft final del documento	Alejandro Castro Pablo Zalazar