



DESPACHO DE LA SECRETARIA

Chihuahua, Chihuahua. 04 de agosto de 2023

Oficio: SFP/441/2023

Asunto: Se emiten recomendaciones

CC. Titulares de las dependencias y entidades de la Administración Pública del Estado.

Presentes.-

La Secretaría de la Función Pública es la dependencia encargada del control interno de la administración pública estatal, con el objetivo fundamental de que las dependencias y entidades puedan cumplir con sus objetivos y metas institucionales, en forma alineada a las directrices dictadas por la Gobernadora del Estado en el Plan Estatal de Desarrollo 2022-2027 (y los programas que de él derivan), el Plan Estatal de Seguridad Pública y el Plan Estatal Hídrico.

En esa virtud, las Disposiciones en Materia de Control Interno, publicadas en el Periódico Oficial del Estado de fecha 25 de junio de 2021, prevén que todas las instituciones del Gobierno del Estado deben contar con un Sistema de Control Interno Institucional (SCII), el cual comprende una metodología de administración de riesgos.

Entre los riesgos que las Disposiciones contemplan para ser considerados en los respectivos Programas de Trabajo de Administración de Riesgos (PTAR), están los riesgos de tecnología, los que “están relacionados con la capacidad tecnológica de la entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de su misión”. Las propias Disposiciones definen a las Tecnologías de la Información y Comunicaciones (TIC’s) como el conjunto de herramientas relacionadas con la transmisión, procesamiento y almacenamiento digitalizado de la información.

También son relevantes los riesgos de reputación que “están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la dependencia o entidad”. Usualmente, cuando se materializa un riesgo de tecnología, al mismo tiempo se materializa el riesgo de reputación, dado que la percepción pública hacia la institución afectada por la materialización del riesgo de tecnología se ve disminuida, mermada o dañada.

Las propias Disposiciones señalan que todas las dependencias y entidades del Gobierno del Estado deben tener su Plan Institucional de TIC’s, y entre las cuestiones que estos planes deben abordar está la relativa a “las dificultades o situaciones que causan problemas para su cumplimiento y las acciones de solución emprendidas”. En ese sentido, es un hecho de conocimiento público el problema que han afrontado en tiempos recientes tanto instituciones del Gobierno del Estado como algunos Municipios.

*“2023, Centenario de la muerte del General Francisco Villa”
“2023, Cien años del Rotarismo en Chihuahua”*



SECRETARÍA
DE LA FUNCIÓN
PÚBLICA

Edificio Lic. Óscar Flores, Calle Victoria No. 310, Col. Centro, C.P. 31000, Chihuahua, Chih.
Teléfono (614) 439-7702
www.chihuahua.gob.mx

Por lo anterior y con fundamento en el artículo 34, fracción XXV, de la Ley Orgánica del Poder Ejecutivo del Estado de Chihuahua, esta Secretaría recomienda las siguientes medidas de prevención contra la materialización de riesgos tecnológicos:

MEDIDAS DE PREVENCIÓN

Derivado al incidente tecnológico acontecido recientemente en una institución del Gobierno del Estado, es conveniente realizar medidas de prevención para mitigar su propagación o un nuevo ataque cibernético, malware, en específico un Ransomware, dentro del Gobierno del Estado de Chihuahua. Es fundamental proteger la infraestructura, sistemas y datos contra este tipo de ataques en cada una de las áreas correspondientes para mitigar y colaborar con las acciones correctivas que se requieren en este momento en el Gobierno.

Mantener el software actualizado: Asegurarse de tener todas las aplicaciones y sistemas operativos en las últimas versiones y aplicar regularmente las actualizaciones de seguridad.

Instalar un antivirus y antimalware: Utilizar una solución de seguridad confiable que incluya protección contra ransomware y mantenerla actualizada.

Habilitar el firewall: Asegurarse de que el firewall esté activado tanto en las computadoras como en su red para bloquear el tráfico no autorizado.

Capacitar y sensibilizar al personal: Capacitar a los usuarios sobre los riesgos de ransomware, de cómo identificar correos electrónicos y enlaces sospechosos y qué hacer en caso de una posible infección.

Respaldos regulares: Realizar copias de seguridad regulares de los datos y guárdalos en ubicaciones seguras, preferiblemente fuera de la red principal.

Restricción de privilegios a usuario: Limitar los permisos de acceso a archivos y carpetas solo a los empleados que realmente los necesiten para realizar sus tareas.

Evitar sitios web y descargas sospechosas: Evitar hacer clic en enlaces desconocidos o descargar archivos en sitios web no confiables.

Configura filtros de correo electrónico: Utilizar filtros para bloquear correos electrónicos no solicitados o sospechosos que podrían contener enlaces maliciosos o archivos adjuntos infectados.

Utilizar listas blancas: Configurar sus sistemas para que solo se ejecuten aplicaciones y procesos autorizados y conocidos en conjunto con la CPD.

*"2023, Centenario de la muerte del General Francisco Villa"
"2023, Cien años del Rotarismo en Chihuahua"*



SECRETARÍA
DE LA FUNCIÓN
PÚBLICA

Edificio Lic. Óscar Flores, Calle Victoria No. 310, Col. Centro, C.P. 31000, Chihuahua, Chih.
Teléfono (614) 439-7702
www.chihuahua.gob.mx

9

Monitorea la red: Implementar sistemas de monitoreo para detectar actividades inusuales y comportamientos sospechosos en la red.

Copia de seguridad de la configuración del sistema: Realizar copias de seguridad de la configuración de tu sistema y dispositivos para poder restaurarlos rápidamente en caso de un ataque.

Ejecución aislada: Considera utilizar entornos aislados o máquinas virtuales para ejecutar aplicaciones sospechosas o no confiables.

Bloqueo de macros: Configura los programas de oficina para bloquear las macros en documentos adjuntos de correo electrónico.

Limita el acceso a la red: Implementa medidas de seguridad para restringir el acceso a la red desde dispositivos no autorizados o dispositivos personales.

Reconocemos que ninguna medida de prevención es infalible, pero la combinación de múltiples acciones de seguridad y una cultura de concienciación en ciberseguridad pueden ayudar a reducir significativamente el riesgo de infección por algún ataque cibernético, malware como puede ser el ransomware.

Sin otro particular por el momento, reciba un cordial saludo.

ATENTAMENTE



SECRETARÍA DE LA
FUNCIÓN PÚBLICA


LIC. MARÍA DE LOS ÁNGELES ÁLVAREZ HURTADO
SECRETARIA DE LA FUNCIÓN PÚBLICA

vhgs



SECRETARÍA
DE LA FUNCIÓN
PÚBLICA

"2023, Centenario de la muerte del General Francisco Villa"
"2023, Cien años del Rotarismo en Chihuahua"
Edificio Lic. Óscar Flores, Calle Victoria No. 310, Col. Centro, C.P. 31000, Chihuahua, Chih.
Teléfono (614) 439-7702
www.chihuahua.gob.mx

