LoyalShield

Guía para la creación de una contraseña segura

LoyalShield
SECURITY SOLUTIONS

empower your business

Guía para la creación de una contraseña segura.

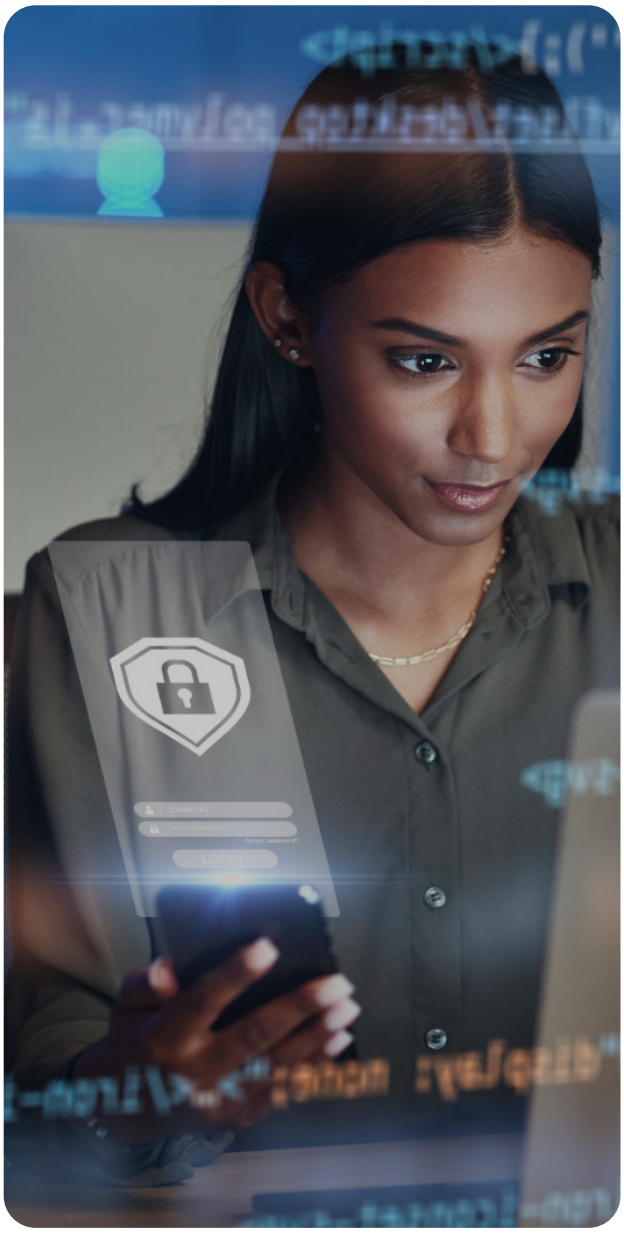
Contenido

Guía para la creación de una contraseña segura.

Introducción

Las **contraseñas** son fundamentales para la seguridad de la información dentro de las empresas. A pesar de ser una medida básica, su mala gestión puede resultar en brechas de seguridad costosas. Este manual tiene como objetivo proporcionarte las mejores prácticas para crear y gestionar contraseñas de forma efectiva.

Mantente siempre un paso adelante de las ciberamenazas



1

¿Qué es una contraseña segura?

Una contraseña segura es una combinación de caracteres diseñada para resistir los intentos de acceso no autorizado. Generalmente, se compone de una mezcla de letras mayúsculas y minúsculas, números y caracteres especiales, lo que aumenta su complejidad y reduce las probabilidades de ser adivinada.

Para los ejecutivos de nivel C (CEO, CFO, COO, CMO, CIO, CTO), comprender la importancia de la ciberseguridad, en particular la protección mediante contraseñas robustas, es esencial para mitigar riesgos. Una contraseña segura no solo debe ser compleja, sino también única y gestionada adecuadamente para resistir intentos de acceso que no hayan sido autorizados.

1.1. La importancia de las contraseñas seguras

Como líderes de la organización, las decisiones estratégicas en torno a la ciberseguridad tienen implicaciones directas en el negocio. Las contraseñas son la primera línea de defensa, y su robustez impacta de manera transversal en todas las áreas operativas.

Primera barrera de seguridad: Una contraseña segura protege el acceso inicial a sistemas clave ya que una brecha en estos sistemas puede paralizar las operaciones.

Prevención de ataques: Evitar el acceso no autorizado a través de técnicas como phishing es crucial para proteger los datos financieros, la propiedad intelectual y las estrategias empresariales.

Cumplimiento normativo: Como ejecutivos, es vital garantizar el cumplimiento de estas normativas para evitar sanciones que afecten las finanzas y reputación.

Confianza de los stakeholders: La capacidad de mantener las contraseñas seguras influye directamente en la confianza de inversores, clientes y socios comerciales.

1.2. Protección de datos sensibles y confidenciales

La protección de datos sensibles es crucial para mantener la integridad y la confidencialidad de la información empresarial. Las contraseñas seguras juegan un rol crucial en la protección de activos críticos, como:

Datos Financieros

Información de Clientes

Propiedad Intelectual

Sistemas Críticos

Medidas adicionales para la protección de datos

1. Cifrado: Utilizar cifrado para proteger datos en tránsito y en reposo.

2. Control de accesos: Implementar políticas de control de acceso basadas en roles para limitar el acceso según las necesidades.

2. Monitoreo y auditoría: Mantener registros de acceso y actividades para detectar y responder a incidentes de seguridad.

1.3. Consecuencias de una mala gestión de contraseñas

La gestión inadecuada de contraseñas puede tener repercusiones graves tanto para individuos como para organizaciones. Las principales consecuencias incluyen:

Filtraciones de datos

Las contraseñas débiles o comprometidas pueden permitir a atacantes acceder a bases de datos, sistemas internos y archivos confidenciales.

Impacto: Pérdida de información sensible, sanciones legales por incumplimiento de normativas, y daño reputacional.

Acceso no autorizado a sistemas críticos

Atacantes pueden infiltrarse en sistemas críticos, lo que les permite manipular operaciones, interrumpir servicios o instalar malware.

Impacto: Interrupción de operaciones, pérdida de productividad, y costos elevados de recuperación y remediación.

Pérdidas financieras

Los costos directos e indirectos asociados con brechas de seguridad pueden ser significativos.

Impacto: Incluye gastos en remediación, multas regulatorias, litigios legales y pérdida de ingresos por interrupciones operativas.

Daño reputacional

Una violación de seguridad puede deteriorar rápidamente la imagen de la empresa, perdiendo la confianza de clientes y mercados.

Impacto: La caída en las ventas, la pérdida de clientes y la devaluación de la marca son solo algunas de las consecuencias que una empresa puede enfrentar tras una brecha de seguridad.

2

Cómo crear una contraseña segura

Crear contraseñas seguras es una práctica esencial para proteger información personal y corporativa.

Este apartado tiene como objetivo proporcionar una guía práctica sobre cómo crear y gestionar contraseñas robustas que protejan tanto los sistemas empresariales como los datos sensibles bajo su responsabilidad.

$4.45M fue el costo promedio de una filtración de datos en 2023

2.1. Reglas básicas de una contraseña segura

Para garantizar que una contraseña sea segura, debe cumplir con una serie de criterios que aumentan su complejidad y resistencia frente a ataques.

Considera las siguientes recomendaciones al crear contraseñas:

1. Longitud: Asegúrate de que tenga al menos 10-12 caracteres; más largos son preferibles.
2. Complejidad: Usa una mezcla de mayúsculas, minúsculas, números y símbolos.
3. Evita patrones obvios: No utilices secuencias numéricas o palabras comunes.
4. No reutilices contraseñas: Cada cuenta debe tener una contraseña única.
5. Frases de contraseña: Considera utilizar frases compuestas por palabras aleatorias que sean fáciles de recordar pero difíciles de adivinar.
6. Uso de un administrador de contraseñas: Herramientas como Kaspersky Password Manager pueden ayudarte a gestionar y almacenar contraseñas de manera segura.

Debes crear contraseñas seguras que resistan las técnicas modernas utilizadas por los delincuentes para obtener información sensible.

Las Técnicas más comúnes son:

Hackeo basado en diccionario: Los atacantes utilizan programas para probar combinaciones de palabras comunes.

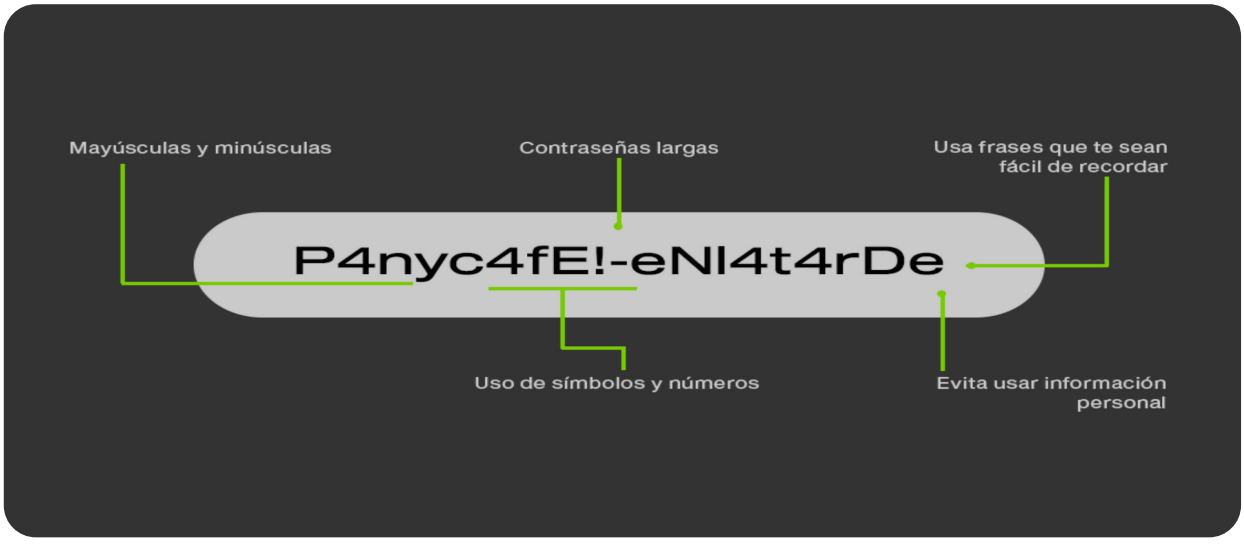
Explotación de información personal: Los delincuentes investigan redes sociales para obtener datos como nombres y fechas de cumpleaños que se utilizan en contraseñas.

Ataques de fuerza bruta: Consisten en generar todas las combinaciones posibles hasta encontrar la contraseña correcta.

Suplantación de identidad: Los estafadores engañan a los usuarios para obtener información personal haciéndose pasar por organizaciones legítimas.

Filtraciones de datos: Las brechas de seguridad en empresas pueden exponer contraseñas reutilizadas, facilitando el acceso a cuentas.

Ejemplo de una contraseña segura



2.2. Estrategias para recordar contraseñas sin comprometer la seguridad

Desde el uso de frases de paso hasta técnicas mnemotécnicas y patrones de teclado complejos, exploraremos métodos que no solo son fáciles de recordar, sino que también garantizan una mayor protección contra los ciberataques. Al empoderar a los usuarios con herramientas prácticas y consejos, buscamos fomentar una cultura de seguridad que permita manejar de manera efectiva la proliferación de contraseñas en la vida digital cotidiana.

Estrategias

Uso de frases de paso (Passphrases)

Las frases de paso son secuencias de palabras que resultan más fáciles de recordar que una serie aleatoria de caracteres, pero que mantienen un nivel de seguridad igual de alto. Esta estrategia no solo facilita el cumplimiento de las políticas de contraseñas, sino que también minimiza los problemas de gestión asociados.

Para crear una frase de paso, se recomienda seleccionar una oración o cita que sea relevante para la empresa. Luego, puedes modificar la frase incorporando números y caracteres especiales para aumentar su complejidad.

Gestores de contraseñas

Los gestores de contraseñas son herramientas diseñadas para almacenar, generar y gestionar las credenciales de forma segura. Es esencial que los ejecutivos fomenten su uso en toda la organización, ya que estos sistemas minimizan el riesgo de reutilización de contraseñas y permiten implementar políticas más estrictas.

Entre las ventajas de utilizar gestores de contraseñas se encuentran el almacenamiento seguro, ya que cifran las contraseñas para protegerlas de intentos de acceso no autorizado, y la generación automática de contraseñas fuertes y únicas para cada cuenta.

Método de iniciales

El método de iniciales consiste en crear contraseñas a partir de las iniciales de una frase, lo que permite construir contraseñas complejas que son fáciles de recordar y difíciles de adivinar. Para implementar esta técnica, selecciona una frase significativa y a continuación, toma las iniciales de cada palabra y añade números y caracteres especiales.

Uso de patrones de teclado complejos

Utilizar combinaciones de teclas que sigan patrones complejos en el teclado en lugar de secuencias predecibles permite crear contraseñas seguras.

Técnicas mnemotécnicas

Las técnicas mnemotécnicas son métodos que facilitan la retención de contraseñas complejas al asociarlas con imágenes, conceptos o historias que resulten fáciles de recordar. Para aplicar esta técnica, se puede relacionar cada caracter de la contraseña con una imagen o palabra. Este enfoque ayuda a que la contraseña sea más memorable, aumentando así la probabilidad de que el usuario la recuerde sin dificultad.

3
Do‘s y Dont‘s de las contraseñas

Adoptar buenas prácticas y evitar errores comunes es esencial para mantener la seguridad de las contraseñas en el entorno corporativo. La protección de los activos digitales y la información sensible no solo depende de la robustez de las contraseñas, sino también de cómo se gestionan y utilizan. A continuación, se presentan las mejores prácticas (Do‘s) y los errores a evitar (Don‘ts) para garantizar una gestión segura de las contraseñas.

3.1. Buenas prácticas

Estas prácticas no solo fortalecen la seguridad, sino que también ayudan a mitigar riesgos y a reducir la probabilidad de compromisos. A continuación, se presentan estrategias efectivas que los ejecutivos de nivel C deben implementar para garantizar que sus contraseñas sean robustas y seguras.

Autenticación de dos factores (2FA)

Implementar la autenticación de dos factores es una de las estrategias más efectivas para aumentar la seguridad de las cuentas. Esta técnica requiere dos formas de verificación antes de conceder acceso, lo que agrega una capa adicional de protección.

Beneficios

+ Protege las cuentas incluso si una contraseña se ve comprometida.
+ Utiliza métodos variados, como aplicaciones de autenticación y llaves de seguridad físicas.

Es crucial que todas las cuentas que lo soporten tengan 2FA configurada, priorizando métodos más seguros que los mensajes de texto.

Cambio regular de contraseñas

Cambiar las contraseñas de manera periódica, idealmente cada 3 a 6 meses, es vital para reducir el riesgo de compromisos a largo plazo. Este cambio es especialmente importante para cuentas que manejan información sensible o son de alto riesgo.

¿Cuándo cambiar contraseñas?

+ Después de una brecha de seguridad.
+ Si existe sospecha de que una contraseña ha sido comprometida.
+ Al compartir acceso con terceros y revocar dicho acceso posteriormente.

Monitoreo de actividad

La vigilancia constante de las cuentas permite detectar accesos o comportamientos sospechosos. Utilizar herramientas de monitoreo y configurar alertas es fundamental para actuar de manera proactiva.

Acciones ante actividades sospechosas

+ Cambiar inmediatamente la contraseña afectada.
+ Notificar al proveedor del servicio si es necesario.

Uso seguro de gestores de contraseñas

Los gestores de contraseñas son herramientas útiles para manejar múltiples contraseñas complejas.

Prácticas recomendadas

+ Elegir gestores con un buen historial de seguridad y actualizaciones frecuentes.
+ Proteger el gestor con una contraseña maestra fuerte y habilitar 2FA.

Esto no solo simplifica la gestión de contraseñas, sino que también asegura que estén protegidas adecuadamente.

3.2. Errores comunes

A pesar de la conciencia creciente sobre la importancia de la ciberseguridad, muchas organizaciones todavía cometen errores críticos en la gestión de contraseñas.

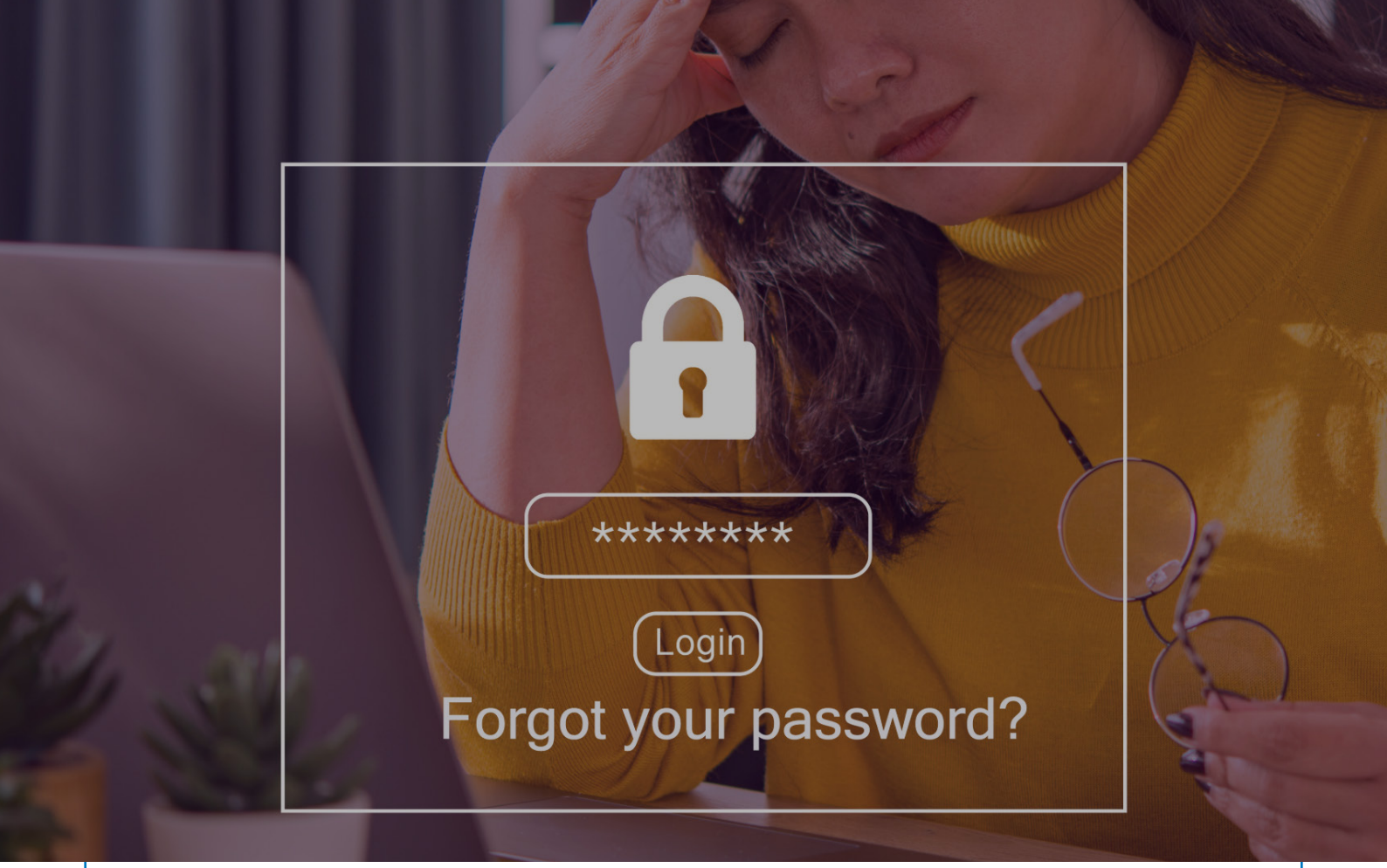
En esta sección, exploraremos los errores más frecuentes que se cometen en la gestión de contraseñas y cómo el evitarlos puede marcar la diferencia en la seguridad organizacional.

Uso de contraseñas débiles

Nunca utilices contraseñas simples o fáciles de adivinar, como „123456“ o „contraseña“.

Consecuencias

+ Estas son las primeras que los atacantes intentan, comprometiendo rápidamente la seguridad de las cuentas.



Reutilización de contraseñas

Evitar el uso de la misma contraseña en múltiples sitios o servicios es crucial. Si una contraseña se filtra, el riesgo de compromisos múltiples aumenta drásticamente.

Ignorar notificaciones de seguridad

No prestar atención a las alertas de seguridad puede resultar en la pérdida de la oportunidad de actuar rápidamente ante una posible brecha.

Falta de educación en ciberseguridad

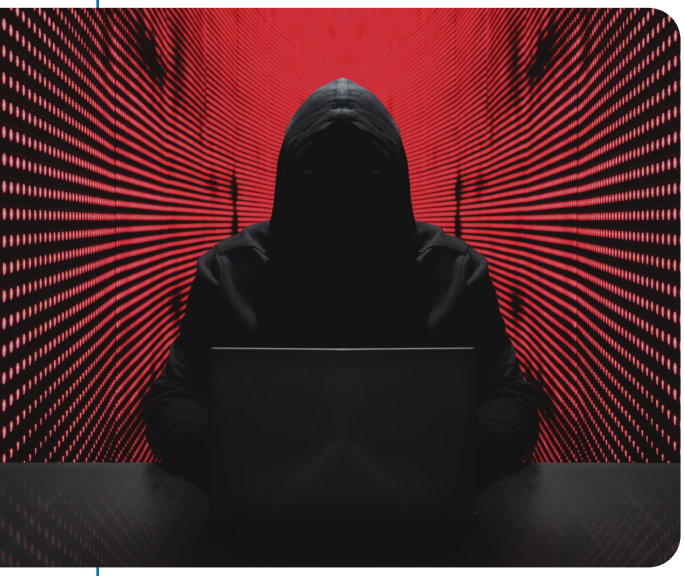
Subestimar la importancia de la formación en ciberseguridad puede llevar a decisiones inapropiadas que pongan en riesgo toda la organización. Fomentar una cultura de seguridad donde se valore y entienda la correcta gestión de contraseñas es fundamental para proteger los activos de la empresa.

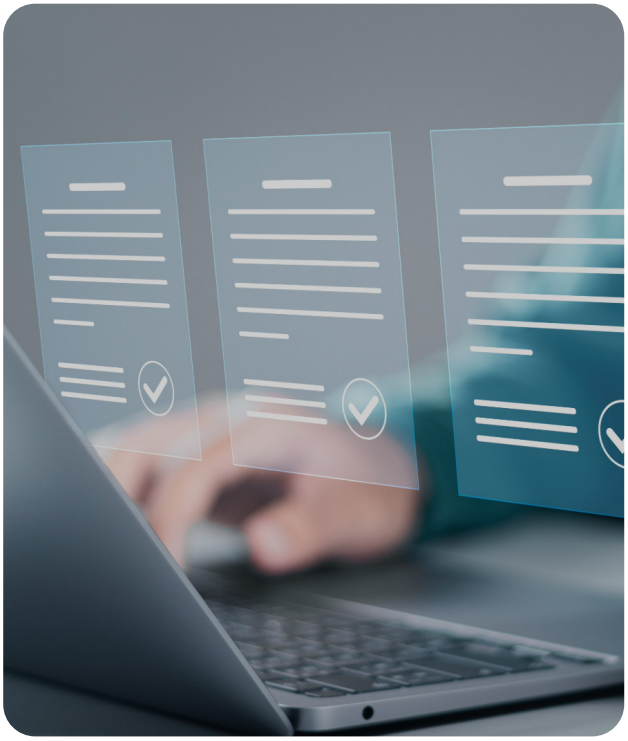
11 segundos fue el tiempo promedio entre ataques ransomware en 2023

4
Política de contraseñas

No basta con simplemente imponer reglas estrictas sobre la complejidad de las contraseñas; es necesario también desarrollar estrategias efectivas para su gestión, asegurando que los colaboradores comprendan y apliquen las buenas prácticas.

En esta sección, abordaremos los procedimientos clave ante sospechas de brechas de seguridad, las responsabilidades del equipo de ciberseguridad y la importancia de fomentar una cultura de seguridad en toda la organización. Desde la creación de políticas claras hasta la educación continua de los colaboradores, cada aspecto de la política de contraseñas debe estar orientado a prevenir vulnerabilidades y proteger los activos.





4.1. Procedimientos a seguir ante la sospecha de una brecha de seguridad

Ante la sospecha de una brecha de seguridad, es esencial actuar con rapidez y precisión para minimizar el impacto. Los procedimientos bien definidos permiten al equipo de ciberseguridad y a la organización contener el incidente de manera efectiva.

1. Identificación y evaluación de la brecha

El primer paso ante una posible brecha de seguridad es detectarla a través de sistemas de monitoreo y evaluar su alcance.

Pasos

+ **Alertas de seguridad:** Utilizar herramientas de monitoreo para recibir notificaciones sobre actividades sospechosas.
+ **Evaluación inicial:** Determinar qué sistemas y datos han sido comprometidos.
+ **Clasificación del incidente:** Evaluar la severidad y el impacto potencial de la brecha.

2. Contención y mitigación

Una vez identificada la brecha, es fundamental limitar su alcance y detener el acceso no autorizado lo antes posible.

Acciones

+ **Bloquear cuentas comprometidas:** Suspender el acceso a las cuentas afectadas hasta que la seguridad esté verificada.
+ **Cerrar vulnerabilidades:** Identificar y corregir las debilidades explotadas.
+ **Aislar sistemas afectados:** Separar los sistemas comprometidos para evitar la propagación del ataque.

3. Notificación a los usuarios afectados

Informar a los usuarios cuya información ha sido comprometida es un paso crítico para mitigar el impacto de una brecha.

Elementos clave de la notificación

+ **Descripción del incidente:** Explicar lo sucedido de manera clara y concisa.
+ **Impacto potencial:** Informar qué información podría haberse expuesto.
+ **Acciones recomendadas:** Proporcionar instrucciones claras sobre cómo protegerse, como cambiar contraseñas y estar atentos a actividades sospechosas.
+ **Contacto para soporte:** Ofrecer canales de comunicación para asistencia adicional.

4. Revisión y mejora de la seguridad

Después de contener una brecha, es crucial analizar lo sucedido para prevenir futuros incidentes.

Pasos

+ **Análisis forense:** Investigar la causa raíz de la brecha y las vulnerabilidades que se aprovecharon.
+ **Actualización de políticas:** Revisar las políticas de contraseñas y otros protocolos de seguridad con base en los hallazgos.
+ **Implementación de mejoras:** Adoptar nuevas herramientas y prácticas para reforzar la seguridad.
+ **Documentación del incidente:** Registrar detalladamente el incidente y las medidas tomadas para referencia futura y cumplimiento normativo.

4.2. Responsabilidad del equipo de ciberseguridad

El equipo de ciberseguridad tiene la responsabilidad central de implementar, monitorear y mejorar continuamente la política de contraseñas de la empresa, asegurando que se sigan las mejores prácticas para minimizar riesgos.

1. Desarrollo e implementación de políticas de contraseñas

El equipo de ciberseguridad debe definir políticas claras sobre la creación y gestión de contraseñas, alineadas con las necesidades de la empresa.

Elementos de la política

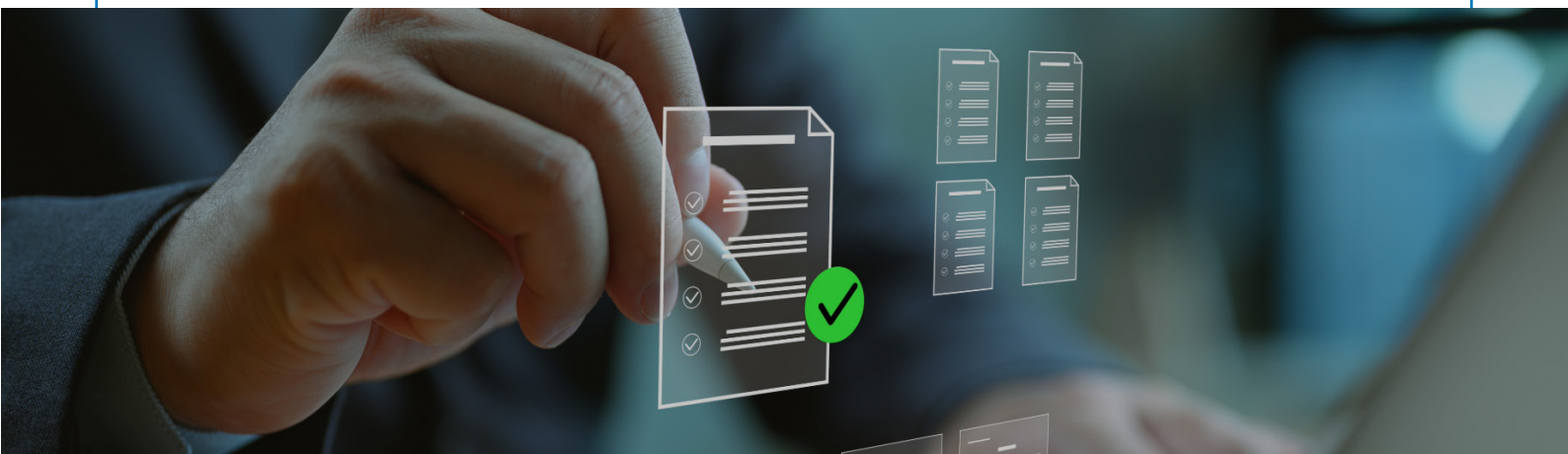
+ **Frecuencia de cambio:** Establecer intervalos regulares para actualizar las contraseñas.
+ **Manejo de contraseñas temporales:** Incluir procedimientos para contraseñas provisionales y su posterior cambio.
+ **Uso de 2FA:** Solicitar el uso de la autenticación de dos factores donde sea necesario.

2. Supervisión y auditoría de contraseñas

Es responsabilidad del equipo de ciberseguridad monitorear el cumplimiento de las políticas de contraseñas mediante auditorías regulares.

Actividades

+ **Revisiones periódicas:** Evaluar si las contraseñas utilizadas cumplen con los requisitos de seguridad.
+ **Auditorías de seguridad:** Realizar pruebas de penetración para identificar debilidades en las contraseñas.
+ **Reporte de incumplimientos:** Notificar a las autoridades internas sobre contraseñas que no cumplen con la política.



3. Educación a colaboradores

Proporcionar a los colaboradores los recursos necesarios para gestionar sus contraseñas de manera segura es clave para una política efectiva.

Acciones

+ **Capacitación:** Organizar talleres y/ pláticas sobre mejores prácticas de contraseñas.
+ **Soporte técnico:** Brindar asistencia en el uso de gestores de contraseñas y la recuperación de cuentas comprometidas.
+ **Actualización continua:** Mantener a los colaboradores informados sobre nuevas amenazas y soluciones de seguridad.

4.3. La importancia de una cultura de seguridad

La ciberseguridad es responsabilidad de todos los miembros de la empresa, y fomentar una cultura de seguridad es esencial en todo momento.

Compromiso de la alta dirección: El liderazgo debe mostrar un compromiso claro con la seguridad para motivar a toda la organización a seguir las políticas.

Acciones
+ **Comunicación constante:** Enviar mensajes regulares sobre la importancia de la seguridad.
+ **Asignación de recursos:** Invertir en herramientas y capacitación en ciberseguridad.
+ **Reconocimiento:** Incentivar a los empleados que sigan buenas prácticas de seguridad.

Integración de la seguridad en los procesos diarios: Incorporar medidas de seguridad en las rutinas diarias de trabajo es crucial para que la seguridad sea una prioridad constante.

Estrategias:
+ **Automatización de seguridad:** Utilizar herramientas que integren la seguridad sin interrumpir la productividad.
+ **Políticas claras:** Definir y comunicar políticas de seguridad comprensibles para todos.

4.4. Capacitación y concienciación continua para colaboradores

Una de las piezas clave en la protección de los activos digitales de una empresa es la educación y concienciación constante de todos los colaboradores.

Es vital que la empresa implemente programas regulares de formación en ciberseguridad, donde se aborden no solo las mejores prácticas para la gestión de contraseñas, sino también los riesgos más recientes en el ámbito de la seguridad digital.

Las capacitaciones pueden incluir
+ **Simulaciones de ataques cibernéticos:** como phishing, para evaluar cómo reaccionan los empleados y reforzar el aprendizaje en tiempo real.
+ **Actualizaciones periódicas:** sobre nuevas políticas de seguridad y normativas.
+ **Cursos en línea:** accesibles para todos, con módulos interactivos sobre la creación y manejo de contraseñas seguras.

La concienciación debe ser reforzada con recordatorios frecuentes a través de boletines internos, campañas y pláticas, asegurando que la ciberseguridad esté siempre presente en la mente de los colaboradores. Esto no solo protege a la empresa, sino que también empodera a los colaboradores para que sean parte activa en la defensa contra ciberataques.

4.5. Twilight Cyber y contraseñas seguras

Twilight Cyber es una herramienta avanzada que protege contraseñas y otros activos digitales en tiempo real. Su sistema se basa en la detección temprana de credenciales comprometidas y brechas de seguridad, monitoreando continuamente la dark web y redes críticas. Esto permite detectar compromisos de credenciales en horas, mucho antes que las soluciones tradicionales.

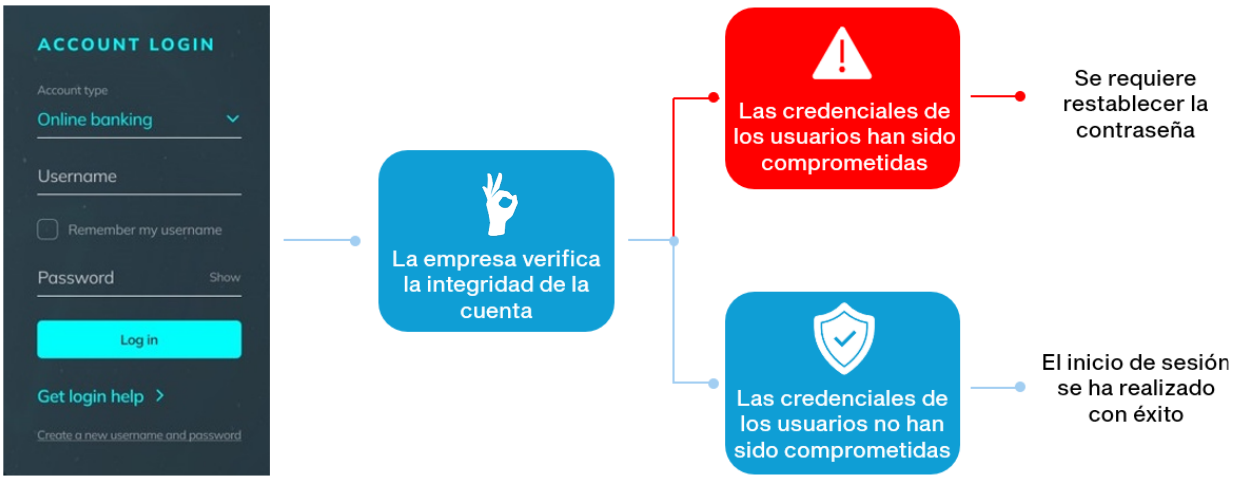
TWILIGHT CYBER
ONE STEP AHEAD

Para la protección de contraseñas, Twilight Cyber ofrece monitoreo constante de la seguridad de credenciales durante cada inicio de sesión, autenticación sólida, y actualización de credenciales comprometidas. Además, proporciona alertas en tiempo real, lo que permite respuestas rápidas y minimiza riesgos como el ransomware y filtraciones de datos.
La plataforma ayuda a las empresas a gestionar de manera efectiva las contraseñas comprometidas, asegurando una acción inmediata antes de que los atacantes puedan explotarlas.

Twilight Cyber también detecta vulnerabilidades en la cadena de suministro, protegiendo a la empresa incluso si los terceros con los que trabaja presentan debilidades en sus credenciales.

Ventajas

+ Permite actuar en tiempo récord, detectando amenazas dentro de las primeras horas.
+ Nuestra solución asegura la rápida notificación de brechas, permitiéndote actuar con rapidez para neutralizar credenciales comprometidas y contener incidentes.
+ Garantiza la continuidad de tu negocio y la reputación de tu marca al detener los ataques antes de que sucedan.



Recibe alertas en tiempo real de las credenciales comprometidas de tus clientes antes de ser utilizadas por los atacantes.