Ciudad de México a 27 de marzo de 2024

COMUNICADO

AL PERSONAL DE MANDO, DIRECTIVO, DOCENTE, DE APOYO Y ASISTENCIA A LA EDUCACIÓN ADSCRITOS A LA AUTORIDAD EDUCATIVA FEDERAL EN LA CIUDAD DE MÉXICO

En apego al Marco de Gestión de Seguridad de la Información (MGSI), que indica los objetivos institucionales de TIC y la Política General de Seguridad de la Información (PGSI), donde su principal objetivo es fortalecer los niveles de confidencialidad, integridad y disponibilidad de la información generada, recibida, procesada, almacenada y compartida por la AEFCM a través de sus sistemas y aplicaciones, bases de datos, capacitaciones, personal e infraestructura de servicios y comunicaciones se comparte el **"Decálogo de Ciberseguridad para usuarios"** emitido por la Coordinación de Estrategia Digital nacional.

Decálogo de Ciberseguridad

En dispositivos

- No modifiques la instalación por default.
- No instales aplicaciones no autorizadas.
- Establece una clave de acceso segura y activa el bloqueo automático.

Navegación

- Evita acceder a páginas web no confiables o sin que tengan cifrado (https).
- No des clic en enlaces sospechosos o que vengan dentro de un correo que no tengas la certeza de su origen.
- Recuerda que la suplantación de empresas de compra en línea o bancarias está siendo usada para fraudes. Verifica la autenticidad de la página por algún medio diferente a internet.

Antimalware

- Utiliza un antimalware para revisar correos electrónicos, dispositivos de almacenamiento como memorias USB y cualquier archivo que vayas a usar en tus dispositivos.

Correo electrónico

- Elimina todo correo sospechoso o que contenga archivos que no hayas solicitado.
- Evita correos en cadena
- Antes de descargar archivos adjuntos, verifica la extensión y comprueba que presenten rasgos sospechosos.

Fugas de Información

- No facilites información sensible si no estás seguro de quién es el receptor de esta.
- Destruye la información sensible en formato papel. No la tires a la basura.
- No mantengas conversaciones confidenciales en lugares donde puedan ser oídas por terceros.

Protección de la Información

- Realiza copias de seguridad de aquella información sensible que solo esté alojada en tus dispositivos.

Equipo de trabajo

- Asegúrate que tu equipo de trabajo tenga instalado y actualizado un software de antimalware y las aplicaciones tengan todos los parches de seguridad al día.
- Realiza copias de seguridad de manera periódica para evitar que la información se pierda, ya sea por accidente, por pérdida del equipo o por infecciones de malware.
- No conectes dispositivos USB no confiables.

Uso de la nube

- Utiliza la capacidad de almacenamiento en la nube de la institución para guardar información y evitar almacenarla en dispositivos USB.

Cuidado de credenciales

- No compartas tus credenciales (usuario y password)
- No apuntes tus credenciales en lugares visibles y preferentemente apréndetelos.

Seguridad Activa

- Si detectas cualquier actividad sospechosa o un funcionamiento anómalo de tu equipo de trabajo o correo electrónico, da aviso al departamento de Soporte Técnico.

El Decálogo se encuentra publicado en el sitio:

https://wikiguias.atencion.gob.mx/es/seguridad-de-la-informacion/decalogoCiberseguridad

ATENTAMENTE

LA COORDINACIÓN GENERAL DE RECURSOS HUMANOS
DE LA AUTORIDAD EDUCATIVA FEDERAL EN LA CIUDAD DE MÉXICO