POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. Introducción

La seguridad de la información es un aspecto crítico en la protección de los datos, activos digitales y la privacidad de los usuarios en la Coordinación Estatal en la Ciudad de México IMSS-BIENESTAR (CECDMX), es fundamental para mantener la confidencialidad, integridad y disponibilidad de la información.

Esta política tiene como objetivo establecer las normas y procedimientos que guiarán la seguridad de la información dentro de la CECDMX.

2. Objetivos

Proteger la confidencialidad, integridad y disponibilidad de la información.
Prevenir el acceso no autorizado a los sistemas y datos.
Establecer mecanismos de control y auditoría para garantizar el cumplimiento de las políticas de seguridad.
Fomentar la cultura de la seguridad de la información entre todos los empleados.

3. Alcance

Esta política aplica a todos los empleados, contratistas, proveedores y terceros que accedan, gestionen o procesen la información y los sistemas de la CECDMX, incluyendo los datos almacenados en dispositivos electrónicos, redes y servicios en la nube.

4. Definiciones

- **Confidencialidad**: La propiedad de la información que garantiza que solo personas autorizadas puedan acceder a ella.
- **Integridad**: La propiedad que garantiza que la información no será alterada de forma no autorizada.
- **Disponibilidad**: La propiedad de la información que asegura que estará accesible cuando sea necesario.

- **Amenaza**: Cualquier circunstancia o evento que pueda comprometer la seguridad de la información.
- **Vulnerabilidad**: Una debilidad en un sistema que puede ser explotada por una amenaza.

5. Políticas Generales de Seguridad

5.1. Gestión de Accesos

- Para poder llevar el seguimiento de los accesos a los sistemas de información de la CECDMX será necesario que el Departamento de Personal mantenga informado al Departamento de Tecnologías de la Información de las altas y bajas que se lleven a cabo tanto en el personal de estructura como el de apoyo, para el alta y baja de usuarios de accesos.
- El acceso a la información y a los sistemas debe estar limitado a personal autorizado por parte de las áreas resguardantes de los sistemas, que necesite dicha información para cumplir con sus funciones laborales.
- Todo el personal de la CECDMX debe contar con credenciales únicas (nombre de usuario y contraseña), para los sistemas institucionales.
- El acceso a todos los sistemas institucionales debe ser gestionado mediante controles de autenticación (como contraseñas, autenticación multifactor).
- Las contraseñas de los sistemas de la CECDMX, deben cumplir con los siguientes requisitos: longitud mínima de 8 caracteres, inclusión de mayúsculas, minúsculas, números y caracteres especiales.
- Los accesos de administrador a los sistemas deben ser auditados y actualizados regularmente.

5.2. Control de Uso de Dispositivos

- El uso de dispositivos personales para almacenar datos de la organización deberá de ser a únicamente como medio de respaldo, teniendo en todo momento disponible la información de la CECDMX en el equipo institucional para la salvaguarda de la misma.

- Los dispositivos móviles deben ser protegidos con contraseñas y, cuando sea posible, con cifrado de datos.
- En caso de contar con equipo móvil proporcionado por la CECDMX se deberá implementar políticas de "borrado remoto" para dispositivos móviles en caso de pérdida o robo.

5.3. Protección de Datos

- Todos los datos sensibles deben ser cifrados tanto en tránsito como en reposo.
- Se debe realizar una copia de seguridad periódica de los datos críticos y asegurarse de que estén almacenadas en un entorno seguro.

5.5. Gestión de Vulnerabilidades

- Todos los sistemas operativos y desarrollos deberán ser revisados y actualizados con regularidad, incluyendo parches de seguridad y actualizaciones de software.
- El área responsable de la seguridad de la información podrá llevar a cabo escaneos periódicos de vulnerabilidades y pruebas de penetración para identificar y mitigar riesgos, en equipos de cómputo y red institucional.
- Las vulnerabilidades identificadas deben ser tratadas de acuerdo a su nivel de criticidad y los riesgos asociados.

5.6. Gestión de Incidentes de Seguridad

- Todos los incidentes de seguridad, tales como violaciones de datos o accesos no autorizados, deben ser reportados inmediatamente al Departamento de Tecnologías de la Información.
- Debe existir un protocolo de respuesta ante incidentes que incluya la contención, mitigación, análisis y recuperación.
- Se debe mantener un registro detallado de todos los incidentes de seguridad para su análisis posterior.

5.7. Formación y Concientización en Seguridad

- Todo el personal de la CECDMX deberá de recibir formación regular sobre buenas prácticas de seguridad de la información.
- Se fomentará la cultura de seguridad a través de campañas de concientización periódicas.
- Los empleados deberán recibir formación específica sobre el manejo seguro de información confidencial y sobre cómo identificar amenazas como el phishing, ramsomware, etc...

6. Procedimientos de Auditoría y Monitoreo

- Todos los sistemas y redes deben ser monitoreados para detectar actividades sospechosas.
- Los accesos a los sistemas deben ser auditados regularmente, y los registros de acceso deben almacenarse de manera segura durante al menos un año.
- Las auditorías internas y externas deben llevarse a cabo con el fin de asegurar que las políticas y controles de seguridad se estén aplicando correctamente.

7. Excepciones

Cualquier solicitud para una excepción a estas políticas debe ser aprobada por el Departamento de Tecnologías de la Información en coordinación con la jefatura de servicio que haga la solicitud., y se deberán documentar los riesgos asociados con la excepción.

8. Revisión y Actualización

- Esta política debe ser revisada y actualizada periódicamente, al menos una vez al año, para adaptarse a los cambios tecnológicos, los riesgos emergentes y las actualizaciones normativas.
- Cualquier cambio en la política será comunicado a todos los usuarios para su conocimiento y cumplimiento.

9. Conclusión

La seguridad de la información es un proceso continuo que requiere la participación de todos los miembros de la organización. Estas políticas son fundamentales para proteger la información y los activos de la organización, y deben ser seguidas rigurosamente por todos los empleados, contratistas y socios comerciales.

Autorizó
DR. JESÚS ORTÍZ RAMÍREZ
TITULAR DE LA COORDINACIÓN ESTATAL EN LA CIUDAD DE MÉXICO IMSS- BIENESTAR

Elaboró
MTRO. HÉCTOR EZEQUIEL ZURITA RODRÍGUEZ.
TITULAR DEL DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN

Revisó
LIC. JESUS ANTONIO GARRIDO ORTIGOSA.
TITULAR DE LA JEFATURA DE SERVICIOS ADMINISTRATIVOS Y FINANZAS