

PROTOCOLO ■■■

PROVINCIAL DE CIBERSEGURIDAD

Estándar de IT: Política de Uso Aceptable de Recursos de Tecnología de la Información

08
CAPÍTULO



Estándar de TI: Política de Uso Aceptable de Recursos de Tecnología de la Información

1.0 Propósito y Beneficios

El uso adecuado por parte de la Repartición respecto de la información y de los recursos de TI, así como la seguridad eficaz de dichos recursos, requieren la participación y el apoyo del personal de la Repartición (“usuarios”). Un uso inadecuado expone a la Repartición a riesgos potenciales como ataques de virus, compromiso de los sistemas, servicios de red y problemas legales.

2.0 Alcance

Esta política se aplica a los usuarios de cualquier sistema de información o infraestructura física, independientemente de su forma o formato, creado o utilizado para soportar la organización. Es responsabilidad del usuario leer y comprender esta política y realizar sus actividades de acuerdo con sus términos. Además, los usuarios deben leer y comprender la Política de seguridad de la información del Gobierno de la Provincia de Jujuy y sus estándares asociados.

3.0 Declaración de información

Excepto por cualquier privilegio o confidencialidad reconocido por la ley, las personas no tienen expectativas legítimas de privacidad durante el uso de los recursos de TI de la organización o de cualquier dato sobre esos recursos. Cualquier uso puede ser monitoreado, interceptado, grabado, leído, copiado, accedido o capturado de cualquier manera, incluso en tiempo real, y utilizado o divulgado de cualquier manera, por personal autorizado sin previo aviso adicional a las personas. Se realizará un monitoreo periódico de los sistemas utilizados, incluidos, entre otros: todos los archivos informáticos; y todas las formas de comunicación electrónica (incluidos correo electrónico, mensajes de texto, mensajería instantánea, teléfonos, sistemas informáticos y otros registros electrónicos). Además del aviso proporcionado en esta política, los usuarios también pueden ser notificados con un mensaje de texto de advertencia en los puntos de entrada del sistema donde los usuarios inician sesión para ser monitoreados y se les

puede recordar que no se permite el uso no autorizado de los recursos de TI de la Repartición.

El MPEyM puede imponer restricciones, sobre el uso de un recurso de TI en particular. Por ejemplo, el MPEyM puede bloquear el acceso a ciertos sitios web o servicios que no sirven para fines comerciales legítimos o puede restringir la capacidad del usuario para conectar dispositivos a los recursos de TI de la organización (por ejemplo, unidades USB personales, iPods, etc).

Los usuarios que accedan a las aplicaciones y recursos TI de la organización a través de dispositivos personales, sólo deberán hacerlo con la aprobación o autorización previa de la Repartición.

USO ACEPTABLE

Todos los usos de la información y los recursos de tecnología de la información deben cumplir con las políticas, estándares, procedimientos y directrices de la organización, así como con los acuerdos de licencia y las leyes aplicables, incluidas las leyes nacionales, provinciales y de propiedad intelectual.

Consistente con lo anterior, el uso aceptable de la información y los recursos informáticos comprende los siguientes deberes:

- Comprender los controles básicos de seguridad de la información necesarios para proteger la confidencialidad, integridad y disponibilidad de la información;
- Proteger la información y los recursos de la organización del uso o divulgación no autorizados;
- Proteger información personal, privado, sensible o confidencial procedente de uso o divulgación no autorizados;
- Observar los niveles autorizados de acceso y utilizar únicamente dispositivos o servicios de tecnología de TI aprobados; y
- Informar de inmediato sospechas de incidentes o brechas de seguridad de la información a la autoridad correspondiente, ya sea la Dirección de Ciberseguridad (DC), la Secretaría de Innovación Pública (SIP) o encargado de seguridad designado.

3.1 USO INACEPTABLE

La siguiente lista no pretende ser exhaustiva, pero es un intento de proporcionar un marco para las actividades que constituyen un uso inaceptable. Sin embargo,

los usuarios pueden estar exentos de una o más de estas restricciones durante sus responsabilidades laborales autorizadas, después de la aprobación de la autoridad correspondiente de la Repartición, en consulta con el personal de TI de la organización (por ejemplo, almacenamiento de material objetable en el contexto de un asunto disciplinario).

El uso inaceptable incluye, entre otros, lo siguiente:

- Uso o divulgación no autorizados de información personal, privada, sensible y/o confidencial;
- Uso o divulgación no autorizados de información y recursos de la Repartición;
- Distribuir, transmitir, publicar o almacenar cualquier comunicación, material o correspondencia electrónica que sea amenazante, obscena, acosadora, pornográfica, ofensiva, difamatoria, discriminatoria, provocativa, ilegal o intencionalmente falsa o inexacta;
- Intentar representar a la Repartición en asuntos no relacionados con los deberes o responsabilidades laborales autorizados oficialmente;
- Conectar dispositivos no aprobados a la red de la Repartición o cualquier recurso de TI;
- Conectar recursos de TI de la Repartición a redes no autorizadas;
- Conectarse a cualquier red inalámbrica mientras está físicamente conectado a la red cableada de la Repartición;
- Instalar, descargar o ejecutar software que no haya sido aprobado después de una revisión adecuada de seguridad, legal y/o de TI de acuerdo con las políticas de la Repartición;
- Conectarse a sistemas de correo electrónico externos (por ejemplo, Gmail, Hotmail, Yahoo) sin la aprobación previa de la Repartición (El gobierno de la Provincia debe reconocer el riesgo inherente al uso de servicios de correo electrónico externos, ya que el correo electrónico se utiliza a menudo para distribuir malware);
- Usar los recursos de TI de una organización para hacer circular solicitudes o anuncios no autorizados para fines no gubernamentales, incluidas entidades religiosas, políticas o sin fines de lucro;
- Proporcionar a terceros no autorizados, incluidos familiares y amigos, acceso a la información, los recursos o las instalaciones de TI de la organización;

- Usar información o recursos de TI de la Repartición para fines comerciales o personales, en apoyo de actividades “con fines de lucro” o en apoyo de otro empleo o actividad comercial externa (por ejemplo, consultoría remunerada, transacciones comerciales, etc);
- Propagar comunicaciones en cadena, correos masivos fraudulentos, spam u otros tipos de contenido de correo electrónico no deseado, utilizando recursos de TI de la organización; y
- Manipular, desconectar o eludir de otro modo los controles de seguridad de TI de la Repartición o de terceros.

3.2 USO PERSONAL OCASIONAL E INCIDENTAL

Se permite el uso personal ocasional, incidental y necesario de los recursos de TI, siempre que dicho uso: sea consistente con esta política; está limitado en cantidad y duración; y no impide la capacidad del individuo u otros usuarios para cumplir con las responsabilidades y deberes del Gobierno, incluidos, entre otros, el uso extensivo de ancho de banda, recursos o almacenamiento. Es importante ejercer buen juicio con respecto al uso personal ocasional e incidental. Las Reparticiones pueden revocar o limitar este privilegio en cualquier momento.

3.3 RESPONSABILIDAD INDIVIDUAL

Se requiere responsabilidad individual al acceder a todos los recursos de TI y la información de la Repartición. Todos son responsables de protegerse contra actividades no autorizadas realizadas con su ID de usuario. Esto incluye bloquear la pantalla de su computadora cuando se aleja de su sistema y proteger sus credenciales (por ejemplo, contraseñas, tokens o tecnología similar) contra divulgación no autorizada. Las credenciales deben tratarse como información confidencial y no deben divulgarse ni compartirse bajo ninguna circunstancia.

3.4 RESTRICCIONES A LA TRANSMISIÓN Y ALMACENAMIENTO DE INFORMACIÓN FUERA DEL SITIO

Los usuarios no deben transmitir información restringida de la organización, no pública, personal, privada, sensible o confidencial hacia o desde cuentas de correo electrónico personales (por ejemplo, Gmail, Hotmail, Yahoo) ni utilizar una cuenta de correo electrónico personal para realizar las labores de la Repartición a menos que estén autorizados explícitamente. Los usuarios no deben almacenar información restringida del Gobierno, no pública, personal, privada, sensible o confidencial en un dispositivo emitido por otra Entidad o con un servicio de

almacenamiento de archivos de terceros que no haya sido aprobado para dicho almacenamiento por la Provincia de Jujuy.

Los dispositivos que contienen información gubernamental deben estar atendidos en todo momento o asegurados físicamente y no deben ser registrados en los sistemas de equipaje de los transportistas.

3.5 RESPONSABILIDAD DEL USUARIO POR LOS EQUIPOS DE TI

A los usuarios se les asigna o se les da acceso rutinariamente a equipos de TI en relación con sus funciones oficiales. Este equipo pertenece a la Repartición y debe ser devuelto inmediatamente cuando lo solicite o en el momento en que un empleado sea desvinculado de la Repartición. Los usuarios pueden ser financieramente responsables del valor del equipo asignado a su cuidado si no se devuelve a la Repartición. En caso de pérdida, robo o destrucción de equipos informáticos, los usuarios deben proporcionar un informe escrito de las circunstancias que rodearon el incidente. Los usuarios pueden estar sujetos a medidas disciplinarias a instrumentarse en sumario administrativo. La Repartición tiene la discreción de no entregar dispositivos y equipos de TI a usuarios que pierdan o dañen repetidamente equipos de TI.

3.6 USO DE LAS REDES SOCIALES

El uso de sitios públicos de redes sociales para promover actividades gubernamentales requiere la aprobación previa por escrito de la máxima autoridad de la repartición con jerarquía no inferior a Director y notificación de las prohibiciones y responsabilidades al personal encargado de Comunicaciones. La aprobación queda a discreción de la autoridad y puede otorgarse previa demostración de una necesidad gubernamental y una revisión y aprobación de los términos del acuerdo de servicio por parte de la oficina de asesoría legal. La aprobación final debe definir el alcance de la actividad aprobada, incluida, entre otras, la identificación de los usuarios aprobados.

A menos que se autorice específicamente, está prohibido el uso de direcciones de correo electrónico gubernamentales en sitios públicos de redes sociales. En los casos en que los usuarios accedan a sitios de redes sociales en su propio tiempo utilizando recursos personales, deben ser sensibles a las expectativas de que se comportarán de manera responsable, profesional y segura con respecto a las referencias de la Repartición y al personal. Estas expectativas se describen a continuación.

a. Uso de las redes sociales en el ámbito de las funciones oficiales

La autoridad de la repartición con jerarquía no inferior a Director, debe revisar y aprobar el contenido de cualquier publicación de información pública, como comentarios de blogs, tweets, archivos de video o transmisiones, en sitios de redes sociales en nombre de la Repartición. Sin embargo, no se requiere la aprobación para publicaciones en foros públicos de soporte técnico, si la participación en dichos foros está dentro del alcance de las funciones oficiales del usuario, ha sido aprobada previamente por su supervisor y no incluye la publicación de ningún tipo de información confidencial, incluido detalles específicos de la infraestructura de TI. Además, no se requiere la aprobación para publicaciones en sitios privados de colaboración de redes sociales aprobados por la Repartición (por ejemplo, Yammer). Podrán concederse aprobaciones generales, según corresponda.

Las cuentas utilizadas para administrar la presencia de la Repartición en las redes sociales son cuentas privilegiadas y deben tratarse como tales. Estas cuentas son sólo para uso oficial y no deben utilizarse para uso personal. Las contraseñas de cuentas privilegiadas deben seguir los estándares de seguridad de la información, ser únicas en cada sitio y no deben ser las mismas que las contraseñas utilizadas para acceder a otros recursos de TI.

b. Pautas para el uso personal de las redes sociales

El personal debe ser consciente del hecho de que la información publicada en los sitios de redes sociales refleja claramente al individuo y también puede reflejar su vida profesional. En consecuencia, el personal debe actuar con discreción al publicar información en estos sitios y ser consciente de las posibles percepciones y respuestas a la información. Es importante recordar que una vez que la información se publica en un sitio de redes sociales, se puede capturar y utilizar de maneras no previstas originalmente. Es casi imposible retractarse, ya que a menudo permanece en copias, archivos, copias de seguridad y memoria caché.

Los usuarios deben respetar la privacidad del personal de la Repartición y no publicar ninguna información que identifique a ningún miembro del personal sin permiso (incluidos, entre otros, nombres, direcciones, fotografías, videos, direcciones de correo electrónico y números de teléfono). Los usuarios pueden ser considerados responsables de los comentarios publicados en los sitios de redes sociales.

Si un correo electrónico personal, una publicación u otro mensaje electrónico pudiera interpretarse como una comunicación oficial, se recomienda encarecidamente una exención de responsabilidad. Un descargo de

responsabilidad podría ser: “Los puntos de vista y opiniones expresados son los del autor y no reflejan necesariamente los del Gobierno de la Provincia”.

Los usuarios no deben utilizar sus cuentas personales de redes sociales para asuntos oficiales, a menos que lo autorice específicamente el Gobierno de la Provincia. Se desaconseja encarecidamente a los usuarios que utilicen las mismas contraseñas en su uso personal de los sitios de redes sociales que las utilizadas en dispositivos gubernamentales y recursos de TI, para evitar el acceso no autorizado a los recursos si la contraseña se ve comprometida.

4.0 Cumplimiento

Los empleados que incumplan esta política pueden estar sujetos a medidas disciplinarias, así como sanciones penales, civiles y/o administrativas si correspondieren. Los no empleados, incluidos, entre otros, los contratistas, pueden estar sujetos a la rescisión de acuerdos contractuales, a la denegación de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

5.0 Historial de revisiones

Esta política se revisará al menos una vez al año para garantizar su relevancia.

Fecha	Descripción de Cambio	Crítico
26/06/2024	Draft final del documento	Alejandro Castro Pablo Zalazar