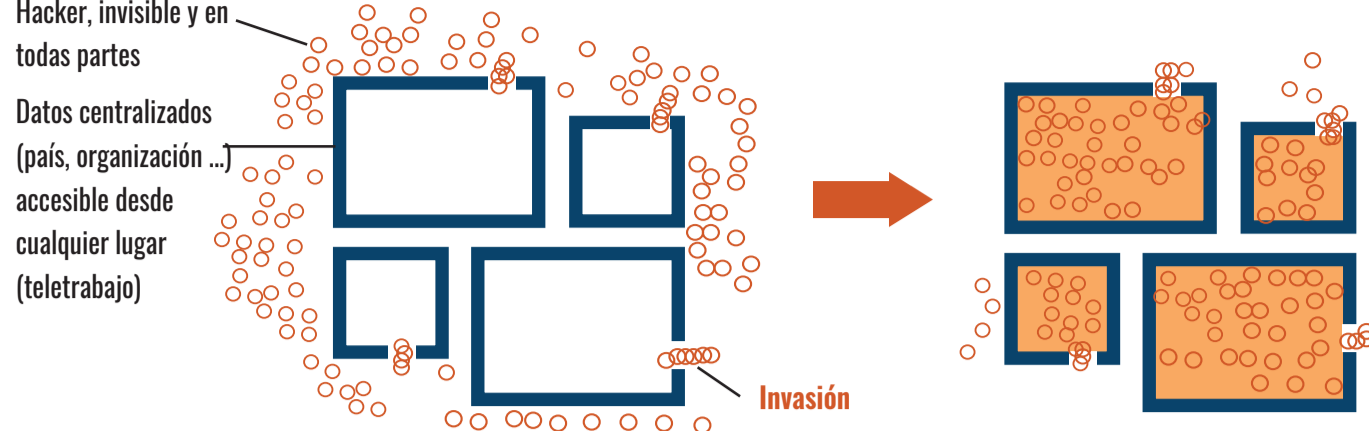


Problema #1 : La centralización de acceso (inicio de sesión único, contraseña maestra) es el talón de Aquiles de las empresas

Solo se necesitan 14 días entre una primera intrusión y una redada en toda la red

Día 1: Primera invasión

Día 14: red pirateada, archivos bloqueados, ransomware



Más del 80% de las filtraciones de datos comienzan por usar una contraseña débil, robada o reutilizada

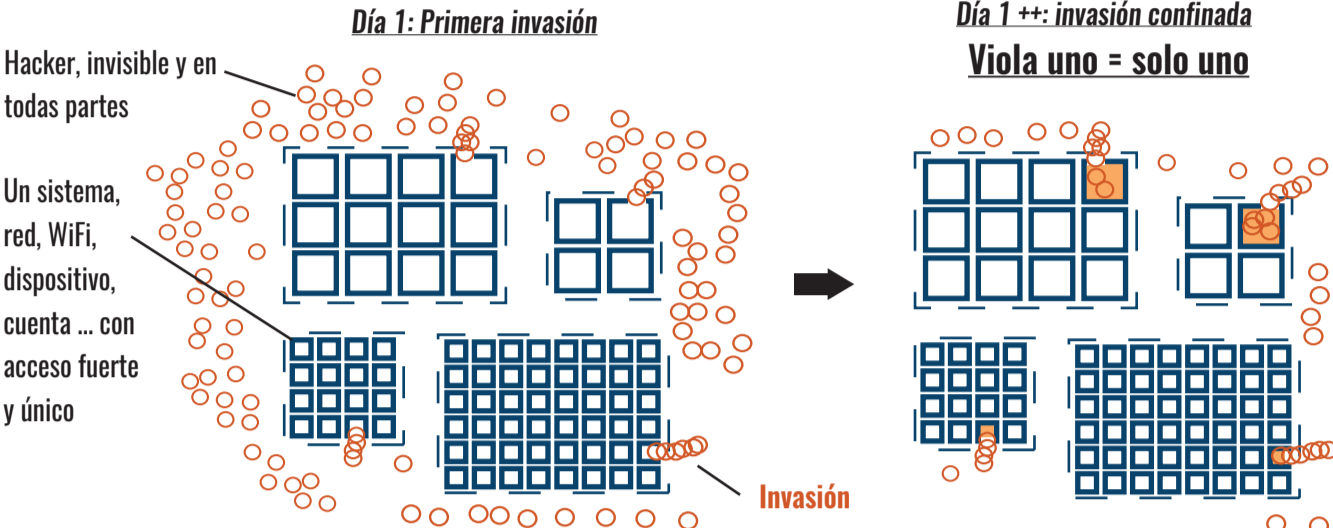
Remedio #1 : Acceso separado a cada sistema y descentralizar las credenciales

Principio: Al igual que en COVID-19, para detener la propagación de un virus es fundamental tener "distancia social".

¿Como se hace eso? Separe el acceso a todos los sistemas, redes, Wi-Fi, aplicaciones, cuentas, dispositivos ..., use credenciales sólidas y únicas para bloquear el acceso, y descentralice las credenciales para que si uno de ellos es robado, los demás permanezcan seguros.

Resultado : Sin punto de acceso centralizado ni contraseña maestra

Las violaciones de datos están contenidas de forma predeterminada



Grupos de datos más pequeños, accesos independientes, sin movimiento lateral

Problema #2 : El cerebro humano es incapaz de recordar contraseñas seguras



Remedio #2 : Proteja las contraseñas en una fortaleza local a la que solo usted pueda acceder

Principio: Las contraseñas son como llaves. No tienes que recordarlos. Solo necesita ser el único que puede acceder y usarlos.

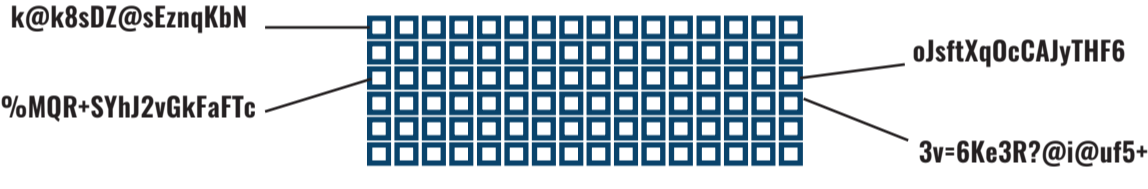
¿Como se hace eso? Utilice MyCena, una solución descentralizada que reemplaza al cerebro en la gestión de contraseñas únicas y seguras.

MyCena crea contraseñas sólidas y únicas para cada sistema, dispositivo, red, aplicación ... que usa y protégelas en un bastión local de credenciales a las que solo usted puede acceder. Mejor aún, su equipo nunca necesitará crear, recordar, escribir o ver una contraseña nuevamente.

Sobre todo, sin una contraseña maestra o un punto de acceso centralizado, no se arriesga a situaciones de "Viola uno = viola todo".

Resultado : Contraseñas únicas y seguras para cada sistema que utilice

Mitigar el riesgo de pérdida total de datos, ransomware e interrupciones comerciales



Portafolio de soluciones MyCena



Solución	MyCena Personal Fortress (MPF)	MyCena Business Fortress (MBF)	MyCena Desk Center (MDC)
Uso	Consumidor final	Empresa (con consola)	Empresa (con consola)
Soporte	Móvil+ Integración escritorio	Móvil+ Integración escritorio	Escritorio (para lugares de trabajo contenidos)
Ideal para	Uso personal	Negocio, oficina en casa	Contact Centers, Call Centers, BPO y BPS

Simplifique la gestión de credenciales únicas y sólidas

usando la consola MyCena



Consola MyCena

PARA MYCENA BUSINESS FORTRESS Y MYCENA DESK CENTER

- Administrar contraseñas, reglas y atributos de contraseñas de sistemas
- Administrar roles y permisos (solo MDC)
- Administrar la lista de usuarios (cargar la lista o usar Active Directory)
- Administrar quién recibe qué credenciales (administrar atributos)
- Supervisar el uso y el posible fraude (complemento: módulo Gobernanza, Riesgo y Cumplimiento)

Inicio de Sesión Seguro Simplificado (3SO)

Para todos los usuarios

MyCena Desk Center para computadoras (Mac, Windows o Linux)

GESTIÓN DE CREDENCIALES PARA LUGARES DE TRABAJO CONTENIDOS

- Centros de contacto, centros de llamadas y BPO
- Organizaciones cuyos empleados manejan información muy sensible (Información de Identificación Personal, información financiera, propiedad intelectual ...) con alto riesgo de fraudes / filtraciones
- Organizaciones cuyos empleados necesitan acceder a múltiples sistemas, redes, aplicaciones, cuentas y bases de datos para uno o varios clientes.

GENERADOR DE CONTRASEÑAS SEGURAS

TRES NIVELES DE SEGURIDAD (BRONCE, PLATA, ORO)

AES-SHA 256 CIFRADO



COPIE Y PEGUE LAS CONTRASEÑAS, SIN ESCRIBIR

COMPARE CONTRASEÑAS CIFRADAS

RECIBIR CONTRASEÑAS Y SISTEMAS PRECARGADOS

RESPALDOS CIFRADOS AUTOMATIZADOS

MyCena Business Fortress para dispositivos móviles (iOS o Android)

GESTIÓN DE CREDENCIALES PARA TRABAJADORES DESCENTRALIZADOS

- Organizaciones que trasladaron datos a la nube, haciendo que los datos sean accesibles desde cualquier lugar.
- Organizaciones cuyos empleados trabajan desde casa (FMH), lo que aumenta la superficie de los ataques de phishing, ingeniería social y ataques de fuerza bruta.
- Organizaciones que utilizan Active Directory, creando grandes grupos de datos para piratas informáticos.
- Organizaciones que utilizan el inicio de sesión único o la identidad centralizada, puntos de entrada ideales para los piratas informáticos

GENERADOR DE CONTRASEÑAS SEGURAS

MÚLTIPLES DISPOSITIVOS IOS / ANDROID

TRES NIVELES DE SEGURIDAD (BRONCE, PLATA, ORO)

RESPALDOS CIFRADOS AUTOMATIZADOS



DESCENTRALIZADO

COMPARE CONTRASEÑAS CIFRADAS

MODO VIAJERO

AES-SHA 256 CIFRADO

SE CONECTA AL ESCRITORIO

Beneficios de MyCena

Para la empresa

Administrar credenciales únicas sólidas

- ✓ Distribuya credenciales sólidas y únicas a cada sistema, red, cuenta, base de datos, WiFi ...
- ✓ Administre las políticas de contraseñas y supervise el uso sin ver las contraseñas de los usuarios
- ✓ Sin contraseña maestra, ID unificada o punto único de falla para el usuario o la empresa
- ✓ Implemente rápidamente sin actualizaciones del sistema ni cambios en su infraestructura existente.
- ✓ Ahorre 50% con sus tickets de TI vinculados al restablecimiento de contraseña
- ✓ Cumple con GDPR (UE), CCPA (California), LGPD (Brasil), NYPA (NY), HIPAA, PCI DSS

Para los usuarios

Inicio de Sesión Seguro Simplificado (3SO)

- ✓ Mejor productividad: Sin contraseña para crear, escribir, ver o recordar
- ✓ Mejor seguridad: contraseñas encriptadas y disponibles solo para el propietario con una combinación de huella digital, reconocimiento facial, PIN, patrón de bloqueo y contraseña de voz
- ✓ Mejor protección: tres niveles de seguridad (bronce, plata u oro) para credenciales de diferente sensibilidad