DONAR ÓRGANOS
ES SALVAR VIDAS

"EL RÍO ATUEL TAMBIÉN
ES PAMPEANO"

"2022 - LAS MALVINAS
SON ARGENTINAS"

PROVINCIA DE LA PAMPA

Ministerio de Conectividad y Modernización

SANTA ROSA, 27 OCT 2022

VISTO:

El Expediente N° 13917/22 caratulado: "MINISTERIO DE CONECTIVIDAD Y MODERNIZACION - SUBSECRETARIA DE TECNOLOGIAS, CONOCIMIENTO E INNOVACION - S/POLITICA DE CONTRASEÑAS"; y

CONSIDERANDO:

Que la Ley N° 3170 establece en su artículo 24 que este Ministerio de Conectividad y Modernización estará facultado a: *"...17) Implementar herramientas y políticas de seguridad informática tendientes a garantizar la confidencialidad de la información generada en el ámbito de su competencia..."*;

Que el Plan Estratégico de Modernización e Innovación de la Administración Pública Provincial, aprobado por Decreto N° 2431/20 establece entre sus Lineamientos Estratégicos: *"...4. Seguridad de la Información- Ciberseguridad. Definir, implementar y auditar la aplicación de una arquitectura de ciberseguridad para toda la Administración Pública Provincial y en particular para las Infraestructuras Críticas y las Infraestructuras de Información Críticas; por medio normas, procedimientos y controles destinados a proteger los activos de información propios y/o administrados por el Estado Provincial, basados en los principios de Confidencialidad, Integridad y Disponibilidad, en un todo de acuerdo a los objetivos del Gobierno, la legislación vigente, estándares nacionales e internacionales, y recomendaciones de las buenas prácticas reconocidas"*;

Que igualmente, entre las acciones del Objetivo Específico 4.1 del mencionado Plan se encuentra la de: *"... 4.1.5. Proponer la normativa necesaria destinada a la protección de los activos de información del Estado Provincial"*;

Que asimismo, el artículo 3° del mencionado Decreto designa como Autoridad de Aplicación a este Ministerio;

Que en función de lo expuesto, a fojas 3/6 la Subsecretaría de Tecnologías, Conocimiento e Innovación conjuntamente con la Dirección de Cyberseguridad ha elaborado la propuesta de una Guía de Buenas Prácticas a fin de propiciar la gestión y utilización segura de las contraseñas de acceso a todos los servicios, sistemas de información y sitios web de la Administración Pública Provincial, Entes Autárquicos y Descentralizados;

Que la mencionada propuesta tiene como documento de referencia la Norma ISO/IEC 27001 sobre seguridad de la información;

Que en consecuencia corresponde proceder a la definición y aprobación de una Guía de Buenas Prácticas de Contraseñas, como parte de un marco más amplio de control de acceso a la información y a las instalaciones de procesamiento de información;

Que la misma permitirá avanzar en el perfeccionamiento de un marco integral que establezca que los usuarios deben tener acceso controlado por un procedimiento de inicio seguro y restringido;

Que ha tomado intervención la Delegación de Asesoría Letrada de Gobierno actuante

//

//2.-

ante este Ministerio;

Que corresponde dictar el presente acto administrativo;

POR ELLO:

EL MINISTRO DE CONECTIVIDAD Y MODERNIZACIÓN

RESUELVE:

Artículo 1°.- Apruébase la Guía de Buenas Prácticas de Contraseñas para los agentes de la Administración Pública Provincial, Entes Autárquicos y Descentralizados, que como Anexo forma parte integrante de la presente Resolución.

Artículo 2°.- Regístrese, comuníquese y publíquese.

RESOLUCIÓN Nº 112 /22.-

PROVINCIA DE LA PAMPA * Ministerio de Conectividad y Modernización *

ABOG. ANTONIO CURCIARELLO
Ministro de Conectividad
y Modernización

PROVINCIA DE LA PAMPA
Ministerio de Conectividad y Modernización

ANEXO

Guía de Buenas Prácticas de Contraseñas

1. **Objetivo, alcance y usuarios**
   El objetivo de la presente Guía de Buenas Prácticas de Contraseñas es establecer los lineamientos que propicien la gestión y utilización segura de las contraseñas de acceso de los agentes de la Administración Pública Provincial, Organismos Descentralizados y Entes Autárquicos a los servicios, sistemas de información y sitios web provistos.

2. **Características recomendadas para una contraseña**
   - Secreta: la contraseña sólo debe ser conocida por su propietario.
   - Intransferible: la contraseña no debe ser revelada a ningún tercero para su uso.
   - Modificable sólo por el titular: el cambio de contraseña, sea cual fuere el motivo, debe ser realizado por su propietario. Sólo podrá ser restablecida por el administrador cuando el usuario la hubiera olvidado o si estuviera en riesgo la seguridad de la administración, como en el caso de que se detecte como comprometida. Se debe llevar registro en cualquiera de los dos casos.
   - Formato mínimo que debiera cumplir una contraseña:
     - Contener al menos ocho caracteres.
     - Contener al menos un carácter numérico.
     - Contener al menos un carácter alfabético en mayúscula y uno en minúscula.
     - Contener al menos un carácter especial.

3. **Responsabilidad de los usuarios**
   Se establecen los siguientes lineamientos en cuanto a la elección y uso de contraseñas:
   - El usuario es responsable de elegir una contraseña que no pueda ser descifrada fácilmente, de acuerdo a lo siguiente:
     - La contraseña elegida debe estar de acuerdo con lo especificado en el punto 3 a fin de que la misma no sea obtenida fácilmente.
     - Se aconseja establecer una nueva contraseña cada 6 meses, o bien, cuando el sistema lo solicite. No se podrán utilizar nuevamente las últimas tres contraseñas.
     - Una clave no debiera ser solo una palabra que se encuentre en el diccionario, en un dialecto o jerga de ningún idioma; como tampoco ninguna palabra escrita en forma inversa.
     - Se recomienda que las contraseñas no estén relacionadas con datos personales (por ejemplo: fecha de nacimiento, domicilio, nombre de un familiar).
     - Las contraseñas no deben ser almacenadas en un sistema de registro automatizado (por ejemplo: macros o navegador).
     - No utilizar las mismas contraseñas personales para fines privados y para fines laborales.
     - No revelar la contraseña a ninguna persona.
     - Las contraseñas de acceso no deben ser divulgadas a terceros por ningún medio.
     - Las contraseñas deben ser cambiadas a la brevedad, si existen indicios de que puedan estar comprometidas.

3.1. **Gestión de las contraseñas de acceso.**
Cuando se asignan y utilizan contraseñas de acceso, se aconseja tener en cuenta lo

//

//2.-

siguiente:

- Cada usuario tendrá la posibilidad de escoger su propia clave.

- Los sistemas de gestión de identidades validarán que las contraseñas cumplan con lo especificado en el punto 3.
- Las contraseñas de primer acceso generadas manualmente por un administrador, se establecerán como vencidas para que el usuario las modifique en el primer ingreso. Deben ser comunicadas al usuario de forma segura y se debe verificar previamente la identidad del usuario.
- De forma automática, los sistemas marcarán la contraseña como vencida cada 6 meses. En ese momento, el usuario debe poder establecer su nueva contraseña. No se podrán utilizar nuevamente las últimas tres contraseñas. Siempre que sea factible, el sistema deberá informar al usuario de la proximidad del vencimiento.
- Si el usuario solicita una nueva clave, el sistema de gestión de identidades debe determinar la identidad del usuario, siguiendo el procedimiento establecido.
- El usuario debe confirmar la recepción de la clave siguiendo el procedimiento establecido por el administrador del sistema.
- La contraseña no debe ser visible en la pantalla durante el inicio de sesión.
- Si un usuario ingresa una clave incorrecta un número determinado de veces consecutivas, el sistema debe bloquear la cuenta de usuario en cuestión. El número de veces a determinar dependerá del criterio del administrador del sistema de gestión de identidades.
- Las contraseñas creadas por el fabricante del software o hardware deben ser cambiadas durante la instalación inicial.
- Los archivos que contienen contraseñas deben ser guardados en forma separada de los datos de sistema de la aplicación.
- Las contraseñas deben almacenarse encriptadas y residir en archivos protegidos.
- La transmisión de contraseñas de acceso por cualquier medio, se realizará de forma segura, utilizando cifrado de extremo a extremo.
- Se utilizará al menos autenticación de dos factores para todos los activos de información identificados con el máximo nivel de criticidad. Para el resto de los niveles es opcional, a requerimiento del propietario.

ANEXO RESOLUCION Nº 112 /22.-

PROVINCIA DE LA PAMPA
Ministerio de Conectividad y Modernización

ABOG. ANTONIO CURCIARELLO
Ministro de Conectividad
y Modernización