



Lineamientos internos para la ciberseguridad, desarrollo y uso de las tecnologías en la Secretaría de Hacienda

2023-2028

Coordinación de Tecnologías de la Información
Actualización: Julio de 2025
Versión 2025.2.4

Contenido:

- a) Programa de Ciberseguridad 3
- b) Políticas de seguridad, uso y desarrollo de las TIC's 13

Presentación

En el marco del Plan Estatal de Desarrollo 2022 – 2028, con el propósito fundamental de consolidar un sistema de gobierno digital, **seguro, eficiente y transparente** la Secretaría de Hacienda mantiene una estrategia de transformación digital, interoperabilidad, ciberseguridad y mejora continua de sus procesos sustantivos.

La encuesta nacional sobre disponibilidad y uso de tecnologías de la información en los hogares (ENDUTIH) realizada por el INEGI, estimó que en México en 2024 había **100.2 millones de personas usuarias de internet**, lo que representa el 83.1 % de la población de seis años o más, siendo esta cifra 1.9 puntos porcentuales mayor respecto a la de 2023. (81.2 %).

El incremento de personas usuarios de internet y el uso de nuevas tecnologías en las organizaciones, hoy representa **grandes retos en materia de ciberseguridad, desarrollo y aprovechamiento de las nuevas tecnologías de la información.**

En este sentido el presente documento es una **guía de sensibilización de los riesgos actuales, integra el uso de buenas practicas a nivel internacional y establece políticas internas de aplicación general** para los usuarios de las plataformas digitales que administra esta Secretaría; Esta diseñado para evolucionar de acuerdo a la normatividad que dicte el gobierno federal y estatal, al uso de nuevas tecnologías y a la dinámica social en el corto, mediano y largo plazo.

Su finalidad principal es promover la **responsabilidad y compromiso** entre los servidores públicos para el uso adecuado de las tecnologías con las que se cuenta actualmente, fortaleciendo la cultura organizacional en materia de control interno y protección de la información; Asegurando un nivel adecuado de prevención, control y recuperación frente a los riesgos, amenazas y vulnerabilidades cibernéticas.

Programa de Ciberseguridad

Programa de Ciberseguridad

El programa de ciberseguridad integra un conjunto de planes, políticas, acciones estratégicas y medidas diseñadas para identificar y proteger los sistemas informáticos, redes, datos y usuarios frente a amenazas cibernéticas aplicables a la Secretaría de Hacienda.

Objetivo general.

Fortalecer las acciones en materia de ciberseguridad aplicables en la Secretaría de Hacienda, de forma que se garantice un nivel adecuado de prevención y resiliencia que permita a Contribuyentes y Entes Públicos el uso de las TIC's de Hacienda de manera segura y eficiente.

Para el logro del objetivo general se plantean 3 acciones estratégicas: prevención, control y recuperación, en las cuales se agrupan los principios establecidos en la guía CSF 1.1 del Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología NIST, estándar internacional que brinda una visión integral del ciclo de vida para gestionar el riesgo de ciberseguridad a lo largo del tiempo.

Acciones estratégicas.

- **Prevención (Identificar, Detectar).**- Elaborar diagnósticos de capacidades tecnológicas y de riesgos, en los que se identifiquen posibles vulnerabilidades a la infraestructura tecnológica de la Secretaría, estableciendo protocolos de actuación y lineamientos que ayuden a sensibilizar a los servidores públicos.
- **Control (Proteger):** Fortalecer los mecanismos de control interno, protección y monitoreo para mitigar los riesgos cibernéticos de los activos de información, sistemas informáticos e infraestructura crítica, protegiendo prioritariamente la confidencialidad, integridad y disponibilidad de datos y sistemas de información institucionales.
- **Recuperación (responder, recuperar):** Ampliar las capacidades de resiliencia del Centros de Datos y actualizar los protocolos para limitar las pérdidas e inaccessibilidad a los activos de información; Actualizando planes de recuperación de la infraestructura crítica y de respaldos de los sistemas de información institucionales que se vean afectados a partir de un incidente de seguridad.

Riesgos Cibernéticos

Sensibilizar a los Servidores Públicos es fundamental, por lo que es importante definir que es un riesgo cibernético, su impacto y tipos de riesgos actuales.

De acuerdo con el Instituto Nacional de Estándares y Tecnología (NIST), se define el riesgo cibernético como la posibilidad de pérdida financiera, interrupción operativa o daño, debido a la falla de las tecnologías digitales empleadas para funciones informativas y/o operativas introducidas a un sistema por medios electrónicos sin acceso autorizado, para el uso, divulgación, interrupción, modificación o destrucción de los sistemas. Los principales riesgos cibernéticos de acuerdo al glosario de términos utilizados por el NIST son:

1. Malware: Término simplificado para denotar “malicious code” y consiste en software que realiza procesos no autorizados o de robo de datos a un sistema de información. Dentro de esta categoría se encuentran principalmente los siguientes tipos:

- **Virus:** Sección oculta y auto replicante de software informático, que se propaga al infectar (es decir, al insertar una copia de sí mismo en otro programa y convertirse en parte de él). Un virus no puede correr solo; requiere que su programa huésped se ejecute para activarlo.
- **Spyware:** Software que se instala de forma secreta en un sistema de información para recopilar datos sobre individuos u organizaciones sin su conocimiento.
- **Adware:** Software que reproduce o descarga automáticamente material publicitario a una computadora después de instalar el software o mientras se utiliza la aplicación. El programa malicioso está diseñado para mostrar publicidad no deseada en la computadora de la víctima sin su permiso, los pop-ups o anuncios son incontrolables y tienden a comportarse de forma errática, por lo general aparecen muchas veces en la pantalla.
- **Trojan Horse:** Programa de computadora que tiene una función oculta y potencialmente maliciosa que evade los mecanismos de seguridad, a veces explotando autorizaciones legítimas de una entidad que invoca el programa, recopilando información sin ninguna autorización.
- **Ransomware:** Es un virus que impide que el usuario acceda a los archivos o programas y para su eliminación se exige pagar un “rescate” a través de ciertos métodos de pago en línea.

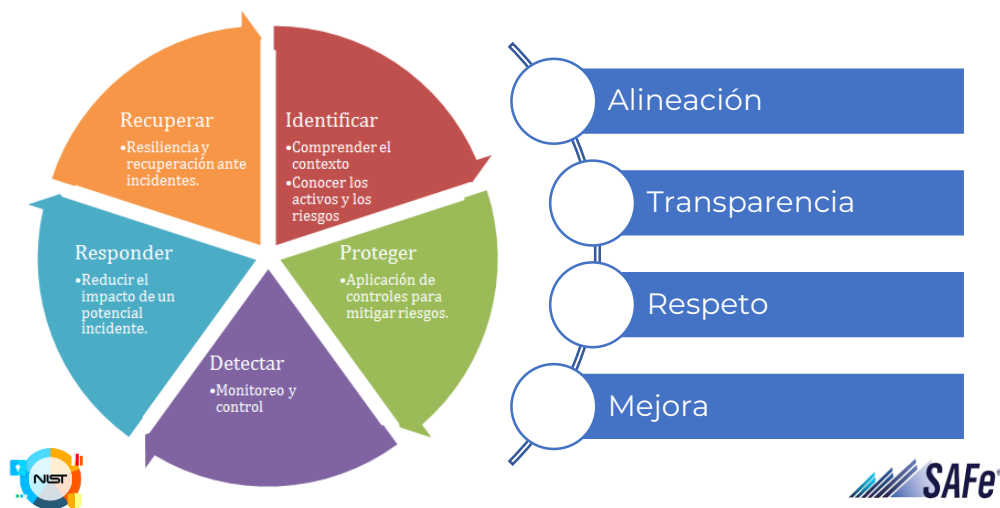
Riesgo Cibernético

- 2. Phishing:** Técnica para intentar adquirir datos confidenciales, como números de cuentas bancarias, a través de una solicitud fraudulenta en un correo electrónico o en un sitio web, en la que el perpetrador se hace pasar por un negocio o persona legítima.
- 3. Man-in-the-middle attack (MitM):** Ataque MitM es cuando un atacante altera la comunicación entre dos usuarios, haciéndose pasar por ambas víctimas para manipularlos y obtener acceso a sus datos. Los usuarios no son conscientes de que realmente se están comunicando con un atacante y no entre ellos.
- 4. Distributed denial-of-service attack (DDoS):** Ataque que inunda sistemas, servidores o redes. con tráfico para agotar los recursos y el ancho de banda. Como resultado, el sistema no puede cumplir con solicitudes legítimas. Los atacantes también pueden usar múltiples dispositivos comprometidos para lanzar este ataque. Esto se conoce como un ataque de denegación de servicio distribuido.
- 5. SQL injection:** Ocurre cuando un atacante inserta código malicioso en un servidor que utiliza SQL (Structured Query Language). Sólo tienen éxito cuando existe una vulnerabilidad de seguridad en el software de una aplicación. Los ataques de SQL exitosos obligan a un servidor a proporcionar acceso o modificar datos.
- 6. Zero-day attack:** Ataque que explota vulnerabilidades de hardware, o software por el uso de software obsoleto (no parchado). Un ataque de día cero puede ocurrir cuando una vulnerabilidad se hace pública antes de que el desarrollador haya implementado un parche o una solución.
- 7. C&C Callbacks:** Indica que es probable que su sistema haya sido comprometido por un malware. Significa que su sistema intenta comunicarse con un servidor de comando y control (C&C), que los atacantes utilizan para controlar sistemas comprometidos y extraer datos.

Buenas practicas

La ciberseguridad, desarrollo y uso de TIC's no solo implica el uso de herramientas de seguridad informática, como firewalls, software antivirus, autenticación, cifrado de datos, sino también implementar un conjunto de políticas y buenas practicas, diseñadas para salvaguardar la confidencialidad, integridad y disponibilidad de los datos y sistemas de información.

Bajo esta visión, las acciones de fortalecimiento de ciberseguridad y en la Secretaria de Hacienda, se ejecutan bajo **el marco metodológico ágil SAFe** que define el conjunto de acciones de planeación y despliegue del **Programa de Ciberseguridad** incluido en el Plan Institucional de Tecnologías, aprobado por la titular de la Secretaria de Hacienda y **el marco internacional de ciberseguridad NIST CSF 1.1** para gestionar el riesgo de ciberseguridad a lo largo del tiempo, asegurando eficiencia, alineación estratégica, y cumplimiento normativo en los proyectos tecnológicos que se implementen.



Buenas Practicas:

- **Guía del Marco de Ciberseguridad del NIST.**

El uso de buenas practicas como la guía NIST, proporciona la **orientación a los encargados del Programa de Ciberseguridad** para mejorar la gestión de riesgos mediante la utilización de un marco internacional de ciberseguridad.

El marco está organizado por cinco funciones clave: identificar, proteger, detectar, responder y recuperar. Estos cinco términos cuando se consideran en conjunto, brindan una visión integral del ciclo de vida para gestionar el riesgo de ciberseguridad a lo largo del tiempo.

Identificar



IDENTIFY

Develop an organizational understanding to manage cybersecurity risk to: systems, assets, data, and capabilities.

- **Identifique los procesos y activos empresariales críticos** : ¿Cuáles son las actividades de su empresa que absolutamente deben continuar para ser viables? Por ejemplo, esto podría consistir en mantener un sitio web para recuperar pagos, proteger la información del cliente/paciente de forma segura o garantizar que la información que recopila su empresa siga siendo accesible y precisa.
- **Flujos de información de documentos** : es importante no solo comprender qué tipo de información recopila y utiliza su empresa, sino también dónde se encuentran los datos y cómo se utilizan, especialmente dónde se contratan contratos y socios externos.
- **Mantenga el inventario de hardware y software** : es importante comprender las computadoras y el software de su empresa porque con frecuencia son puntos de entrada de actores maliciosos. Este inventario podría ser tan simple como una hoja de cálculo.
- **Establezca políticas de ciberseguridad que incluyan roles y responsabilidades** : estas políticas y procedimientos deben describir claramente sus expectativas sobre cómo las actividades de ciberseguridad protegerán su información y sus sistemas, y cómo respaldan los procesos empresariales críticos. Las políticas de ciberseguridad deben integrarse con otras consideraciones de riesgo empresarial (por ejemplo, financiero, reputacional).
- **Identifique amenazas, vulnerabilidades y riesgos para los activos** : asegúrese de que se establezcan y gestionen procesos de gestión de riesgos para garantizar que las amenazas internas y externas se identifiquen, evalúen y documenten en registros de riesgos. Asegúrese de que las respuestas a los riesgos se identifiquen, prioricen, ejecuten y se supervisen los resultados.

Buenas Practicas:

• Guía del Marco de Ciberseguridad del NIST.

Proteger

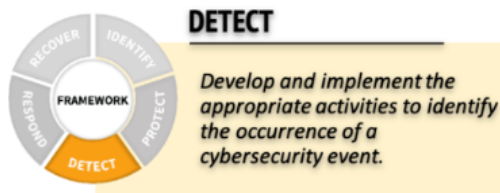


- **Administre el acceso a activos e información** : cree cuentas únicas para cada empleado y asegúrese de que los usuarios solo tengan acceso a la información, las computadoras y las aplicaciones que necesitan para sus trabajos. Autenticar a los usuarios (por ejemplo, contraseñas, técnicas multifactor) antes de que se les conceda acceso a información, computadoras y aplicaciones. Administre y realice un seguimiento estricto del acceso físico a los dispositivos.
- **Proteja los datos confidenciales** : si su empresa almacena o transmite datos confidenciales, asegúrese de que estos datos estén protegidos mediante cifrado tanto mientras se almacenan en las computadoras como cuando se transmiten a otras partes. Considere utilizar una verificación de integridad para garantizar que solo se hayan realizado cambios aprobados en los datos. Elimine y/o destruya datos de forma segura cuando ya no sean necesarios o necesarios para fines de cumplimiento.
- **Realice copias de seguridad periódicas** : muchos sistemas operativos tienen capacidades de copia de seguridad integradas; También hay disponibles software y soluciones en la nube que pueden automatizar el proceso de copia de seguridad. Una buena práctica es mantener fuera de línea un conjunto de datos del que se realiza una copia de seguridad frecuente para protegerlo contra el ransomware.
- **Proteja sus dispositivos** : considere instalar firewalls basados en host y otras protecciones, como productos de seguridad para terminales. Aplique configuraciones uniformes a los dispositivos y controle los cambios en las configuraciones de los dispositivos. Desactive los servicios o funciones del dispositivo que no sean necesarios para respaldar las funciones de la misión. Asegúrese de que exista una política y de que los dispositivos se eliminen de forma segura.
- **Administre las vulnerabilidades de los dispositivos** : actualice periódicamente tanto el sistema operativo como las aplicaciones instaladas en sus computadoras y otros dispositivos para protegerlos de ataques. Si es posible, habilite las actualizaciones automáticas. Considere el uso de herramientas de software para escanear dispositivos en busca de vulnerabilidades adicionales; remediar vulnerabilidades con alta probabilidad y/o impacto.
- **Capacitar a los usuarios** : capacitar y volver a capacitar periódicamente a todos los usuarios para asegurarse de que conozcan las políticas y procedimientos de ciberseguridad empresarial y sus funciones y responsabilidades específicas como condición de empleo.

Buenas Practicas:

- **Guía del Marco de Ciberseguridad del NIST.**

Detectar



- **Probar y actualizar procesos de detección** : desarrollar y probar procesos y procedimientos para detectar entidades y acciones no autorizadas en las redes y en el entorno físico, incluida la actividad del personal. El personal debe ser consciente de sus funciones y responsabilidades en materia de detección y presentación de informes relacionados, tanto dentro de su organización como ante las autoridades legales y de gobierno externas.
- **Mantener y monitorear registros** : los registros son cruciales para identificar anomalías en las computadoras y aplicaciones de su empresa. Estos registros registran eventos como cambios en sistemas o cuentas, así como el inicio de canales de comunicación. Considere el uso de herramientas de software que puedan agregar estos registros y buscar patrones o anomalías en el comportamiento esperado de la red.
- **Conozca los flujos de datos esperados para su empresa** : si sabe qué y cómo se espera que se utilicen los datos para su empresa, es mucho más probable que se dé cuenta cuando sucede lo inesperado, y lo inesperado nunca es bueno cuando se trata de ciberseguridad. Los flujos de datos inesperados pueden incluir información del cliente que se exporta desde una base de datos interna y sale de la red. Si ha contratado trabajo con un proveedor de servicios administrados o en la nube, analice con ellos cómo rastrean los flujos de datos e informan, incluidos los eventos inesperados.
- **Comprenda el impacto de los eventos de ciberseguridad** : si se detecta un evento de ciberseguridad, su empresa debe trabajar rápida y exhaustivamente para comprender la amplitud y profundidad del impacto. Busca ayuda. Comunicar información sobre el evento a las partes interesadas adecuadas le ayudará a mantenerse en buena posición en términos de socios, organismos de supervisión y otros (potencialmente incluidos inversores) y a mejorar las políticas y los procesos.

Guía conceptual del Marco de Ciberseguridad del NIST.

Responder



RESPOND

Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

- **Asegúrese de que los planes de respuesta se prueben :** es aún más importante probar los planes de respuesta para asegurarse de que cada persona conozca sus responsabilidades al ejecutar el plan. Cuanto mejor preparada esté su organización, más efectiva será la respuesta. Esto incluye conocer los requisitos legales de presentación de informes o el intercambio de información requerido.

- **Asegúrese de que los planes de respuesta estén actualizados :** probar el plan (y su ejecución durante un incidente) inevitablemente revelará las mejoras necesarias. Asegúrese de actualizar los planes de respuesta con las lecciones aprendidas.
- **Coordine con las partes interesadas internas y externas :** es importante asegurarse de que los planes de respuesta y las actualizaciones de su empresa incluyan a todas las partes interesadas clave y proveedores de servicios externos. Pueden contribuir a mejoras en la planificación y ejecución.

Recuperar



RECOVER

Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

- **Comunicarse con las partes interesadas internas y externas :** parte de la recuperación depende de una comunicación eficaz. Sus planes de recuperación deben tener en cuenta cuidadosamente qué, cómo y cuándo se compartirá la información con las distintas partes interesadas para que todas las partes interesadas reciban la información que necesitan pero no se comparta información inapropiada.

- **Asegúrese de que los planes de recuperación estén actualizados :** al igual que con los planes de respuesta, la ejecución de pruebas mejorará la conciencia de los empleados y socios y resaltarán las áreas de mejora. Asegúrese de actualizar los planes de recuperación con las lecciones aprendidas.
- **Gestionar las relaciones públicas y la reputación de la empresa :** uno de los aspectos clave de la recuperación es gestionar la reputación de la empresa. Al desarrollar un plan de recuperación, considere cómo gestionará las relaciones públicas para que la información que comparta sea precisa, completa y oportuna, y no reaccionaria.

Programa de Ciberseguridad

De acuerdo al marco metodológico, esta Secretaría cuenta con un programa para el fortalecimiento de la gestión de seguridad de la información y esta incluido en el Plan Institucional de Tecnologías, el cual se reporta trimestralmente en COCODI.

Objetivo

- Fortalecer las acciones de ciberseguridad aplicables a la infraestructura tecnológica, sistemas institucionales de información y datos que resguarda la Secretaría de Hacienda, asegurando que posean un nivel adecuado de prevención, control y recuperación frente a los riesgos, amenazas y vulnerabilidades cibernéticas.

Líneas de Acción

- Prevención.- Elaborar diagnósticos de capacidades tecnológicas y de riesgos, que permitan identificar posibles vulnerabilidades en la infraestructura tecnológica de la Secretaría de Hacienda.
- Control.- Fortalecer los mecanismos de control interno (Lineamientos, Cartas de Confidencialidad, XDR) de los activos de información y sistemas informáticos..
- Recuperación.- Implementar planes DRP para la recuperación de los sistemas de información que se vean afectados a partir de un incidente de seguridad.

Alcances

- Inventario de capacidades e infraestructura tecnológica actualizado.
- Diagnósticos de Ciberseguridad aplicados a los Sistemas de Información Institucionales y riesgos detectados atendidos.
- Lineamientos de Ciberseguridad, y cartas de confidencialidad actualizadas.
- Planes de Respaldo y de Recuperación de Desastres actualizados.
- Cultura de Ciberseguridad fortalecida.

Áreas Responsables

- Enlaces del Subcomité de Tecnologías de la Secretaría de Hacienda.
- Coordinación de Tecnologías de la Información. (Equipo de Ciberseguridad).

Políticas de Seguridad, Uso y Desarrollo de las Tecnologías de la Información.

Políticas de Seguridad, Uso y Desarrollo de las Tecnologías de la Información.

En el ámbito de las atribuciones de la Coordinación de Tecnologías de la Información (CTI), establecidas en el Art. 21 del Reglamento Interior de la Secretaría de Hacienda, Fracciones II,V y X; A los lineamientos establecidos en el Reglamento para el Uso y Aprovechamiento de Tecnologías de Información y Comunicaciones en el Poder Ejecutivo del Estado de Hidalgo y a la Ley Nacional para Eliminar Trámites Burocráticos, se establecen las siguientes **políticas de observancia general para el personal adscrito a esta Secretaría:**

Seguridad de la Información.

- I. Las cuentas de acceso a las plataformas de Hacienda son personales e intransferible, por lo que el titular de la cuenta será el responsable de todas las acciones realizadas con ella.
- II. Queda prohibido el uso cuentas de acceso por personas distintas al usuario asignado, con o sin autorización del responsable.
- III. Los servidores públicos de la Secretaría de Hacienda deberán validar sus datos de contacto y CURP en el buzón digital del usuario, de lo contrario la cuenta será suspendida temporalmente y reactivada solo después de haber cumplido con este medio de control interno.
- IV. Los servidores públicos de la Secretaría Hacienda, con acceso a Sistemas de Información Institucionales, deberán contar con carta compromiso de confidencialidad firmada y validada de forma autógrafa o digitalmente, de lo contrario la cuenta será suspendida temporalmente y reactivada solo después de haber cumplido con este medio de control interno.
- V. Si se detecta que las actividades de una cuenta de usuario pueden comprometer la integridad y seguridad de la información, el acceso a dicha cuenta será suspendida temporalmente y reactivada solo después de haber tomado las medidas necesarias.
- VI. Los equipos de cómputo conectados a la red institucional del Poder Ejecutivo, deben tener instalado un programa antimalware XDR con licencia, cuando así lo requiera el sistema operativo instalado.

Políticas de Seguridad, Uso y Desarrollo de las Tecnologías de la Información.

- VII. Los servidores públicos que opten por no utilizar el programa antimalware institucional, deberán contar con el visto bueno de su jefe inmediato y firmar la carta responsiva solicitada por la Dirección General de Innovación Gubernamental.
- VIII. Si un servidor público detecta una vulnerabilidad en la seguridad de la información o si su equipo esta comprometido por algún tipo de malware debe informarlo inmediatamente a su jefe inmediato y notificarlo a la Coordinación de Tecnologías de la Información.
- IX. El servidor público que tiene asignada una cuenta de Correo Electrónico Institucional, es el único responsable ante cualquier queja o denuncia por el uso inapropiado o por la información transmitida por este medio.
- X. Los activos de información se clasificara de la siguiente forma:
- Restringida.- Información con mayor grado de sensibilidad; su transferencia debe ser autorizado por el propietario de la misma.
 - Confidencial.- Información sensible que solo debe ser divulgada a aquellas usuarios que la necesiten para el cumplimiento de sus funciones.
 - Uso Interno.- Datos generados para facilitar las operaciones diarias: deben ser manejados de manera discreta, pero no requiere de medidas elaboradas de seguridad.
 - General.- Información que es generada específicamente para su divulgación a la población general.
- XI. La transferencia de cualquier activo de información (bases de datos, archivos digitalizados, documentación de sistemas, procedimientos operativos o de recuperación) clasificado como “Restringido o Confidencial” debe asegurar que el destinatario de la información esta autorizado a recibir dicha información y en su caso establecer un acuerdo administrativo de entrega de información.

Políticas de Seguridad, Uso y Desarrollo de las Tecnologías de la Información.

- XII. Los medios de almacenamiento, incluyendo discos duros o memorias, que albergan información clasificada como “Restringida o Confidencial” deben ser ubicados en ambientes cerrados y en su caso protegida con técnicas de encriptación.
- XIII. Se prohíbe al servidor público:
1. Ingresar sin autorización a los sitios o servicios digitales del Poder Ejecutivo mediante la utilización de herramientas intrusivas (hacking) o cualquier otro medio no permitido;
 2. Realizar pruebas de vulnerabilidad sin la autorización correspondiente;
 3. Cargar archivos que contengan malware o cualquier otro software similar que pueda perjudicar el funcionamiento de los equipos de cómputo y comunicaciones digitales del Poder Ejecutivo;
 4. Presentar, almacenar o transmitir información, imágenes, textos que no estén relacionadas a las actividades propias de la función que desempeña;
 5. Enviar correo basura, spam indiscriminado o encadenado, no autorizado o consentido previamente por los destinatarios;
 6. Instalar software que no cuente con licenciamiento vigente ni autorización formal por parte del jefe inmediato superior.

Uso de las Tecnologías de la Información y Comunicaciones.

- XIV. El equipo de cómputo y de comunicaciones, propiedad del Gobierno del Estado, deberá estar asignado y bajo el resguardo de un Servidor Público.
- XV. El servidor público usuario de bienes informáticos es responsable del uso, custodia y protección de los bienes asignados para el desempeño de sus funciones y tiene la obligación de cuidarlo y mantenerlo en buen estado.

Políticas de Seguridad, Uso y Desarrollo de las Tecnologías de la Información.

- XVI. Las solicitudes de soporte técnico a Sistemas de Información Institucionales y mantenimiento preventivo de bienes informáticos de esta Secretaría, se deberán registrar a través de los servicios de Mesa de ayuda OTRS, medio oficial para su seguimiento y atención.
- XVII. El procedimiento de mantenimiento correctivo para los bienes informáticos así como la adquisición e instalación de refacciones, se deberá realizar de acuerdo a lo lineamientos emitidos por la Oficialía Mayor.
- XVIII. El proceso de baja de bienes informáticos se realizaran de acuerdo a los lineamientos emitidos por la Oficialía Mayor.
- XIX. Los servidores públicos deben abstenerse de realizar intercambio o préstamo de bienes informáticos, sin las autorizaciones necesarias y fuera de los procesos establecidos.
- XX. Es responsabilidad del servidor publico realizar el respaldo periódico de la información del equipo que tiene asignado y de su adecuado resguardo.

Desarrollo de las Tecnologías de la Información y Comunicaciones.

- XXI. Para el desarrollo y modernización de los procesos sustantivos de la Secretaría de Hacienda, de forma anual, se elaborará el Plan Institucional de Tecnologías de la Información.
- XXII. Las iniciativas en materia de TIC's a incluir en el Plan Institucional de Tecnologías, se desarrollarán de forma colaborativa con los integrantes del Subcomité de Tecnologías de la Información de esta Secretaría, y deberán estar alineadas a los objetivos establecidos en el Programa Sectorial de Desarrollo de Hacienda.
- XXIII. El desarrollo de iniciativas tecnológicas orientadas a trámites y servicios deberán priorizar los procesos de digitalización que permitan proveer trámites digitales simplificados y con utilidad social, de acuerdo a los principios establecidos en la Ley Nacional para Eliminar Trámites Burocráticos.

Políticas de Seguridad, Uso y Desarrollo de las Tecnologías de la Información.

XXIV. Las Iniciativas se deberán formalizar de acuerdo a los medios de comunicación oficiales, en el caso de iniciativas internas enviando solicitud signada por el titular del Área operativa a la Coordinación de Tecnologías de la Información y tratándose de proyectos externos a través de solicitud oficial dirigida a la titular de la Secretaría de Hacienda.

XXV. Se adoptara el Modelo Nacional para eliminar trámites burocráticos, de forma que faciliten el acceso y obtención de trámites y servicios, conforme al título tercero, capítulo 1 y título cuarto capítulo 1 de la Ley Nacional para Eliminar Trámites Burocráticos.

XXVI. El desarrollo y mantenimiento de Sistemas de Información autorizados en el Plan Institucional de Tecnologías, se ejecutarán bajo el uso de los marcos metodológicos:

- Un marco ágil SAFe para la planeación, seguimiento y entrega de flujos de valor.
- Un marco de ciberseguridad NIST para gestionar el riesgo de ciberseguridad a lo largo del tiempo.

XXVII. Las iniciativas y proyectos tecnológicos estarán registradas para su control en el sistema de Portafolios de Proyectos en la plataforma ehacienda, y su avance se informará de forma trimestral en las sesiones ordinarias de COCODI.

Sanciones

XXVIII. Los servidores públicos que incumplan las disposiciones establecidas en estas políticas, estarán sujetos a las sanciones establecidas por la Ley General de Responsabilidades Administrativas y demás normatividad aplicable, sin perjuicio de las sanciones de índole penal o la responsabilidad civil, en las que pudieran incurrir.

Referencias

- Decreto que contiene el Reglamento Interno de la Secretaría de Hacienda. Reglamentos Internos. 28 de julio de 2023. Periódico Oficial del Estado de Hidalgo TOMO CLV, Alcance 7 núm. 30
- Reglamento para el uso y aprovechamiento de Tecnologías de Información y Comunicaciones en el poder ejecutivo. 15 de febrero de 2021.
https://periodico.hidalgo.gob.mx/?tribe_events=Periodico-Oficial-Ordinario-0-del-15-de-febrero-de-2021
- *DECRETO por el que se expide la Ley Nacional para Eliminar Trámites Burocráticos.* 16 de julio de 2025..
https://dof.gob.mx/nota_detalle.php?codigo=5763166&fecha=16/07/2025#gsc.tab=0
- Marco de Seguridad, National Institute of Standards and Technology. National Institute of Standards and Technology (NIST). 2024. <https://www.nist.gov/cyberframework/csf-11-quick-start-guide>
- Marco de Gestión Ágil de Proyectos “Scaled Agile Framework® (SAFe®)”. 2025. <https://scaledagile.com/business-solutions/industries/agile-government/>

Elaboró

- Ignacio Armando Lara Acosta
Director de Administración de Base de Datos, Seguridad y Vinculación.
Coordinación de Tecnologías de la Información
- Edmundo Arteaga Salas
Director de Planeación Estratégica Y Coordinación de Archivo.
Coordinación de Tecnologías de la Información

Autorizó

- Carlos Domínguez Hernández
Coordinador de Tecnologías de la Información
Secretaría de Hacienda.

Coordinación de Tecnologías de la Información
Actualización: Julio de 2025
Versión 2025.2.4

