intiza

Norma de Gestión de Contraseñas

Versión: 3.1

Confeccionó	Revisó	Aprobó
Horacio Pasandi Consultoría Externa	 Carla Leiva - CISO	 Francisco Canale - Director

NORMA DE GESTIÓN DE CONTRASEÑAS	intiza Clasificación: Restringida
Tipo: Norma	Fecha vigencia: 13/11/2025
Código: NO-SI-03- Gestión de Contraseñas	Versión: 3.1

Contenido

1. Objetivo

Definir y establecer los lineamientos generales para la Gestión de Contraseñas de acceso que utilizan los usuarios de INTIZA.

2. Alcance

Esta norma involucra a todas las personas que realicen cualquier actividad para INTIZA, como los empleados efectivos, personal pasante, contratado, tercerizados o cualquier otra modalidad de empleo directa o indirectamente que pudiera generar un vínculo laboral.

En esta norma se encuentra la Gestión de Contraseñas de todas las cuentas utilizadas para tener acceso a información de INTIZA.

3. Responsabilidades

Seguridad de la Información es responsable de mantener y verificar que se cumplan los lineamientos de gestión de contraseñas.

Todos los **Colaboradores** son responsables de cumplir con los lineamientos establecidos en esta norma e incorporarlos a hábitos cotidianos.

4. Desarrollo

4.1. Autenticación

La contraseña de autenticación debe tener las siguientes características:

- Debe ser definida con una longitud mínima de 8 (ocho) caracteres.
- Combinar letras mayúsculas y minúsculas, incluir números, caracteres no estándar (ñ, $, % ë â...).
- No utilizar terminología técnica conocida (admin).

- No debe incluir secuencias ni caracteres repetidos. Cadenas como "12345678", "222222", "abcdefg" o el uso de letras adyacentes en el teclado no ayudan a crear contraseñas seguras.
- No deben vincularlas a una característica personal (teléfono, D.N.I., patente del automóvil, etc.).
- No se deben utilizar palabras comunes ni nombres de fácil deducción por terceros (nombre de mascota, hijos, etc.).
- No debe ser identificable durante la transmisión e ilegible en el almacenamiento.
- Las contraseñas para usuarios nuevos o que se solicite bajo autorización correspondiente blanqueo de clave, deberá configurarse con un valor único para cada uno y el usuario deberá cambiarla obligatoriamente la primera vez que ingrese al sistema.
- Debe cambiarse obligatoriamente en un período máximo de 90 (noventa) días, debiendo el sistema solicitar automáticamente el cambio de esta al cumplirse este período.
- La nueva contraseña debe ser distinta a, por lo menos, las últimas 4 (cuatro) contraseñas y no se debe permitir el cambio de esta hasta pasado 1 (un) día, a menos que sea solicitado formalmente como una excepción de Seguridad.
- Toda vez que el sistema solicite un cambio de contraseña, debe ingresar la confirmación de la contraseña anterior y de la nueva, siempre que la plataforma lo permita.
- Debe permanecer cifrada en archivos ocultos y protegidos, siempre que el sistema lo permita.
- No debe ser visible por pantalla al momento de ser ingresada.

4.2. Autorización

- Duración del bloqueo de cuenta: Siempre bloqueada la cuenta, la misma será desbloqueada por un administrador.
- Restablecer recuentos de bloqueo de cuentas tras 24 horas.

- Desconexión automática de la sesión de usuario en la aplicación y en la red por tiempo de inactividad a los 15 (quince) minutos.
- Bloqueo permanente de la cuenta del usuario ante 3 (tres) intentos de acceso fallidos.
- Todos los sistemas deben requerir y autenticar un identificador de usuario y contraseña o token válido previo a conceder el acceso a la red o a los recursos de la empresa.

4.3. Segregación de Funciones

- Cada usuario será responsable del Id y contraseñas asignadas.
- Las contraseñas serán secretas y sólo conocidas por sus usuarios asignados.
- Las contraseñas correspondientes a los nuevos identificadores de usuario deben expirar en el primer inicio de sesión y deberán ser cambiadas en forma inmediata sólo por el usuario dueño del identificador de usuario correspondiente.
- El identificador de usuario y la contraseña no deben ser escritas en el computador o guardadas en los scripts de acceso para un login automático, o de cualquier otra manera que permita a personas no autorizadas acceder a las redes y sistemas.

4.4. Auditoría y Control

Todos los sistemas deben registrar y guardar la fecha y hora de todos los cambios de contraseña, sean estos exitosos o fallidos.

5. Referencias

5.1. Normativa Relacionada

Categoría	Título	Código
Política	Seguridad de la Información	PO-SI-01
Norma	Gestión de Cuentas de Usuarios	NO-SI-02

5.2. Definiciones

Término	Descripción
Login	Proceso que controla el acceso individual a un sistema informático mediante la identificación del usuario utilizando credenciales provistas por el usuario.
Carácter Especial	Es una unidad de información que corresponde con un grafema o con una unidad o con un símbolo (ej.: @, * , # , _ , -).
Autenticación	Es el proceso que debe seguir un usuario para tener acceso a los recursos de un sistema o de una red de computadoras. Este proceso implica identificación.
Script	secuencia de comandos o guión es un término informal que se usa para designar a un programa relativamente simple.

6. Historial de Versiones

Versión	Fecha	Resumen de Cambios
1.0	10/08/2021	Creación de la Norma de Gestión de Contraseñas.
1.0	28/10/2021	Aprobado por Comité de Dirección: MI-DI-01- Minuta de Comité de Dirección N° 1.

2.0	07/09/2022	Revisión y confirmación de vigencia de los lineamientos definidos.
2.0	11/10/2022	Aprobado por Comité de Dirección: MI-DI-06- Minuta de Comité de Dirección N° 6.
3.0	08/06/2023	Se aclaró la política completa de contraseña a aplicar (longitud, nivel de complejidad, etc.).
3.0	12/06/2023	Aprobado por el Comité de Seguridad.
3.1	10/11/2025	Se agregaron las responsabilidades del colaborador y se actualizó el formato del documento.
3.1	13/11/2025	Aprobado por el Comité de Seguridad.