POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO DE CAPACITACIÓN PARA EL TRABAJO DEL ESTADO DE CHIHUAHUA

Instituto de Capacitación para el Trabajo del Estado de Chihuahua
Políticas de seguridad de la información Versión 1.0
Chihuahua, Chihuahua a 20 de noviembre de 2024

JOSE ÁRTURO MORALES REYES
Director General

ALBA ABISSAG DOMÍNGUEZ RÍOS
Jefa del Departamento Jurídico

EUGENIA HAYDEE JACINTO RIOSVELASCO
Directora de Vinculación

YASMIN AIDA MURILLO CHANEZ
Directora Académica

GLADYS CHÁVEZ PORTILLO
Directora de Planeación

ALBERTO JORGE GARCÍA NAVARRO
Director Administrativo

Elaboraron:
TANIA VICTORIA SÍGALA TARÍN
SELENE HERNÁNDEZ MUÑOZ

www.icatech.edu.mx

Autorizado en H. Junta Directiva mediante acuerdo ICT-15.04/2024 el día 20 de noviembre de 2024.

Contenido

I.INTRODUCCIÓN

Un Sistema de Gestión de la Seguridad de la Información (SGSI) es un marco de políticas, procedimientos y controles diseñados para gestionar la seguridad de la información en una organización. Su objetivo principal es proteger la confidencialidad, integridad y disponibilidad de la información, que son los pilares de la seguridad de la información.

La Política de Seguridad de la Información es un documento fundamental dentro de un Sistema de Gestión de la Seguridad de la Información (SGSI), y establece las directrices y principios que guían la gestión y protección de la información en una organización

El presente documento refleja las políticas de seguridad de la información definidas por el Departamento de Sistemas adscrito a la Dirección de Planeación del Instituto de Capacitación para el Trabajo del Estado de Chihuahua (ICATECH), con el objetivo de mantener en la medida de lo posible la seguridad e integridad de la seguridad de la información del ICATECH buscando los máximos niveles posibles de la confidencialidad, integridad y disponibilidad, autenticidad, confiabilidad, trazabilidad y no repudio de la información Institucional generada, recibida, procesada, almacenada y compartida a través de sus sistemas, aplicaciones, infraestructura y personal.

El Departamento de Sistemas será responsable de la aplicación y actualización de este documento.

Esta política es de observancia obligatoria para todo el personal del Instituto, personal de apoyo, personas prestadoras de servicio social y prácticas profesionales, y en general, a toda persona externa a la que se le de acceso a la red institucional. Además, abarca a los sistemas informáticos, software, documentación o información, equipos y demás recursos de Tecnologías de la Información.

II.GLOSARIO

Activos de información. Elemento, recurso, canal, persona, equipo o intangible, que tiene la capacidad para incidir en la generación, almacenamiento, transmisión o gestión en general de datos e información de la organización o de sus terceros.

ICATECH o Instituto. Instituto de Capacitación para el Estado de Chihuahua del Estado de Chihuahua

Equipo. computadoras de escritorio, equipos portátiles, servidores y de comunicaciones electrónicas con todos sus componentes de software y hardware, así como internos, tarjetas de expansión o componentes externos como bocinas o módems, monitor, teclado y ratón, sin ser estos los únicos existentes. Incluye también equipo de proyección e

impresión de cualquier modelo, tipo o marca que sirva como interfaz de salida física en papel u otro medio.

TICs, Tecnologías de la Información y Comunicaciones. Son el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios; que permiten la compilación, procesamiento, almacenamiento, transmisión de información como: voz, datos, texto, video e imágenes.

Usuario. Toda persona interna o externa que accede y utiliza activos de información.

1. POLÍTICA DE SEGURIDAD INFORMÁTICA

1.1. DEFINICIÓN

Se define la seguridad de la información como la preservación de la confidencialidad, integridad y disponibilidad de la información. Estas propiedades de la información la podemos definir de la siguiente manera:
Confidencialidad: Acceden a la información únicamente quienes están autorizados, trátese de personas, entidades o procesos.
Integridad: La información es precisa, confiable y completa.
Disponibilidad: La información está disponible cuanto la necesitan quienes están autorizados a acceder a ella.

1.2. INVENTARIO DE ACTIVOS DE INFORMÁCIÓN

El Departamento de Recursos Materiales realizará los resguardos y proporcionará de forma mensual los inventarios con los datos de número de inventario, responsable del activo, costo de inversión, datos del contrato y proveedor en caso de aplicar, al Departamento de Sistemas quien complementará que tipo de información que contienen, procesan, transfieren, transportan o almacenan.

El Departamento de Sistemas concentrará un inventario centralizado y actualizado de los recursos (equipos, sistemas, licencias, marcas, dominios, infraestructura, entre otros) de Tecnologías de la Información del Instituto, donde se detallará: el responsable del activo, tipo de información que contienen, procesan, transfieren, transportan o almacenan, costo de la inversión, datos del contrato y proveedor en caso de aplicar.

1.3. USO DE ACTIVOS DE INFORMACIÓN

El personal, prestadores de servicio social, proveedores y terceros son responsables de los recursos asignados para el buen uso de la información; cuando se autorice el acceso a algún recurso, el responsable del activo definirá las políticas para otorgar el acceso y asignará una carta responsiva donde el usuario aceptará las normas para la administración, control y operación del recurso asignado.

Se contará con un procedimiento de resguardo y restauración de información para el uso de los activos de la información; de acuerdo con lo siguiente:

- Equipos de cómputo, equipos portátiles; el usuario utilizará la herramienta que designe el Departamento de Sistemas para el respaldo y restauración de la información.
- Servidores, el responsable del activo realizará las tareas de respaldo según la periodicidad que defina registrando esta situación en una bitácora la cual debe contener por cada respaldo realizado: fecha y hora, tamaño y nombre del archivo, ubicación, nombre y firma de quien supervisó el respaldo. Es importante realizar pruebas periódicas para asegurarse que los respaldos funcionan correctamente y que los datos se pueden restaurar en caso de una pérdida. Estas pruebas deben realizarse al menos una vez al año.

1.4. ADMINISTRACIÓN DE RIESGOS

El análisis de riesgos informáticos es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de estas, a fin de determinar los controles adecuados para evitar, asumir, reducir, compartir y transferir la ocurrencia de un riesgo.

El Departamento de Sistemas generará una Matriz de Riesgos para sus activos de información, generando acciones de control, las cuales incluirá en el Plan Institucional de TIC´s que elabora cada año; presentando los avances en las sesiones del Comité de Control y Desempeño Institucional.

El seguimiento, evaluación y reevaluación de la Administración de Riesgos se llevará conforme a la normatividad emitida por la Secretaría de la Función Pública.

1.5. RESPONSABILIDADES ADMINISTRATIVAS

Las políticas de seguridad informática deberán cumplirse en todo momento, cualquier incumplimiento será tratado conforme a la normatividad aplicable.

1.6. CAPACITACIÓN DEL PERSONAL EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN

Dentro del plan de trabajo del Departamento de Sistemas se deberá considerar la capacitación periódica al personal del Instituto para que tome conciencia de los problemas de seguridad de la información, fomentando una cultura de seguridad de la información, realizando esto a través de:

- Correos electrónicos.
- Videos institucionales.
- Pláticas.
- Capacitaciones.

1.7. ESTÁNDARES ADICIONALES

El Departamento de Sistemas podrá complementar estas políticas con normas que emita el Gobierno del Estado de Chihuahua.

2. RESPONSABILIDADES

2.1. USUARIOS

a) Proteger la seguridad de los recursos de tecnologías de la información bajo su control, de acuerdo con las instrucciones y la capacitación recibida.
b) Cumplir con las instrucciones y los procedimientos de seguridad aprobados y aquellas responsabilidades de seguridad especificas documentadas en los objetivos personales y la descripción de tareas.
c) Mantener la confidencialidad de los usuarios, contraseñas asignadas y evitar que terceros utilicen los derechos de acceso de los usuarios autorizados.
d) Informar al Departamento de Sistemas cualquier sospecha de violaciones de seguridad y de cualquier debilidad detectada en los controles de esta, incluyendo sospechas de divulgación de contraseñas.

2.2. DEL JEFE DE DEPARTAMENTO DE SISTEMAS

a) Sobre el personal a su cargo: Revisar que las descripciones de puestos incluyan las responsabilidades específicas de seguridad informática previo a la firma del contrato de trabajo.

b) Documentar las autorizaciones que le otorgue al personal y/o terceros de acceso a los servidores y bases de datos a su cargo y en caso de baja, suspensión o detecte un riesgo, realizar un cambio de contraseñas

2.3. CONTRATOS DE SERVICIO

En caso de contratar algún servicio para suministrar bienes o prestar servicios de informática el área requirente deberá exigir al proveedor que cumpla con las políticas de seguridad informática, describiendo las que apliquen en el contrato del servicio.

3. SEGURIDAD FÍSICA

3.1. INSTALACIONES DE TICs

Las instalaciones de TICs deberán ser ubicadas y diseñadas de forma que se reduzcan los riesgos resultantes de desastres naturales y riesgos de otra naturaleza; para su construcción o remodelación se deberá buscar asesoría en la materia.

Deberá considerar:

- Control de acceso físico.
- Energía eléctrica y servicios de telecomunicaciones.
- Medidas de prevención de incendios, inundaciones.
- Control de temperatura, humedad y ventilación.

3.2. CONTROLES DE ACCESO FÍSICO

El titular del Departamento de Sistemas documentará las autorizaciones de acceso a las instalaciones de TICs detallando: quien accede, equipo al cual se accede, periodo de tiempo, motivo.

3.3. POLÍTICAS DE USO DE EQUIPOS

Se describen en el documento “Políticas de uso de equipos de cómputo en el Instituto de Capacitación para el Trabajo del Estado de Chihuahua”.

4. SEGURIDAD VIRTUAL

4.1. CONTROLES DE ACCESO VIRTUALES

4.1.1. ACCESO A SERVIDORES Y BASE DE DATOS

El titular del Departamento de Sistemas documentará las autorizaciones de acceso a los servidores y bases de datos detallando: quien accede, equipo al cual se accede, periodo de tiempo, motivo.

4.1.1. ACCESO A SISTEMAS Y APLICACIONES

Para otorgar acceso a los sistemas y aplicaciones administrados por el Departamento de Sistemas adscrito a la Dirección de Planeación se seguirán las siguientes políticas:

- La solicitud de alta o modificación de usuarios se deberá capturar en el Sistema Informático Integral, y será por persona. La solicitud deberá detallar a que sistemas o aplicaciones se dará acceso y en el caso del Sistema Informático Integral se especificarán las funciones que desempeñará. La captura de la solicitud será conforme a lo siguiente:

  - ✓ Para los puestos de dirección general, direcciones de área, direcciones de plantel, jefaturas de acción móvil y jefatura del departamento jurídico, la captura la realizará el titular del Departamento de Capital Humano.

  - ✓ Para el resto del personal no incluido en el párrafo anterior, la captura la realizará el jefe directo.

  - ✓ Para personas ajenas al Instituto, la captura la realizará el director de área donde se encuentre comisionada dicha persona.

- La persona a la cual se le asigne usuario firmará una carta responsiva aceptando las normas para la administración, control y operación de los sistemas o aplicaciones asignados.

4.1.2. BAJA O SUSPENSIÓN DE SISTEMAS Y APLICACIONES

Para proteger la infraestructura, sistemas y datos se limitará el acceso a los sistemas y aplicaciones administrados por el Departamento de Sistemas conforme a lo siguiente:

- La solicitud de baja o suspensión temporal de usuarios se deberá capturar en el Sistema Informático Integral, especificando la fecha del movimiento, en el caso de suspensión, el periodo que comprende esta. La solicitud se captura por persona y debe detallar a que sistemas o aplicaciones se cancelará o limitará el acceso, en el caso del Sistema Informático Integral se detallarán las funciones que se cancelarán. La captura de la solicitud será de acuerdo con lo siguiente:

✓ Para baja o suspensión de usuarios, será el jefe directo de la persona quien capturará la solicitud.

✓ En caso de requerirlo, el usuario podrá solicitar también su baja o suspensión temporal.

✓ Para baja o suspensión temporal del usuario por motivo confidencial, será el titular del Departamento de Capital Humano quien realizará la captura, pudiendo informar verbalmente al titular del Departamento de Sistemas, quien le solicitará la captura de la solicitud posteriormente.

4.2. CONTRASEÑAS

Consideraciones de contraseñas para usuarios de sistemas y aplicaciones a cargo del Departamento de Sistemas

- La contraseña debe de ser mínimo 9 caracteres, contener al menos una letra mayúscula, una minúscula, un número y un carácter especial, no deberá ser compartida con ningún otro colaborador.
- En caso de bloqueo u olvido de la contraseña y no poder reestablecerla, deberá enviar correo electrónico al Departamento de Sistemas quien indicará lo conducente.

Consideraciones de contraseñas para servidores:

- Rotación programada de contraseñas.
- Evitar incluir palabras comunes, nombres o información personal.
- No reutilizar contraseñas en varios sistemas.
- Utilizar frases de paso que sean fáciles de recordar, pero difíciles de adivinar (ejemplo una frase modificada con símbolos y números).