# DOCUMENTO DE GESTIÓN

## Proyecto: Proyecto de Mejoramiento y Ampliación de los Servicios de Soporte para la Provisión de los Servicios a los Ciudadanos y Empresas a Nivel Nacional - SGSI

**Versión: 1.0**

| Registro de Cambios | | | | |
|---|---|---|---|---|
| **Versión** | **Páginas** | **Fecha** | **Descripción** | **Autor** |
| 1.0 | 5 | 08-03-2022 | Versión inicial | Andrés Cómina Jara |

| Control documental | | |
|---|---|---|
| | **Preparado y revisado por** | **Aprobado por** |
| **Nombre**<br>**Rol** | Andrés Cómina Jara<br>Responsable del SGSI de la PNGD | Manuel Humberto Valdera García<br>Subsecretario (e) de la Subsecretaría de Tecnología y Seguridad Digital |
| **Fecha** | 08-03-2022 | 10-03-2022 |

**ÍNDICE**

## 1. INTRODUCCIÓN

El objetivo de crear la política de seguridad de la información en relación al uso de contraseñas seguras, para la Plataforma Nacional de Gobierno Digital (PNGD), en la Secretaría de Gobierno y Transformación Digital (SGTD), dentro de la Presidencia del Consejo de Ministros (PCM), es establecer los compromisos y el marco general (legal y regulatorio) para gestionar los riesgos asociados al uso de contraseñas débiles y/o que han sido comprometidas y se utilizan para el acceso a los activos de información como parte de la prestación de los servicios ofrecidos a fin de minimizar los riesgos de seguridad de la información y prevenir las amenazas.

## 2. DEFINICIONES

**Autenticación:** Es el proceso que consiste en verificar que el usuario es quién dice ser.

**Acceso:** Es la consecuencia de una autenticación positiva.

**Activos de información**: Todo aquello que es o contiene información que es de valor para la PNGD. Por ejemplo: documentos digitales o físicos, servicios, aplicaciones, equipos, entre otros activos que la organización valora y protege de cualquier vulnerabilidad que amenaza con la divulgación, indisponibilidad y pérdida de integridad de la información.

**Amenazas:** Evento que puede afectar adversamente la operación de las empresas y sus activos de información, mediante el aprovechamiento de una vulnerabilidad.

**Contraseña:** También denominada clave, es una forma de autenticación para controlar el acceso hacia algún recurso informático, ya sea un archivo, un programa o un equipo.

**Credencial:** Conjunto de datos que incluye la identificación y prueba de identificación que se utiliza para obtener acceso a recursos locales y de red.

**Parte interesada:** Persona u organización que puede afectar, verse afectada o percibirse como afectada por las decisiones o actividades que realiza la PNGD. Por ejemplo: trabajadores de la PNGD, trabajadores de proveedores contratados por la PNGD, entre otros.

**Registro:** Un documento que se puede usar como evidencia.

**Resetear:** Reinicio o reposición al estado inicial.

**Seguridad de la información:** Es la preservación de la confidencialidad, integridad y disponibilidad de los activos de información.

**Riesgos:** Las amenazas de ataques y las vulnerabilidades de la tecnología.

## 3. ALCANCE

Las disposiciones de este documento son de aplicación obligatoria para las partes interesadas, las instalaciones y los activos de información involucrados en la prestación de los servicios ofrecidos por la PNGD.

## 4. OBJETIVOS

a) Definir y formalizar una política alineada a los marcos legales o regulatorios (contrato entre la PNGD y los clientes y proveedores de esta), que ayudarán a la PNGD a mitigar los riesgos de seguridad de la información en la relación al establecimiento y uso adecuado de contraseñas empleadas para el acceso a los activos de la información.

b) Establecer compromisos con la finalidad de monitorear el establecimiento y uso adecuado de contraseñas seguras durante la ejecución de los servicios que brinda la PNGD, a fin de minimizar riesgos de seguridad de la información y prevenir las amenazas sobre los activos de información.

## 5. POLÍTICA DE USO DE CONTRASEÑAS SEGURAS

La Presidencia del Consejo de Ministros (PCM), a través de la Secretaría de Gobierno y Transformación Digital (SGTD), realiza la gestión de la seguridad de la información en la relación al uso de contraseñas seguras como parte de la gestión eficiente de la seguridad de la información, la mitigación de los riesgos de seguridad de la información asociado a los activos de información que requieran el uso de contraseñas para su utilización, a fin prevenir pérdida, copia y/o modificación de la información en la PNGD.

Para garantizar el uso de contraseñas seguras, la SGTD asume los siguientes compromisos:

1. Difundir la política de uso de contraseñas seguras.

2. Determinar una persona responsable en la PNGD encargado de asignar inicialmente a las partes interesadas una contraseña para el uso de activos de información a los cuales tenga permitido el acceso.

3. Realizar el cambio durante la primera autenticación por cada parte interesada que recibe una contraseña.

4. Activar, cuando esté disponible, la configuración que obligue a toda parte interesada que posee una contraseña, a cambiar la misma durante la autenticación realizada posterior a la creación y/o reseteo de la contraseña.

5. Establecer criterios para la creación de contraseñas que consideren un tamaño mínimo, combinación de caracteres (mayúscula, minúscula, números y caracteres especiales), cantidad de caracteres iguales que se pueden repetir de manera sucesiva, que previamente no se hayan utilizado en un número determinado de oportunidades y que no se parezcan a las utilizadas previamente.

6. Establecer tiempo de vigencia de la contraseña.

7. Solicitar de manera obligatoria la creación de una nueva contraseña, cada vez que ésta ha cumplido con su tiempo de vigencia.

8. Concientizar a las partes interesadas sobre los criterios que deben tener en consideración para la creación de la contraseña, para no compartir y/o divulgar las contraseñas propias o de otras partes interesadas.

9. Establecer un número mínimo de intentos de uso de una contraseña. Luego de esto el uso de la credencial asociada a la contraseña quedará bloqueado de manera temporal o definitiva según lo establecido por PNGD.

10. Prohibir el acceso a los activos de información con una cuenta diferente a la asignada.

11. Prohibir el uso de contraseñas similares para uso de cuentas de las partes interesadas.

12. Registrar y monitorear los intentos de accesos exitosos y fallidos de autenticación.

13. Documentar todas las excepciones que se hayan aprobado al cumplimiento de la presente política.