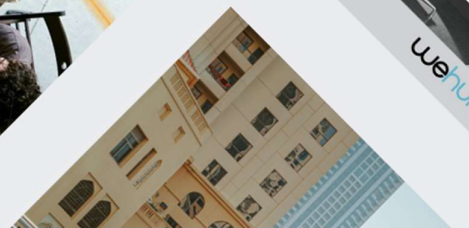
ABAI CX Digital Management

Política de Gestión de Contraseñas

13 de Mayo 2024

www.abaigroup.com



Control de cambios

Realizado	Cargo:	Responsable CTSO
	Nombre:	Samuel Payano Castañeda
	Fecha:	2024-04-22
Revisado	Cargo:	Gerente de Infraestructura y TI
	Nombre:	Alexis Roman
	Fecha:	2024-04-22
Aprobado	Cargo:	Director General
	Nombre:	Juan Diego De Lavalle
	Fecha:	2024-05-13

Registro de Cambios			
Versión	**Fecha**	**Descripción del cambio**	**Autor del cambio**
1.0	2024-05-13	Primer Documento	*Samuel Payano* *Responsable de CTSO*

ÍNDICE

Este documento contiene información propiedad de ABAI PERÚ. Los materiales, ideas y conceptos contenidos en este documento no deberán ser divulgados fuera de su organización o utilizados con propósitos distintos a los mencionados. No está permitido su reproducción total o parcial ni su uso con otras organizaciones para ningún otro propósito, excepto autorización previa por escrito.

1. Objeto

El objetivo de esta política es definir los estándares para la protección, creación y eliminación de contraseñas para ABAI Perú.

Establecer, difundir y verificar el cumplimiento de buenas prácticas en el uso de contraseñas para los usuarios estándar y para los usuarios con privilegios de administrador de los diferentes sistemas de información.

Esta política gobierna la interacción entre todo los activos y recursos, para todas las áreas de ABAI Perú que incluye sistemas operativos, software de aplicaciones, hardware de cómputo, redes y servicios en la nube, para todo equipo manejado por ABAI Perú (de propiedad, bajo arrendamiento) o donde resida datos de ABAI Perú.

2. Ámbito de Aplicación

Esta política aplica a Colaboradores y Proveedores de ABAI Perú, siempre que se maneje información y use infraestructura y/o servicios de tecnología.

El alcance de los lineamientos que se definen en esta política da cubrimiento a los accesos que involucren:

- Bases de datos.
- Aplicativos.
- Sistemas de información.
- Elementos de infraestructura tecnológica (Firewall, Router, Switch).
- Equipos de cómputo.

Estos deberán preservar la confidencialidad de la información de ABAI Perú, los cuales están sujetos a los mismos requerimientos de seguridad, y tienen las mismas responsabilidades de salvaguardar la información; así como están obligados a continuar protegiendo y cumpliendo los acuerdos de confidencialidad durante y una vez terminada su relación laboral y/o contractual con ABAI Perú.

3. Definiciones

- **Colaborador:** Se refiere a directores, gerentes, o empleados permanentes o temporales y practicantes que forman parte de ABAI Perú.
- **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.
- **Proveedor:** Personas e instituciones con las cuales ABAI Perú mantiene vínculos comerciales, contractuales o empresariales e incluye en sentido amplio a los proveedores, contratistas, prestadores de servicios, consultores, subcontratistas, asesores, agentes, distribuidores, socios comerciales, etc.

- **TI:** Tecnología de la Información.

4. Responsabilidades

Responsable	Funciones
Gerente de Infraestructura y TI	• Administrar y proporcionar la contraseña para las diferentes plataformas y sistemas.
Responsable CTSO	• Supervisar el cumplimiento de la presente Política y elabora mejoras.
Usuario	• Dar cumplimiento a lo establecido en esta política. Aplica para personas que tienen asignado un equipo de cómputo y/o escritorio de trabajo.

5. Documentación de Referencia

- ISO 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad.

6. Desarrollo

- Asegurar de que haya una correcta administración de autenticación de usuarios para usuarios y administradores en todos los componentes del sistema y que se use, al menos, uno de los siguientes métodos para autenticar todos los usuarios:
    - Algo que el usuario sepa, como una contraseña o frase de seguridad
    - Algo que el usuario tenga, como un dispositivo token o una tarjeta inteligente
    - Algo que el usuario sea, como un rasgo biométrico.
- El administrador de cada sistema de información es responsable de asegurar que se solicite las credenciales de acceso (usuario y contraseña) para permitir el acceso.
- El administrador de cada sistema es responsable de asegurar que el mismo solicite cambio de contraseña cada vez que esta es reestablecida manualmente a un usuario.
- El colaborador es responsable de asegurar la privacidad de las contraseñas asignadas para acceder a los sistemas de información.
- Las credenciales de acceso para los diferentes sistemas de información son personal e intransferible.

- El administrador de cada sistema es responsable de asegurar que las contraseñas que se transmitan a través de redes públicas estén protegidas contra acceso no autorizado mientras se encuentren en tránsito.
- El usuario de los sistemas de información es responsable de establecer una contraseña segura, que cumpla con las siguientes características:
    a) El administrador del sistema debe utilizar contraseñas diferentes como usuario y como administrador.
    b) Si hay indicios para creer que una contraseña ha sido comprometida, debe cambiarse inmediatamente.
    c) No deben usarse contraseñas que sean idénticas o substancialmente similares a contraseñas previamente empleadas. Siempre que sea posible, debe impedirse que los usuarios vuelvan a usar contraseñas anteriores, esto se debe gestionar desde el sistema que asigne las credenciales.
    d) Es responsabilidad del administrador de cada sistema establecer los mecanismos para que la contraseña asignada al usuario le sea transmitida de la manera más confidencial posible.
    e) No se debe escribir la contraseña en papeles y dejarla en sitios donde pueda ser encontrada por terceros.
    f) No se debe almacenar la contraseña en la computadora. Algunos cuadros de diálogo o ventanas emergentes de los navegadores presentan una opción para guardar o recordar la contraseña; no debe seleccionarse esa opción.
    g) Las aplicaciones deben almacenar las contraseñas en forma cifrada.
    h) Las contraseñas predefinidas que traen los equipos y aplicaciones deben cambiarse inmediatamente al ponerse en operación.
    i) Las contraseñas deben cambiarse cuando una persona que tiene acceso a cuentas privilegiadas compartidas ya no es parte de la entidad como colaborador.
    j) Las credenciales asociadas a un usuario que se encuentre en vacaciones deberán ser inactivadas durante el periodo de vacaciones del colaborador.
- En caso de utilizar autenticación SSO (Single Sign On), para dos o más sistemas de información como es el caso del acceso al equipo de cómputo y el paquete de office 365 (Outlook, correo, Skype), las contraseñas deben cumplir los numerales mencionados con anterioridad.
- Para los administradores de los sistemas de información, aplicaciones, equipos de infraestructura tecnológica, bases de datos se recomienda la creación de un usuario alterno o de contingencia con los privilegios mínimos de administración.
- Cada vez que se realicen los cambios de las credenciales de acceso de las bases de datos, sistemas de información o aplicativos, elementos de infraestructura tecnológica, deben informados al Gerente de Infraestructura y TI.

- El administrador de cada sistema es responsable de eliminar los usuarios por defectos que se generan inicialmente en todo sistema.
- El usuario es responsable de bloquear su equipo en el momento en que se retire de su puesto de trabajo a una zona donde pierda visibilidad de este.
- Los criterios para la elaboración de las contraseñas serán:
  - Longitud mínima de la contraseña: 8 caracteres
  - No podrá contener el nombre de cuenta del usuario, el email, el nombre completo o partes del nombre completo del usuario (nombre o apellidos).
  - Deberá de incluir caracteres de tres de las siguientes categorías:
    - Mayúsculas (de la A a la Z)
    - Minúsculas (de la a a la z)
    - Dígitos de base 10 (de 0 a 9)
    - Caracteres especiales no alfanuméricos (por ejemplo: !, $, #, %)
- Todas las contraseñas del sistema (cuentas de administrador, cuentas de administración de aplicaciones, interacciones críticas, etc.), deberán cambiarse con una periodicidad de al menos una vez en el rango de 45 a 60 días.

7. Registros

- PS-IT-GIF-PLL-002S_PER Acta de Entrega Usuario y Contraseña.

8. ANEXOS

- N/A