

	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
	Política de Contraseñas seguras para Safe Comercial	
VIGENCIA: 25/06/2024	VERSIÓN: 1	Pag 1 de 3

Este documento presenta una política sencilla y clara para la creación y gestión de contraseñas seguras en Safe Comercial. Está alineada con la norma internacional ISO 27001 para asegurar el manejo adecuado de accesos a sistemas críticos. Aquí encontrará los requisitos mínimos de contraseña, directrices para su almacenamiento, procedimientos para cambios regulares y el uso de autenticación multifactor, entre otros aspectos esenciales para proteger la información corporativa. Este material es clave para prepararse ante la auditoría que tendrá lugar próximamente.

1. Requisitos Mínimos de Contraseña

Para garantizar un nivel óptimo de seguridad acorde a ISO 27001, Safe Comercial establece que todas las contraseñas deben poseer una longitud mínima de 12 caracteres. Esta medida supera la recomendación básica de la norma, reforzando la protección contra intentos de acceso no autorizados.

Las contraseñas deben incluir, sin excepción, al menos una letra mayúscula y una minúscula, un número y un símbolo. Los símbolos aceptados abarcan una amplia variedad, tales como: **!@#\$%^&*() +=-`~[]{}|;':",./<>?**. Esto ayuda a incrementar la complejidad y reduce la vulnerabilidad frente a ataques automatizados.

Está prohibido emplear palabras comunes del diccionario, nombres propios o cualquier información personal que facilite la predicción o ingeniería social. Además, Safe Comercial utiliza una herramienta automatizada para verificar la complejidad de la contraseña durante su creación y cambios futuros, asegurando el cumplimiento estricto de estos criterios.

2. Gestión y Almacenamiento de Contraseñas

Para proteger la integridad de las credenciales, Safe Comercial prohíbe estrictamente compartir contraseñas entre usuarios o terceros. Cada usuario debe ser responsable exclusivo de la confidencialidad de sus datos de autenticación.

No se permite registrar contraseñas en medios inseguros como papeles físicos, documentos sin cifrado o correos electrónicos que no cuenten con protección adecuada. Esta prohibición busca minimizar riesgos de accesos no autorizados por pérdida o robo de dichas anotaciones.

Safe Comercial recomienda y aprueba el uso del gestor de contraseñas **Lastpass**, que ofrece funcionalidades como generación automática de contraseñas seguras, almacenamiento cifrado y sincronización entre dispositivos. Más información sobre esta herramienta está disponible en su página oficial: <https://www.lastpass.com/es/features/password-generator>.

Cambios de Contraseña

La política requiere que todos los usuarios cambien sus contraseñas de forma obligatoria cada 90 días para mantener un nivel adecuado de seguridad. Este periodo está alineado con

	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
	Política de Contraseñas seguras para Safe Comercial	
VIGENCIA: 25/06/2024	VERSIÓN: 1	Pag 2 de 3

las mejores prácticas de la industria y contribuye a limitar el riesgo de accesos prolongados no autorizados.

Si existe sospecha de que una contraseña ha sido comprometida, el cambio debe realizarse de manera inmediata para evitar incidentes de seguridad. Además, no se permitirá la reutilización de las últimas 12 contraseñas usadas, forzando así una renovación constante y aumentando la dificultad para los atacantes.

Los usuarios recibirán un recordatorio automático 15 días antes de la fecha límite para cambiar su contraseña, facilitando el cumplimiento proactivo y evitando bloqueos por caducidad. Esta medida ayuda a mantener la continuidad del acceso sin interrupciones.

3. Autenticación Multifactor (MFA)

Safe Comercial ha implementado el requisito de habilitar la autenticación multifactor (MFA) en todas las cuentas donde sea posible, especialmente en correos electrónicos, VPN y sistemas críticos. Esta capa adicional de seguridad dificulta significativamente el acceso fraudulentos, incluso si la contraseña es comprometida.

Los métodos aceptados incluyen aplicaciones de autenticación como Authy o Microsoft Authenticator, que generan códigos temporales sincronizados o permiten verificaciones biométricas. Este enfoque elimina las vulnerabilidades relacionadas con el uso exclusivo de contraseñas.

El MFA se considera obligatorio para cualquier acceso remoto a la red corporativa, reforzando la defensa en un entorno donde las conexiones fuera de la oficina presentan mayores riesgos.

4. Uso de Contraseñas para Diferentes Sistemas

Una práctica fundamental en Safe Comercial es evitar el uso de la misma contraseña para múltiples sistemas o cuentas. Esta medida limita el impacto potencial de una brecha de seguridad, ya que no compromete automáticamente otras plataformas.

Se recomienda crear contraseñas fuertes y únicas para cada servicio, especialmente en aquellos que almacenan información sensible o accedan a recursos críticos. Esto asegura que incluso si una cuenta es vulnerada, el daño quede aislado.

El uso del gestor de contraseñas facilita la administración de múltiples contraseñas complejas sin necesidad de recordarlas todas, incrementando la adherencia a esta práctica esencial de seguridad.

5. Cumplimiento y Sanciones

El cumplimiento con esta política es obligatorio para todos los empleados, contratistas y usuarios con acceso a los sistemas de Safe Comercial. El incumplimiento puede acarrear

	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
	Política de Contraseñas seguras para Safe Comercial	
VIGENCIA: 25/06/2024	VERSIÓN: 1	Pag 3 de 3

consecuencias disciplinarias que incluyen desde advertencias hasta la suspensión del acceso a recursos corporativos.

Para asegurar la vigencia y relevancia de esta política, se revisará y actualizará anualmente o con mayor frecuencia si se identifican nuevas amenazas, requisitos regulatorios o innovaciones en seguridad informática.

La alta dirección de Safe Comercial se compromete a promover una cultura de seguridad y responsabilidad, facilitando los recursos necesarios para que los usuarios adopten buenas prácticas y protejan la integridad de la información empresarial.