Guía de seguridad informática

Para la protección de datos personales

Suprema Corte
de Justicia de la Nación

UGTSIJ/DGTI

Noviembre 2020

I. PROPÓSITO

Esta guía desarrolla diversas medidas de seguridad en materia informática dirigidas a cualquier usuario y, particularmente, a los servidores públicos que realizan tratamientos de datos personales en los bienes informáticos bajo su resguardo.

Por ello cumple con un doble propósito: **i**) fomentar una serie de medidas de seguridad para la protección de los bienes informáticos que almacenan datos personales y que se plasmaron en el *Plan de Trabajo en materia de protección de datos personales*, aprobado por el Comité de Transparencia de la Suprema Corte de Justicia de la Nación (SCJN); **y, ii**) reforzar los alcances del *Programa de concientización y capacitación en Seguridad Informática 2020* a cargo de la Dirección General de Tecnologías de la Información (DGTI).

De acuerdo con el citado programa, se reconoce al usuario como el eslabón más importante de la cadena de la seguridad. Por ello y como parte de la estrategia de seguridad informática, es importante generar consciencia en los usuarios sobre el papel que representan y mostrarles cómo pueden prevenir los riesgos que pudiera ocasionar una suplantación de identidad o una vulneración de datos personales.

Bajo esta visión institucional, existe una campaña permanente de publicación de *InfoTips*, a través de los cuales se divulga información sobre los riesgos en seguridad informática a los que están expuestos los servidores públicos de la SCJN, así como recomendaciones de acciones preventivas que pueden evitar ataques y ciberdelincuencia. Los temas que se difunden se refieren a prevención de robo de datos personales (correo *phishing*), ciberseguridad para trabajo remoto, contraseña segura y *ransomware* (secuestro de información), entre otros.

Este documento integra recomendaciones y medidas de seguridad en materia informática para que los servidores públicos de la SCJN se protejan de cualquier actividad maliciosa que ponga en

peligro los bienes informáticos, la información que ahí se almacena y, en especial, los datos personales que se tratan en dichos bienes de conformidad con sus atribuciones y las disposiciones en la materia.

Derivado de la evolución tecnológica, las medidas de seguridad que aquí se desarrollan pueden actualizarse y/o adaptarse con la normativa institucional especializada en seguridad informática.

II. RECOMENDACIONES DE SEGURIDAD INFORMÁTICA

Para hacer buen uso de los bienes informáticos y proteger la información que ahí se almacena, se recomienda adoptar las siguientes medidas básicas:

1. Cuidado de los bienes informáticos

Los bienes informáticos son todos aquellos elementos que conforman el soporte físico (hardware) del dispositivo informático (equipo de

cómputo de escritorio o portátil, servidor, escáner, impresora, equipo de comunicación como telefonía fija y móvil y videoconferencia, entre otros); así como el software respectivo que conforma el soporte lógico del elemento informático.

Para proteger los bienes informáticos, los usuarios deben observar lo siguiente:

- Utilizarlos única y exclusivamente para desarrollar las funciones que son propias de la SCJN.
- Cumplir con las medidas y recomendaciones de seguridad relacionadas con el uso y manejo de su contraseña.
- Mantenerlos en buen estado, evitando pegar etiquetas o colgar objetos en cualquiera de sus componentes. Cuando las etiquetas de inventariado se estén desprendiendo o sean ilegibles como consecuencia del tiempo y uso, avisar a la DGTI por medio de la mesa de servicios para su sustitución.
- Al retirarse de su lugar de trabajo, proteger la información contenida y el acceso a la red institucional cerrando la sesión y apagando el equipo, salvo que el administrador de la red o personal de la DGTI, por causas debidamente justificadas, indiquen lo contrario. En caso de ausentarse temporalmente de su estación de trabajo, es necesario bloquear la sesión.
- Evitar fallas en los equipos de cómputo procurando:
  - No colocar, sobre y/o cerca de los equipos y sus periféricos, alimentos o bebidas, ni consumirlos mientras los operan.
  - Colocar el equipo en un lugar libre de polvo.
  - No colocar la computadora cerca de corrientes de aire o directamente al sol.
  - No obstruir las ranuras de ventilación (en el caso de laptops no colocarlas en las piernas).

- Evitar sobrecalentamiento, apagando el equipo de cómputo al término de la jornada laboral.
- No desconectar el equipo sin antes haberlo apagado correctamente.

- No cambiar su ubicación física. En caso de que así se requiera, notificar a la DGTI mediante el levantamiento de un reporte en la mesa de servicios.
- En caso de robo o extravío, apegarse a la normativa vigente aplicable, conforme a la póliza contratada por la SCJN y/o al procedimiento establecido por el prestador de servicios, en el caso de equipo de cómputo arrendado.
- No abrirlos y/o desarmarlos.
- Asegurarse que su equipo cuente con un software antivirus y funcione con las últimas actualizaciones. Notificar mediante la mesa de servicios cualquier mensaje de error y/o advertencia que reporte el software de antivirus, respecto de su vigencia, actualizaciones y/o amenazas detectadas.
- Abstenerse de desinstalar o deshabilitar el software antivirus; alterar o cambiar la configuración de protección del antivirus o instalar un programa antivirus diferente al institucional.

2. Instalación de dispositivos y software no autorizados

Otra recomendación fundamental para el cuidado de los bienes informáticos es abstenerse de instalar dispositivos o software no autorizados en los equipos de cómputo. Para asegurarse de ello, los usuarios responsables deben observar las siguientes medidas:

- No modificar la configuración y/o instalar algún software no autorizado en el equipo de cómputo asignado; en caso de requerirlo, se deberá realizar la solicitud a través de la mesa de servicios,

justificando dicho requerimiento. La autorización para realizar la configuración le corresponde únicamente a la DGTI.

- La red de datos de la SCJN es de uso exclusivo para los equipos de cómputo propiedad de esta, o bien para aquellos que sean asignados por la DGTI. En caso de requerir el servicio de uso de la red de datos para equipos externos, se deberá justificar y solicitar por escrito a la DGTI, quien analizará la viabilidad de utilizar dicho servicio. Lo anterior, con la finalidad de proteger la seguridad de los sistemas informáticos, así como para no afectar la configuración estandarizada de los equipos de cómputo administrados por la DGTI.
- No realizar acciones que puedan interferir con la operación normal de los servicios informáticos institucionales de la SCJN, como la instalación de software o aplicaciones no autorizadas, o modificar la configuración estándar del equipo.
- Queda prohibido conectar a los equipos de cómputo dispositivos externos que puedan alterar la configuración estandarizada de los bienes informáticos.
- Para el uso de memorias USB o medios de almacenamiento externo, éstos deben ser revisados previamente con el software antivirus instalado en su equipo de cómputo.

3. Traslado de equipos de cómputo

El traslado de los equipos de cómputo fuera de las instalaciones de la SCJN es una actividad que representa un riesgo y/o amenaza para dichos bienes y la información que ahí se alberga. Para realizar de manera adecuada el traslado de dichos equipos, los usuarios responsables deben considerar lo siguiente:

- La DGTI es la única facultada para emitir oficios y/o pases de salida de los equipos de cómputo, los cuales deberán llevar rúbrica y/o sello tanto de ésta como de la Dirección General de Seguridad.

- Resguardar el bien con los cuidados necesarios, manteniéndolo en todo momento bajo su custodia. En caso necesario, atender las recomendaciones al alejarse temporalmente del equipo de cómputo.
- Ser responsable del buen uso y manejo de la información, particularmente de los datos personales, así como de sus credenciales (nombre de usuario y contraseña), considerando que es susceptible de que la información sea sustraída del equipo y mal manejada.
- Realizar el respaldo de la información contenida en su equipo de cómputo, ya sea mediante el uso de office 365 o un medio de almacenamiento externo. En caso de requerir apoyo comunicarse a la mesa de servicios de la DGTI.
- Reportar inmediatamente cualquier incidente con motivo del traslado del equipo de cómputo a la mesa de servicios.

4. Contraseñas

Las contraseñas que se asignen y/o elijan para el acceso a recursos o bienes informáticos de la SCJN, deben considerarse de carácter personal, únicas, confidenciales e intransferibles. Para su cuidado correcto debe cumplirse con lo siguiente:

A. Contar con una longitud de mínimo 9 caracteres.

B. Incluir, por lo menos, una letra mayúscula, una letra minúscula, un símbolo especial y un número.

C. Evitar el uso de palabras comunes o datos personales.

D. Ser renovadas en lapsos no mayores de 90 días.

Cada usuario es responsable de las cuentas y contraseñas que le asignen para el acceso a los recursos o bienes informáticos de la SCJN.

En caso de que un usuario tenga conocimiento o sospeche que alguna de sus contraseñas para acceso a su cuenta de correo electrónico o aplicaciones institucionales ha sido vulnerada o comprometida, deberá notificarlo inmediatamente a la mesa de servicios de la DGTI, para tramitar el cambio de la misma.

5. Respaldo de información

Se recomienda realizar respaldos de información de manera periódica para garantizar que la información almacenada en los equipos de cómputo no se afecte con alguna falla y esto se traduzca, a su vez, en una vulneración de la información, particularmente de los datos personales (pérdida o destrucción no autorizada).

Se puede hacer uso de office 365 para el respaldo de su información o, en su caso, a través de una unidad de almacenamiento externo.

Para realizar respaldos de la información, los usuarios pueden solicitarlo a la mesa de servicios, quien asesorará y apoyará en el procedimiento para realizar el respaldo de la información guardada en el equipo de cómputo asignado.

Todos los usuarios son responsables de la información que generen, utilicen y transfieran, así como de implementar y supervisar los controles para protegerla durante su manejo considerando la clasificación y gestión de la información de acuerdo con sus funciones.

6. Uso de correo electrónico

Las cuentas de correo electrónico son personales e intransferibles, por lo que cada usuario es responsable directo de la información contenida en su buzón de correo, su uso y contraseña correspondiente.

No se debe proporcionar la cuenta de correo electrónico institucional para recibir información que no sea con fines laborales ni compartir la cuenta con otros usuarios.

Los usuarios deben eliminar todo correo electrónico de dudosa procedencia, sin abrir los archivos adjuntos que acompañen a los mismos y evitar reenviar estos correos a cuentas internas o externas. En todo caso, el usuario que llegue a detectar un correo con posible riesgo o amenaza, deberá reportarlo de forma inmediata a la mesa de servicios de la DGTI.

Los usuarios de correo electrónico son responsables de la información que intercambien a través de su cuenta de correo institucional o de aquella que resguarden en su buzón. Toda cuenta de correo electrónico institucional creada, deberá tener a un servidor público de la SCJN como responsable de la misma.

III. REPORTE DE INCIDENTES Y VULNERACIÓN DE DATOS PERSONALES

Para la atención de cualquier solicitud, incidente o posible evento que constituya un riesgo o una amenaza sobre los bienes o servicios tecnológicos, deberá reportarse a la mesa de servicios:

- Vía telefónica: 55 41131000, ext. 1111
- Correo electrónico: 1111@scjn.gob.mx
- A través de la Ventanilla Única de Servicios (intranet).

Los horarios de atención son de 9:00 am a 18:00 hrs.

En caso de que se presente un incidente de los bienes informáticos que implique, a su vez, alguna vulneración de datos personales (pérdida o destrucción no autorizada; robo, extravío o copia no autorizada; uso, acceso o tratamiento no autorizado; daño, alteración o modificación no autorizada), se deberá dar aviso a la DGTI, a través de la mesa de servicios en los días y horarios establecidos, sin perjuicio de observar el procedimiento establecido en el *Instructivo para registrar y reportar vulneraciones de datos personales*.

Dudas o comentarios dirigirse a:

Mtro. Benjamín Alejandro Cervantes Pérez
Correo electrónico: bcervantes@scjn.gob.mx
Teléfono: 55 4113-1000 Ext. 5817
Unidad General de Transparencia
y Sistematización de la Información Judicial

Ing. Francisco Javier Rojas Romero
Subdirector General de Servicios Tecnológicos
Correo electrónico: frojas@scjn.gob.mx
Teléfono: 55 4113-1000, Ext. 1786

Mtro. Omar Salinas García
Director de Seguridad Informática
Correo electrónico: osalinasg@scjn.gob.mx
Teléfono: 55 4113-1000, Ext.5479
Dirección General de Tecnologías de la Información

Mesa de Servicio DGTI
1111@scjn.gob.mx
Teléfono: 55 4113-1000 Ext. 1700