C I R C U L A R CSJCUC23-340

Fecha: 5 de octubre de 2023

Para: **SERVIDORES JUDICIALES DEL DISTRITO JUDICIAL DE CUNDINAMARCA Y AMAZONAS**

De: CONSEJO SECCIONAL DE LA JUDICATURA CUNDINAMARCA Y AMAZONAS

Asunto: "*Recomendaciones prácticas para fortalecer las habilidades informáticas*"

Estimados servidores judiciales,

De manera atenta, y a efectos de fortalecer las habilidades informáticas de la entidad, se sugiere las siguientes mejores prácticas:

1. Usted es blanco de los delincuentes informáticos

   No diga nunca: "no me pasará". Todos estamos en riesgo y también está en juego el bienestar personal y financiero suyo y de la entidad; la cadena es tan fuerte como su eslabón más débil. La ciberseguridad es responsabilidad de todos y cada uno, no solamente de las áreas de tecnología o de su personal. Al seguir las recomendaciones y mantenerse vigilante, usted hace su parte para protegerse y para proteger a los demás, incluyendo a los suyos.

2. Mantenga actualizado su software

   Las actualización de su sistema operativo y de sus programas es crítico. Mantenga encendida la función de actualizaciones automáticas de su sistema operativo (menú inicio --> configuración --> actualización y seguridad --> buscar actualizaciones). Mantenga actualizados sus navegadores de internet (clic en el botón contextual ubicado en la parte superior derecha con tres puntos suspensivos --> ayuda --> acerca de). No use extensiones en los navegadores. Todo el software que necesita se lo debe proporcionar la mesa de ayuda, únicamente.

   No instale ni intente instalar software no proporcionado por la entidad. De haber recibido aplicaciones de dicha Mesa de Ayuda, manténgalas actualizadas. Si existe software instalado en su computador que no usa, pida a la Mesa de Ayuda que lo desinstale. Su usuario del sistema operativo NO debe tener privilegio de administrador; si detecta lo contrario, póngase en contacto con la Mesa de Ayuda.

3. Evite las estafas de suplantación

   Tenga cuidado de correos electrónicos, mensajes instantáneos, mensajes de texto, llamadas por datos, llamadas por voz y/o interacciones en redes sociales sospechosos. Mediante diversas tácticas de ingeniería social, los ciber-delincuentes intentarán engañarlo para que divulgue información personal e información tal como: usuarios, contraseñas, información bancaria y/o crediticia. Las estafas de suplantación pueden presentarse por medio de cualquiera de los medios mencionados, pero principalmente a través de correo electrónico. Sospeche de cualquier correo electrónico que parezca oficial o de cualquier llamada en donde le indaguen por información personal o financiera.

4. Practique una buena gestión de contraseñas

   Todos tenemos muchas contraseñas a administrar, y es fácil tomar atajos, tal como reusar contraseñas. Un gestor de contraseñas le puede ayudar a mantener contraseñas únicas fuertes para todas sus cuentas. Pida a la mesa de ayuda que le proporcione un gestor de contraseñas apropiado. Si la entidad le ofrece la protección de un segundo factor de autenticación (2AF) o la protección de múltiples factores de autenticación (MAF) para los servicios web oficiales, haga uso de dicha protección. Cambie sus contraseñas con frecuencia.

5. Sea cuidadoso con los enlaces a los que le da clic

   Mantenga su hábito de navegación web restringido a asuntos laborales; no visite sitios web desconocidos o de índole personal; atienda el mensaje de su navegador cuando le indica que el sitio web al cual va a ingresar es inseguro, absteniéndose de ingresar. No descargue software de fuentes desconocidas; todo el software que necesita se lo debe proporcionar la mesa de ayuda, únicamente. A menudo, dichos sitios web hospedan programas maliciosos que se pueden instalar automática y silenciosamente en su computador, tableta, teléfono inteligente, etc. (en su TV inteligente, por ejemplo). Si enlaces o adjuntos en el correo electrónico lucen sospechosos, por cualquier razón, no de clic en éstos. En lugar de dar clic, reporte el correo sospechoso a reportesgsi@deaj.ramajudicial.gov.co .

6. No deje sus dispositivos descuidados

   La seguridad física de sus dispositivos es tan importante como su seguridad técnica. Si necesita abandonar su computador, tableta o teléfono por cualquier periodo de tiempo, bloquéelo de forma que nadie más pueda usarlo. Si debe abandonar datos en una unidad extraíble, asegúrese de que la unidad esté cifrada y bloqueada con contraseña. Al final de la jornada, apague su equipo en lugar de dejarlo hibernado o suspendido. Si ha sido víctima de robo o pérdida de cualquiera de los dispositivos proporcionados por la entidad o de cualquier dispositivo desde el cual accede a servicios de la entidad, repórtelo a:

   reportesgsi@deaj.ramajudicial.gov.co

7. Salvaguarde los datos protegidos

   Sea consiente de los datos que gozan especial protección por la constitución y los tratados internacionales, la ley y las demás disposiciones aplicables. Si debe manejar datos de este tipo, hágalo siempre con las herramientas que le proporciona la entidad y no los deje al alcance de terceros[1]. No imprima información protegida.

[1] Puede encontrar un ejemplo en relación con el derecho a la intimidad, art. 15 C.P., en SU355-22.

8. Use sus dispositivos móviles de forma segura

   Los dispositivos móviles son muy susceptibles a ataque informático. Bloquee sus dispositivos móviles mediante PIN o contraseña y nunca los transporte en público sin bloquear. Instale aplicaciones desde fuente segura como lo es la tienda de aplicaciones proporcionada por el fabricante del dispositivo (AppStore, Google Play, etc.). Mantenga el sistema operativo de sus dispositivos móviles actualizado. Cuando consulte correos electrónicos, mensajes de texto, mensajes instantáneos o sitios web desde sus dispositivos móviles, no de clic en enlaces o adjuntos no solicitados. Evite transmitir o almacenar información personal en sus dispositivos móviles; si resulta inevitable, haga uso de la funcionalidad de cifrado de datos del dispositivo y consulte el manual del dispositivo proporcionado por el fabricante para usar dicha funcionalidad correctamente.

9. Instale protección de antivirus

   La entidad administra y proporciona el antivirus ESET Endpoint Security a todos los computadores; valide que dicho antivirus se encuentre instalado en su computador y, en caso de no estar instalado, pida a la Mesa de Ayuda que lo instale. Luego, mantenga actualizado su antivirus (abrir aplicación ESET Endpoint Security --> Actualización --> Buscar actualizaciones), para que la protección sea efectiva. Si aún después de recibir el apoyo de la Mesa de Ayuda vuelve a ocurrir que el antivirus deja de reconocer el licenciamiento o no actualiza correctamente, repórtelo a:

   reportesgsi@deaj.ramajudicial.gov.co .

10. Haga copia de respaldo de sus datos

    Haga copia de sus datos con frecuencia. Si resulta ser víctima de un incidente de seguridad de la información, la única forma de restaurar sus datos es con la copia de seguridad. La entidad dispone de la herramienta OneDrive web, la cual puede abrir con su navegador y su cuenta institucional, de forma tal que pueda cargar sus datos allí. Esto, con el fin de restaurarlos de nuevo en su computador si llega a necesitarlo. La entidad no proporciona medios extraíbles para realizar copia de respaldo o para otro fin. En general, se desaconseja el uso y la compartición de medios extraíbles (memorias USB, discos duros externos). En la excepción de que la entidad le haya proporcionado un medio extraíble, preocúpese por: no conectar dicho dispositivo a equipos distintos al proporcionado por la entidad, no transportar el dispositivo fuera del lugar de trabajo, dejarlo bajo llave cuando no lo esté usando, usar el software especializado de cifrado del dispositivo que le entregó la entidad cuando le proporcionó el medio extraíble.

11. Mantenga los asuntos personales segregados de los asuntos oficiales

    Los equipos y servicios proporcionados por la entidad son de uso oficial. Absténgase de realizar actividades privadas desde dichos equipos y servicios. Por ejemplo, no use el correo oficial para enviar correos electrónicos de índole privada o para suscribirse a listas de distribución de tipo comercial, no ingrese a su cuenta bancaria o sus redes sociales a través del computador proporcionado por la entidad.

12. El acceso remoto debe ser restringido

    Por regla general, no es necesario habilitar el acceso remoto a su computador. Si, excepcionalmente, recibió permiso para acceder de forma remota a su equipo, p.ej., a

través de una VPN, haga un buen uso del servicio y cumpla con las políticas de seguridad de la información[2][3] que le entregaron junto con el servicio.

13. La conexión a internet debe ser segura

    Su computador no debe ser conectado a proveedores de internet distintos al proporcionado por la entidad, mucho menos a redes de WiFi públicas. Si su conexión de internet con el proveedor oficial falla, póngase en contacto con la Mesa de Ayuda telefónicamente.

14. Pida ayuda

    Si es sujeto a presiones para realizar actos contrarios a la seguridad de la información, apóyese en las personas y en los canales de la entidad; usted no está solo, las áreas de bienestar, riesgos profesionales, tecnología y demás áreas de apoyo están preparadas para atenderlo y brindar soluciones.

    No comparta información que en el futuro pueda ser explotada en contra de la entidad y/o en contra de los suyos. Recuerde que internet es una fuente de información pública y que rutinariamente es catalogada por los buscadores de internet, de forma que es muy poco probable que la información que usted compartió y que llegó a internet sea borrada definitivamente. Use su sentido común: si está a punto de compartir información por medios digitales, piense que eso es equivalente a compartirla a gritos en la calle.

    Si perdió acceso a los equipos y/o servicios proporcionados por la entidad o si después de leer esta guía identifica que se ha materializado un incidente de seguridad de la información, repórtelo oportunamente. Exija y acuda a capacitaciones orientadas a fortalecer sus habilidades informáticas. Vuelva a leer esta guía. Con las habilidades adquiridas a través de las capacitaciones de la entidad, cultive en su equipo de trabajo y en su familia una cultura de transparencia y de buenas prácticas de seguridad de la información.

En el pie de página de este oficio encuentra nuestros canales de atención en caso que requiera mayor información.

Cordialmente,

JESÚS ANTONIO SÁNCHEZ SOSSA
Presidente

JASS / eapg

[2] https://www.ramajudicial.gov.co/portal/politicas-de-privacidad-y-condiciones-de-uso
[3] https://www.ramajudicial.gov.co/web/ley-de-transparencia-y-del-derecho-de-acceso-a-la-informacion-publica-nacional/politicas-de-seguridad-de-la-informacion-del-sitio-web