Suprema Corte
de Justicia de la Nación

Guía de
SEGURIDAD INFORMÁTICA
para la protección de datos personales

UGTSIJ

OCTUBRE 2025

DGTI

I. Propósito

Esta guía desarrolla diversas medidas de seguridad en materia informática dirigidas a cualquier persona usuaria y, particularmente, a las personas servidoras públicas que realizan tratamientos de datos personales a través de 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 Documento de Seguridad en materia de protección de datos personales, aprobado por el Comité de Transparencia de la Suprema Corte de Justicia de la Nación (La Corte); y,

ii. Reforzar los alcances del *Programa de concientización y capacitación en Seguridad Informática* a cargo de la Dirección General de Tecnologías de la Información (DGTI).

De acuerdo con el citado programa, se reconoce a las personas usuarias 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 conciencia en las personas usuarias sobre el papel que representan y mostrarles cómo pueden prevenir los riesgos que pudiera ocasionar un incidente de seguridad informática o una vulneración de datos personales.

Bajo esta visión institucional, a partir de febrero de 2023 se implementó la Plataforma en línea de concientización en Seguridad Informática que incluyen contenidos para concientizar a todas las personas usuarias de *La Corte* sobre acciones de prevención y mejores prácticas en la materia, con el objetivo de fortalecer la cultura de la ciberseguridad. De igual manera, existe una campaña permanente de publicación de *InfoTIps*, a través de los cuales se divulga información relativa a los riesgos en seguridad informática a los que están expuestos las personas servidoras públicas de *La Corte*, así como recomendaciones de acciones preventivas que pueden evitar ataques y ciberdelincuencia. Los temas que se difunden a través de estos medios se refieren a prevención de robo de datos personales (correo *phishing*), ciberseguridad para trabajo remoto, contraseña segura y ***ransomware*** (secuestro de información), entre otros.

En ese sentido, esta Guía integra las medidas de seguridad en materia informática para que las personas servidoras públicas de *La Corte* 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.

Toma como referencia lo dispuesto en el Acuerdo General número VIII/2022, por el que se regulan el uso y aprovechamiento de los bienes y servicios de tecnologías de la información y comunicaciones, así como de la seguridad informática. Asimismo, materializa la obligación de establecer y mantener las medidas de seguridad de carácter técnico para la protección de los datos personales que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como para garantizar la confidencialidad, integridad y disponibilidad (artículo 25 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados).

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

II. Recomendaciones de seguridad informática

Para hacer buen uso de los bienes informáticos y proteger la confidencialidad, disponibilidad e integridad de la información, incluyendo datos personales que estos procesan o almacenan, es necesario adoptar las siguientes medidas:

1. Cuidado de los bienes informáticos

Los bienes informáticos[1] son todos aquellos elementos que forman el hardware, ya sea la unidad central de procesamiento, sus periféricos, los equipos que tienen una relación directa de uso con respecto a ellos y que, en conjunto, conforman el soporte físico del elemento informático, como el equipo de cómputo personal de escritorio o portátil, servidor, escáner, impresora, equipos de comunicaciones, telefonía fija y móvil y videoconferencia, entre otros, así como el software que conforma el soporte lógico del elemento informático.

Para proteger los bienes informáticos, las personas usuarias responsables deben observar lo siguiente:

- Utilizarlos única y exclusivamente para el desempeño de las funciones encomendadas por La Corte y demás actividades inherentes a las mismas.
- Cumplir con las medidas y recomendaciones de seguridad relacionadas con el uso y manejo de su contraseña.

[1] AGA VIII/2022

- Mantenerlos en buen estado, evitando pegar etiquetas o colgar objetos en cualquiera de sus componentes. Cuando las etiquetas de inventariado se estén desprendiendo o bien sean ilegibles como consecuencia del tiempo y uso, deberán avisar a la DGTI por medio del Centro de Atención a Usuarios (CAU).
- Al retirarse de su lugar de trabajo, proteger la información contenida 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.
- No colocar, sobre y/o cerca de los equipos y sus periféricos, alimentos o bebidas, ni consumirlos mientras los operan.
- Las personas servidoras públicas deberán abstenerse de desarmar o intentar reparar los equipos de cómputo personal e impresión asignados.
- En el caso de que requieran mantenimiento correctivo a equipos de cómputo personal, deberán levantar un reporte a través del CAU, el cual será canalizado al área responsable de la DGTI a efecto de que se proceda con su atención.
- Para la solución de fallas del equipo de cómputo personal bajo el esquema de administración de servicios, los usuarios deberán comunicarse al CAU y levantar el reporte correspondiente, el cual será atendido conforme a los niveles de servicio establecidos.
- No cambiar su ubicación física. Cualquier reubicación física de un equipo de cómputo asignado a los usuarios resguardantes deberá ser solicitada al CAU para su atención.
- Lo anterior, sin perjuicio de que el equipo de cómputo personal puede ser trasladado fuera de las instalaciones de la Suprema Corte, derivado del trabajo a distancia que requieran realizar las personas usuarias, lo cual será bajo la responsabilidad de éstos.

Asimismo, las personas deben abstenerse de llevar a cabo acciones que puedan interferir con la operación normal de los servicios informáticos institucionales de *La Corte* tales como:

- Desinstalar o deshabilitar el software antivirus, o algún otro software de Ciberseguridad.
- Alterar o cambiar la configuración de protección del antivirus.
- Instalar un programa antivirus diferente al institucional.

- Conectar a los equipos de cómputo personal dispositivos externos o no considerados en el arrendamiento de dichos equipos, que puedan afectar la correcta operación de este. En caso de requerir la conexión de algún componente, como son impresoras, teclados, mouse, pantallas, entre otros, podrá solicitar asesoría y soporte al CAU de la DGTI, con la finalidad de verificar compatibilidad y correcta configuración.

    - Para el uso de medios de almacenamiento tales como USB, discos duros, DVD, CD, entre otros, el usuario deberá revisarlos previamente con el software antivirus de su equipo de cómputo.

- Modificar la configuración, ni instalar algún software no autorizado en el equipo de cómputo personal asignado. En caso de requerirlo para el desempeño de sus funciones, los usuarios deberán realizar la solicitud a través del CAU, justificando dicho requerimiento, la cual será evaluada y, en su caso, autorizada por la DGTI.

2. Uso de la red de datos institucional

La red de datos de *La Corte* será de uso exclusivo para los equipos de cómputo personal y dispositivos móviles propiedad de ésta, así como para equipos arrendados que sean asignados por la DGTI.

Toda persona servidora pública que cuente con un equipo de cómputo personal institucional tendrá derecho al uso del servicio de Internet, cumpliendo con los criterios establecidos, para lo cual debe observar lo siguiente:

- Los usuarios que cuenten con servicios de Internet deberán utilizar las herramientas institucionales aprobadas por la DGTI para el ejercicio de las funciones asignadas.
- 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, la cual analizará la viabilidad de utilizar dicho servicio, procurando en proteger la seguridad de los sistemas informáticos y no afectar la configuración estandarizada de los equipos de cómputo administrados por la DGTI.
- Abstenerse de visitar y realizar navegaciones a las páginas de Internet que se encuentren en las categorías siguientes: contenido sexual explícito y pornografía; sitios dedicados al hackeo o robo de información; juegos, juegos de apuesta, así como cualquier sitio web que pueda poner en riesgo la seguridad de la información y la integridad de los equipos de cómputo personal en *La Corte*.

- No realizar acciones que puedan interferir con la operación normal de los servicios informáticos institucionales de *La Corte*, tales como instalación de software o aplicaciones no autorizadas, o modificar la configuración estándar del equipo.

3. Traslado de equipos de cómputo y trabajo a distancia

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

- La persona servidora pública que firme el resguardo del bien informático que le fue asignado, será responsable en todo momento del uso y traslado dentro y fuera de las instalaciones de *La Corte*.
- En caso de cambio de adscripción de área, las personas usuarias deberán notificar a la DGTI mediante el levantamiento de un reporte al CAU a fin de que se les apoye con la actualización de los resguardos correspondientes.
- Ser responsable del buen uso y manejo de la información, particularmente de los datos personales, así como de su cuenta de usuario y contraseña, considerando que su vulneración hace susceptible que la información sea sustraída del equipo y mal manejada.
- Evitar el uso de redes inalámbricas públicas en equipos de cómputo institucionales.
- Acceder a los recursos en la red de *La Corte* a través de la VPN, para lo cual deberá solicitar al CAU que le sea habilitada y configurada en caso de no contar con ella.
- Tener precaución durante el uso de herramientas de trabajo a distancia, para evitar exponer información sensible (confidencial) como datos personales, al momento de compartir la pantalla de su equipo de cómputo durante las sesiones de trabajo.
- Se recomienda mantener la pantalla del equipo de cómputo (escritorio) despejado, es decir, evitar almacenar, crear accesos directos a archivos o colocar archivos en este, procurando mantener únicamente los iconos de acceso al software de uso frecuente, porque se pueden hacer identificables archivos con información confidencial.

- Cerrar la sesión de trabajo o apagar el equipo de cómputo al retirarse de su lugar de trabajo, salvo que el administrador de la red o personal de soporte de la DGTI, por causas debidamente justificadas, indiquen lo contrario.
- Procurar configurar una contraseña fuerte para la red WiFi que utilice en trabajo a distancia, la cual contenga por lo menos 12 caracteres y se renueve periódicamente.
- Reportar inmediatamente cualquier incidente con motivo del traslado del equipo de cómputo al CAU.

4. Contraseña personal

Las contraseñas que se asignen o elijan para el acceso a los recursos o bienes informáticos de *La Corte* y el uso de estas son responsabilidad de cada persona usuaria. Las contraseñas son consideradas de carácter personal, únicas, confidenciales e intransferibles. Para mayor seguridad de ellas, debe cumplirse con lo siguiente:

A. Contar con una longitud de mínimo 12 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, que se encuentren en un diccionario o datos personales en la construcción de estas.

D. Renovarlas en periodos no mayores a 90 días.

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 al CAU de la DGTI.

5. Respaldo de información

Es recomendable realizar respaldos de la información almacenada en los equipos de cómputo de manera periódica para minimizar el riesgo de pérdida de esta, derivado de alguna falla o extravío del equipo de cómputo y evitar que 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 herramientas en la nube institucional (*OneDrive/Sharepoint* de *Office365*) o un medio de almacenamiento externo.

Para solicitar asistencia con relación al respaldo de la información, las personas usuarias pueden hacerlo a través del CAU, quien asesorará y apoyará en el procedimiento para realizar el respaldo de la información guardada en el equipo de cómputo asignado.

Todas las personas usuarias son responsables de la información que generen, utilicen y transfieran, así como de atender las recomendaciones emitidas por la DGTI 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 serán personales e intransferibles, por lo que el usuario a quien le sea asignada la cuenta y clave será el responsable directo de la salvaguarda de la información, su uso y contraseña correspondiente.

El uso del servicio de correo electrónico institucional será destinado únicamente para apoyar las funciones estrechamente vinculadas a las mismas, como persona servidora pública de *La Corte*. No se debe proporcionar la cuenta de correo electrónico institucional para recibir información que no sea con fines laborales ni compartir la contraseña de la cuenta de correo con otros usuarios.

Las personas usuarias se abstendrán de realizar cambios en la configuración de las herramientas o software habilitadas por la DGTI para el uso del servicio de correo electrónico.

Los usuarios deberán eliminar todo correo electrónico de dudosa procedencia, y no deberán abrir los archivos adjuntos que acompañen a los mismos, así como evitar reenviar estos correos a cuentas internas o externas. En todo caso el usuario que llegue a detectar un correo electrónico como posible riesgo o amenaza, deberá reportarlo de forma inmediata al CAU, a efecto de que la DGTI lleve a cabo las acciones que estime conducentes.

Las personas usuarias son responsables de la información que intercambien a través de su cuenta de correo institucional o de aquella que resguarden en su buzón, por lo que deberán realizar respaldos periódicos de la misma. La DGTI a solicitud del usuario, asesorará y apoyará en el procedimiento para realizar dicho respaldo, previa solicitud al CAU.

7. Prevención de *phishing*, *smishing* y *vishing*

El *phishing*, *smishing* y *vishing*, son tipos de ataques que, mediante el uso de la **Ingeniería social,** pretenden engañar a las personas usuarias para que ella misma proporcione información sensible o permita la instalación de *malware* en sus dispositivos electrónicos. Estos buscan, entre otros objetivos: el robo de datos de acceso a banca en línea, email, redes sociales, etc.; robo de datos personales; instalación no deseada de aplicaciones espía u otro tipo de malware en los dispositivos de la persona usuaria; secuestro de información o cuentas de mensajería para realizar acciones fraudulentas a los contactos de la persona usuaria afectada.

Phishing Consiste principalmente en el envío de correos electrónicos que suplantan la identidad de compañías o instituciones públicas para solicitar información sensible a la persona usuaria o hacerle descargar algún tipo de malware.

Smishing Esta técnica hace uso de mensajes mediante servicios o aplicaciones de mensajería en equipos celulares con el objetivo de suplantar la identidad de compañías o instituciones públicas para, como se comentó anteriormente, incluso secuestrar la cuenta del servicio de mensajería (como "Whatsapp") de la persona usuaria para uso fraudulento a nombre de ella.

Vishing Este tipo de ataque se realiza mediante una llamada telefónica y hace uso de información obtenida previamente mediante internet (redes sociales), para engañar a la persona usuaria.

Para protegernos del ***phishing*** (correo electrónico) o ***smishing*** (mensajería electrónica), es importante seguir las siguientes recomendaciones:

- Validar siempre la dirección de correo electrónico del remitente o cuenta origen del mensaje. Desconfía si es desconocido e inesperado.
- Comprobar el asunto del correo electrónico o del mensaje.
- No dar clic en ningún botón o enlace sospechoso dentro del correo electrónico o mensaje, sin validar la procedencia y autenticidad de este.
- No llamar a ningún número telefónico al que se haga referencia en el correo o mensaje.
- No descargues archivos adjuntos sospechosos.
- Revisa el contenido del correo o mensaje y desconfía si:
    - Contiene faltas de ortografía.
    - Se solicitan datos personales o confidenciales.

- Existe un sentido de urgencia o intentan presionarte para que accedas a algún enlace o archivo adjunto en el correo.
- Te hablan de trabajos (sin que hayas solicitado), premios (sin haber jugado o participado) o paquetes recibidos (sin haberlos pedido).

- Configura un PIN o contraseña de confirmación para los servicios de mensajería como Whatsapp.
- De preferencia utiliza un doble factor de autenticación para acceder a tus servicios personales de correo electrónico, redes sociales, etc.

Aunado a lo anterior, considera que ninguna institución financiera u empresa relacionada te debe pedir o actualizar tu información de cuenta o confirmar NIP de alguna tarjeta por correo electrónico o mensaje de texto. Si es el caso, contacta vía telefónica u otro medio verificado a dicha institución.

Para protegernos del ***vishing*** (llamada telefónica), es importante seguir las siguientes recomendaciones y considerar:

- No publicar información de contacto en redes sociales tales como teléfonos o correo electrónico.
- Algunas veces las llamadas recibidas pueden ser muy persuasivas, ante la más mínima duda o si desconoces a la persona o institución que te contactó, simplemente cuelga.
- Los delincuentes buscarán infundirte miedo o adularte para así aprovecharse de ello. Algunas veces se ofrecen recompensas o premios.
- Realiza preguntas de control de identidad, para identificar quién o de qué institución nos están marcando, solicitando información de contacto y en su caso validar dicha información.
- En ningún caso dar información confidencial.
- En ningún caso, personas usuarias a nombre de La Corte, nos deben pedir información de contraseñas o datos bancarios, ni contactar por medios no institucionales.

Reporta y toma acción

Phishing

- Si recibiste un correo phishing a tu cuenta institucional, repórtalo al CAU de la DGTI y si consideras que se ha comprometido tu contraseña, solicita el apoyo para renovarla.

- Si consideras que has descargado algún tipo de *malware* o *software* malicioso, solicita apoyo al CAU.

Smishing

- Denuncia desde cualquier teléfono al 088 o haz una denuncia anónima al 089.
- Si consideras que se tus contraseñas (banca, redes sociales, servicios o apps de mensajería) han sido comprometidas, cámbialas.
- Si has descargado algún tipo de malware en tu teléfono móvil, resetéalo si sabes cómo hacerlo o contrata un servicio técnico con tu proveedor de telefonía móvil.

Vishing

- Guarda la calma y denuncia al 088 o 089.

III. Reporte de incidentes y vulneraciones

Para la atención de solicitudes, incidentes o posibles eventos que constituyan un riesgo de seguridad informática sobre los servicios tecnológicos, éstos deberán ser reportados al CAU por los medios de contacto institucionales:

- Vía telefónica: 55 41131000, ext. 1111
- Correo electrónico: 1111@mail.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 avisar a la DGTI, a través de su Centro de Atención a Usuarios (CAU) sin perjuicio de observar el procedimiento establecido en el *Instructivo para registrar y reportar vulneraciones de datos personales*.

UNIDAD GENERAL DE TRANSPARENCIA Y SISTEMATIZACIÓN DE LA INFORMACIÓN JUDICIAL

Dirección de Protección de Datos Personales

DIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN

Dirección de Gestión de Seguridad Informática

Suprema Corte
de Justicia de la Nación