

PROTOCOLO SOBRE “BUENAS PRÁCTICAS INFORMÁTICAS”

1. OBJETO

El Protocolo sobre “Buenas Prácticas Informáticas”, establece reglas a observar por los usuarios del Sistema de Gestión Documental Electrónica - GDE y de cualquier otro sistema informático utilizado en la gestión pública.

2.- ALCANCE

Se entiende por “usuarios” a empleados y funcionarios de la Administración Pública Provincial centralizada, descentralizada, autárquica, empresas y sociedades del estado.

3.- PAUTAS DE COMPORTAMIENTO

Conducta acorde: Los empleados y funcionarios deberán ajustar su comportamiento a las responsabilidades de la función asignada, considerando los objetivos constitucionales y legales que el Estado Provincial tiene hacia la ciudadanía.

Confidencialidad y uso de la información Debe guardar estricta discreción con respecto a todos los datos o información de los cuales tenga conocimiento con motivo o en ocasión del ejercicio de sus tareas, haya sido calificado o no como confidencial por el superior. Solo puede brindar información al interesado cuando legalmente corresponda.

4. SEGURIDAD: quien resulte habilitado como usuario, deberá

4.1 Contraseñas:

- Utilizar una contraseña segura, evitando el uso de nombres propios, fechas de nacimiento o palabras comunes.
- Cambiar la contraseña periódicamente.
- No compartir las contraseñas con nadie.

4.2 Software

- No instalar software ni programas. En caso de ser necesario y por la causa que fuera, previamente deberá:

4.2 A: informar la necesidad al superior jerárquico, quien solicitará al área informática:

- a) un informe técnico del tipo de licencia y funcionalidades;
- b) si el software es necesario para el cumplimiento de funciones y objetivos de esa Unidad de Organización.

4.2. B: el titular de la Unidad de Organización dictará Resolución fundada (aprobando o rechazando la instalación). En caso de aprobarse la instalación del software, deberá informarse al Ministerio de Planificación Estratégica y Modernización – Dirección de Conectividad y Comunicación.

4.3 Correo electrónico

- Cada Unidad de Organización del Estado Provincial, debe informar al Ministerio de Planificación Estratégica y Modernización – Dirección de Infraestructura de Conectividad y Comunicación, altas y bajas de correos oficiales de sus dependencias; el listado oficial de correos electrónicos es público por razones de transparencia activa.
- Los usuarios no abrirán correos electrónicos cuyos remitentes no figuren en el listado oficial mencionado en el apartado anterior.
- Solo se abrirán los correos que correspondan a los interesados del trámite, o de instituciones que hubieran firmado convenio de comunicación digital (Dec. 9630-PEYM-2023).
- No hacer clic en enlaces o descargar archivos adjuntos de correos electrónicos sospechosos.
- Estar atentos y rechazar los correos electrónicos de phishing que intentan suplantar la identidad.

4.4 Navegación web

- Cuando en el ejercicio de la actividad laboral sea necesario obtener datos o referencias para ser aplicados o utilizados en trámites administrativos, el usuario solo podrá visitar o navegar sitios web oficiales del Estado Provincial, Nacional y provincias;
- No descargar archivos de sitios web inseguros o desconocidos.

5. Eficiencia

5.1 Organización de archivos

- Conservar los archivos utilizados en trámites administrativos, en una estructura de carpetas organizada por año y mes.
- Utilizar nombres suficientemente descriptivos para los archivos que permita identificar fácilmente su contenido, indicando en el comienzo el número del expediente administrativo.
- Hacer copias de seguridad de los archivos importantes.

5.2 Uso del correo electrónico

- Utilizar el correo electrónico asignado para realizar solo los trámites administrativos oficiales.
- No enviar correos electrónicos masivos no solicitados (spam).

5.3 Uso de Internet

- Utilizar Internet de forma responsable y productiva, y solo para los trámites administrativos oficiales.

6. Disponibilidad

6.1 Cuidado de los equipos informáticos

- No comer ni beber cerca de los equipos informáticos.
- No exponer los equipos informáticos a temperaturas o humedades extremas.
- Apagar los equipos informáticos de forma correcta.

6.2 Copias de seguridad

- Realizar copias de seguridad de los archivos importantes de forma regular.
- Almacenar las copias de seguridad en un lugar seguro.

6.3 Mantenimiento preventivo

- Requerir al área informática la realización de mantenimiento preventivo de los equipos informáticos en forma periódica.
- No intentar reparar los equipos informáticos; requerir siempre la intervención del área técnica.

7. Responsabilidades

Todos los usuarios de las distintas Unidades de Organización son responsables de cumplir con las buenas prácticas informáticas establecidas en este protocolo.

8. Revisión y actualización

Este protocolo será revisado y actualizado de forma periódica para adaptarlo a nuevas necesidades.

Aprobado por Resolución 41-PEyM-24.-