"2024, Bicentenario de la Integración de Oaxaca a la República Mexicana"

DEPENDENCIA: SECRETARÍA DE FINANZAS
SECCIÓN: DIRECCIÓN GENERAL DE TECNOLOGÍAS E INNOVACIÓN DIGITAL
CIRCULAR NÚMERO: SF/DGTID/0039/2024
ASUNTO: SE INFORMA SOBRE POLÍTICAS DE CIBERSEGURIDAD.

Tlalixtac de Cabrera, Oaxaca, a 12 de agosto de 2024

C. TITULARES DE LAS DEPENDENCIAS Y ENTIDADES DE LA ADMINISTRACIÓN PÚBLICA ESTATAL.
P R E S E N T E.

En el ejercicio de las atribuciones y facultades conferidas en el Artículo 5, fracciones I, VI, XI, y en el Artículo 7, fracciones, X, XI, VIII, XIV, XV del Decreto de Creación de la Dirección General de Tecnologías e Innovación Digital; y con el objetivo de **mitigar los riesgos** relacionados a **la ciberseguridad en portales web y sistemas informáticos** desarrollados por las Dependencias y Entidades de la Administración Pública Estatal **a través de proveedores de servicio o con recursos propios,** le informo sobre las políticas de ciberseguridad que debe considerar y poner en práctica a la brevedad posible en sistemas y portales a desarrollar o que ya se encuentren implementados:

1. **Pruebas de seguridad y análisis de vulnerabilidades**: Realizar pruebas regulares de penetración y pruebas de vulnerabilidad de los sistemas, portales y plataformas web que no se encuentran alojados en los servidores administrados por la DGTID, con el objetivo de identificar y solventar las vulnerabilidades halladas antes de que suceda un ataque cibernético.
2. **Actualizaciones constantes;** Asegurar que todos los Softwares estén actualizados con las últimas correcciones de seguridad.
3. **Contraseñas seguras;** Utiliza contraseñas robustas y cámbialas periódicamente.
4. **Acceso controlado;** Limita el acceso a la información sensible sólo a personal autorizado.
5. **Principio de mínimo privilegio**: Asignar los mínimos privilegios necesarios a los usuarios y procesos para reducir el impacto de posibles compromisos de seguridad.
6. **Respaldos Regulares;** Realiza copias de seguridad frecuentes para proteger tus datos en caso de incidentes.
7. **Monitoreo Continuo:** Supervisa activamente la red en busca de posibles amenazas o intrusiones.
8. **Planes de continuidad y recuperación;** Elabora planes de continuidad y recuperación ante desastres, de tal manera que puedas garantizar la continuidad de los servicios y recuperación de información ante cualquier eventualidad.
9. **Educación y concienciación**: Capacitar al personal en prácticas de seguridad informática y concientizar sobre las amenazas cibernéticas y cómo mitigarlas.
10. **Conexiones seguras;** Para acceder a datos personales, información sensible o confidencial desde otros lugares a través de Internet o redes públicas, se recomienda usar una conexión segura a través de una Red Privada Virtual (VPN).
11. **Tecnologías de desarrollo seguras;** Utilizar tecnologías de desarrollo en sus versiones más recientes y estables. Debe evitar el uso de versiones beta, tanto en lenguajes como en librerías, bibliotecas, extensiones, frameworks o cualquier otra herramienta que se utilice.

"2024, Bicentenario de la Integración de Oaxaca a la República Mexicana"

DEPENDENCIA: SECRETARÍA DE FINANZAS
SECCIÓN: DIRECCIÓN GENERAL DE TECNOLOGÍAS E INNOVACIÓN DIGITAL
CIRCULAR NÚMERO: SF/DGTID/0039/2024
ASUNTO: SE INFORMA SOBRE POLÍTICAS DE CIBERSEGURIDAD.

12. **Seguridad durante el desarrollo**: Integrar la seguridad desde la fase inicial del desarrollo de sistemas, considerando aspectos como la autenticación, autorización, y control de acceso desde el diseño del proyecto.
13. **Manejo de entrada de datos maliciosos**; Durante el desarrollo de sistemas y portales web deberá realizar validaciones del lado del cliente y del lado de servidor para reducir la posibilidad de fallos o acciones no deseadas. Además de verificar que todas las consultas realizadas a las Bases de Datos estén protegidas por la utilización de declaraciones preparadas o parametrizadas, para no ser susceptibles a inyecciones SQL.

Es importante mencionar que, considerar las políticas citadas anteriormente, además de la implementación de buenas prácticas de seguridad de la información al interior de su Dependencia o Entidad, disminuirá los riesgos de ataques cibernéticos que pueden provocar, entre otras cosas; **pérdida total de información, robo de información sensible y confidencial, interrupción de los servicios críticos** de la Dependencia o Entidad, así como **dañar la reputación y confianza ciudadana** hacia el Gobierno Estatal.

Es por ello que, en un plazo de 15 días hábiles, a partir de la recepción de esta circular, deberá notificar a través un oficio, la situación actual de su Dependencia o Entidad de acuerdo con las políticas de ciberseguridad citadas anteriormente, especificando;

1. Las políticas de ciberseguridad que se encuentran implementadas al interior de su Dependencia o Entidad y las que no han sido consideradas hasta el momento.
2. Plan de acción, señalando acciones a corto y mediano plazo para la implementación de todas las políticas de ciberseguridad señaladas en esta circular.

Sin otro particular por el momento, aprovecho la ocasión para enviarle un cordial saludo.

ATENTAMENTE,
SUFRAGIO EFECTIVO. NO REELECCIÓN.
"EL RESPETO AL DERECHO AJENO ES LA PAZ".
DIRECTOR GENERAL DE TECNOLOGÍAS E INNOVACIÓN DIGITAL.

Dirección General de Tecnologías e Innovación Digital
Gobierno del Estado de Oaxaca

M.T.I. MOISÉS JUÁREZ RODRÍGUEZ.
C.c.p.
Expediente/Minutario
MJR/rgg/bgv/

A efecto de mantener organizados los documentos para su fácil localización, se solicita que de dar respuesta al presente comunicado se cite el número de expediente y oficio aquí consignado. Lo anterior con fundamento en los artículos 6 y 7 de la Ley de Archivos del Estado de Oaxaca.