INSTRUCTIVO: POLÍTICA DE USO ACEPTABLE (PUA) DE RECURSOS INFORMATICOS

CORTE SUPREMA DE JUSTICIA
PODER JUDICIAL DE TUCUMÁN

OFICINA DE COORDINACIÓN ESTRATÉGICA DE PLANIFICACIÓN Y GESTIÓN
CORTE SUPREMA DE JUSTICIA

OFICINA DE GESTIÓN JUDICIAL
EXCMA CORTE SUPREMA DE JUSTICIA

DIRECCION DE SISTEMAS
EXCMA. CORTE SUPREMA DE JUSTICIA

I. Introducción

1.1 Objetivo

Este documento establece pautas de trabajo admitidas de uso responsable, recomendaciones y restricciones acerca del empleo de los recursos informáticos del Organismo por parte de su personal.

1.2 Alcance

Las directivas que desde este documento se imparten deben ser respetadas por agentes judiciales, funcionarios, magistrados, personal contratado, contratistas y toda aquella persona autorizada debidamente a emplear dichos recursos.

1.3 Historial de Revisiones

Versión: 1.00

Revisión: 2024-05-22

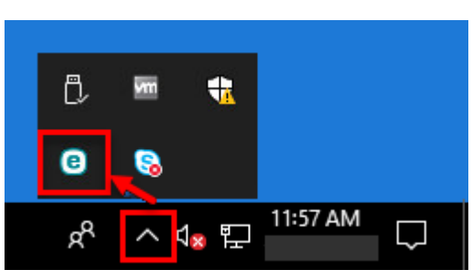
Responsable: Seguridad Informática – Dirección de Sistemas

Cambios: Versión Final

2. Equipamiento Informático

2.1. Estaciones de trabajo

- **2.1.1** Las estaciones de trabajo (computadoras de usuario o notebooks) deben **permanecer apagadas fuera del horario laboral**, como así también los fines de semana, con el propósito de ahorrar energía y minimizar riesgos de incidentes informáticos, a excepción de aquellos equipos que, por condiciones inherentes su tarea, deban quedar encendidos.
- **2.1.2** Si abandona temporalmente su entorno de trabajo, **deje bloqueada la sesión en la computadora** para evitar accesos no autorizados : puede consultar a personal de Dirección de Sistemas para que esto se produzca automáticamente luego de un determinado tiempo de inactividad.
- **2.1.3 No descargue ni instale programas en la estación de trabajo** : ante un requerimiento de este tipo escale una solicitud a **Mesa de Ayuda** o **Area de Sistemas** que le corresponda.
- **2.1.4** Revise que su equipo cuente con la solución antivirus correspondiente y que la misma se encuentra actualizada. Puede verificar esto comprobando la presencia del ícono que se muestra abajo a la derecha en el área de notificaciones de la barra de tareas.



- Si no lo encuentra, o reconoce en el mismo alguna señal de alerta, comuníquese con el sector de **Mesa de Ayuda** al teléfono detallado al pié del documento o **Area de Sistemas** que le corresponda en caso de tratarse de una delegación del interior.
- **2.1.5 No guarde en la estación de trabajo archivos personales** o que no tengan relación con su trabajo.

2.2. Medios de Almacenamiento Externos

- **2.2.1 Evite conectar de medios de almacenamiento externos USB** (pendrives, celulares, discos externos, etc) siempre que sea posible.
- **2.2.2** Evite emplear dispositivos **que no pertenezcan al Organismo** y/o que hayan sido usados en otro ámbito fuera de su oficina.
- **2.2.3** Si se encuentra obligado hacerlo y no está seguro acerca de la procedencia del dispositivo externo, **asegúrese de efectuar una exploración antivirus** sobre el mismo cuando lo conecte a la estación de trabajo.

3. Servicios de red e Internet

3.1 Navegación web

- **3.1.1** Procure **no acceder a sitios no relacionados al ámbito laboral** : existe un alto porcentaje de contenido malicioso en Internet que puede afectar su estación de trabajo o dispositivo.
- **3.1.2 No visite sitios propensos a distribuir software malicioso** (generalmente contenido multimedia o software que se anuncia como "gratis") : además de ir en contra de la primera recomendación estos sitios frecuentemente contienen virus.
- **3.1.3** Si el sistema antivirus le ha reportado en pantalla que un sitio es malicioso **no insista en su intento de accederlo**: todas las instancias de detección son reportadas y quedan expuestas en informes posteriores.
- **3.1.4 No almacene contraseñas en el navegador:** si alguien accede a su dispositivo o si el mismo es vulnerado por algún software malicioso, estas pueden terminar en manos de delincuentes informáticos.

3.2 Correo Electrónico

- **3.2.1** Procure no emplear el **correo oficial** para temas ajenos al Organismo.
- **3.2.2** Procure no emplear el **correo personal** en cuestiones relacionadas con su trabajo en el Organismo.
- **3.2.3 Atienda las recomendaciones mencionadas** en la cabecera de los correos que recibe en el correo oficial: revise con cuidado la identidad del remitente y no siga los enlaces que lleven a sitios externos al Poder Judicial de Tucumán a menos de que esté completamente seguro de que no se trata de un sitio malicioso o suplantado. Ante la duda o sospecha de que puede estar en presencia de un correo malicioso, reenvíelo a ***segurinfo@justucuman.gov.ar*** para su análisis y comunique inmediatamente al sector de **Mesa de Ayuda** o **Area de Sistemas** que le corresponda.
- **3.2.4 Depure frecuentemente los correos de su cuenta de correo oficial**, preservando solo aquellos que le resultarán útiles posteriormente y liberando espacio para la recepción de nuevos correos.
  Ud. es responsable de que su casilla de mail oficial disponga del espacio suficiente para recibir la información que por este medio se distribuye.

- **3.2.5** Procure **no enviar desde el mail oficial adjuntos de gran tamaño** si en su lugar puede enviar un enlace de referencia a la descarga del archivo en cuestión.
- **3.2.6 Evite enviar correos en forma masiva desde el correo oficial a cuentas externas**: esto ocasiona que nuestro dominio, **"*justucuman.gov.ar*"**, sea calificado como distribuidor de correo no deseado y posteriormente bloqueado.
- **3.2.7** Al enviar correos empleando el correo oficial, **evite insertar direcciones de respuesta externas al dominio "*justucuman.gov.ar*"**.

4. Incumplimiento

En virtud de lo expresado y ante evidencia de hacer caso omiso a lo establecido, la **Dirección de Sistemas** puede verse obligada a:

- Restringir el servicio de Internet del dispositivo.
- Restringir las conexiones de red del dispositivo.
- Escalar el incumplimiento a las autoridades competentes, quienes podrían aplicar sanciones en función de la gravedad del mismo.

5. Contacto

Ante cualquier consulta referente lo expresado, el usuario puede comunicarse a :

- Capital : Mesa de Ayuda al 4555155 (o 4555100 / Int. 5555)
- Delegaciones / Juzgados de Paz : Area de Sistemas que le corresponda.
- Oficina de Seguridad Informática de la CSJ : *segurinfo@justucuman.gov.ar*

"LA SEGURIDAD DE LA INFORMACIÓN DEL ORGANISMO TIENE UN VALOR QUE TODOS ESTAMOS OBLIGADOS A CUIDAR. AGRADECEMOS Y CONTAMOS CON SU COLABORACIÓN."