

CASO PRACTICO



Eddie Girón - 1307419



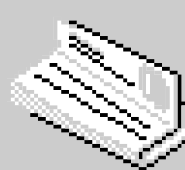
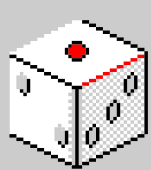
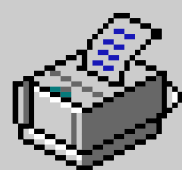
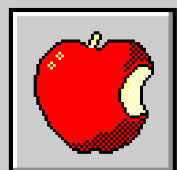
Julio Ruiz - 1284719



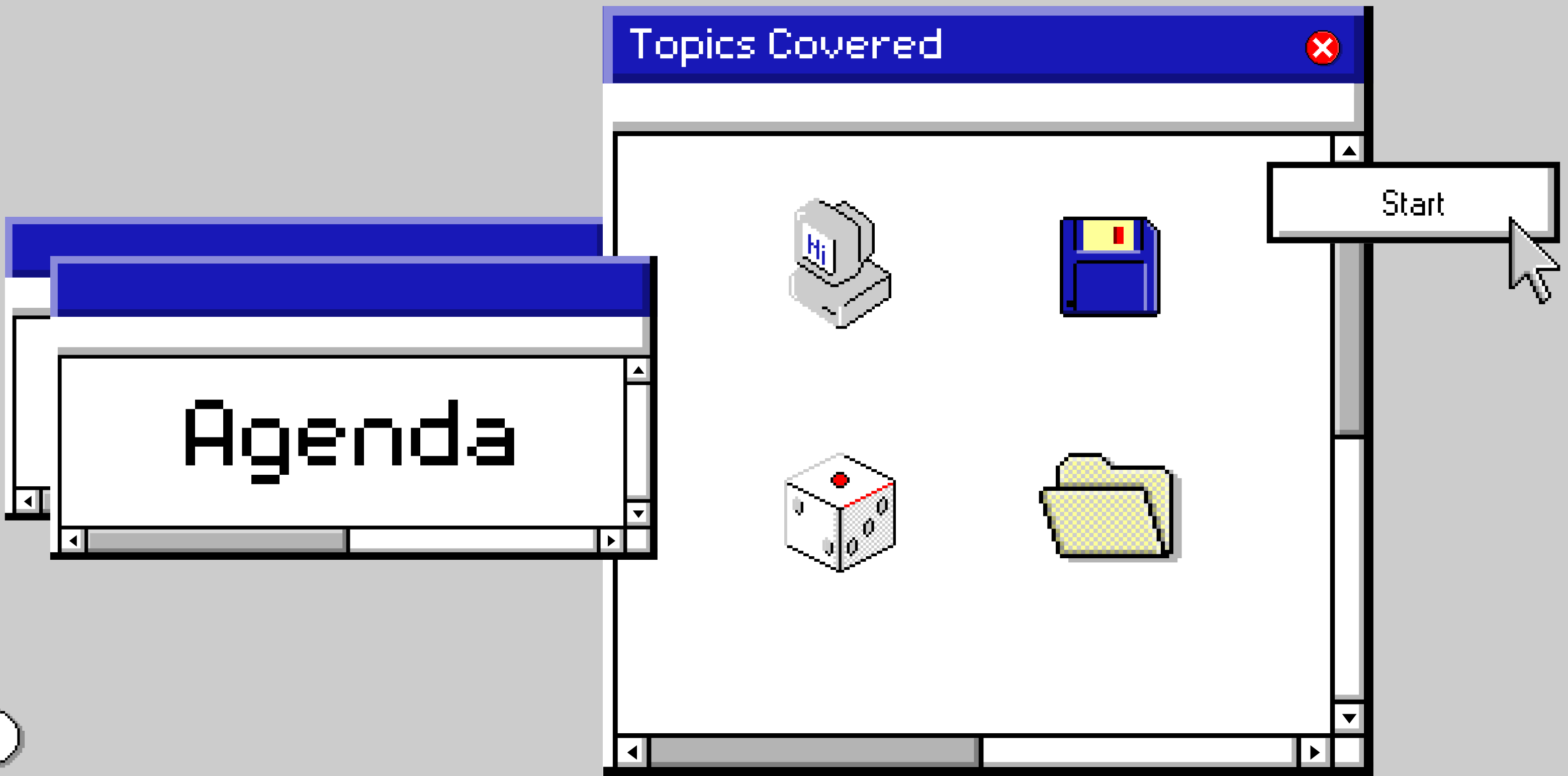
Marlon Roches - 1250918



Jose Giron - 1109419

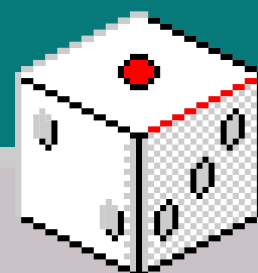


17:11PM



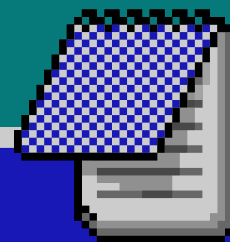
[Riesgo de tiempo de inactividad]

En el caso del tiempo de inactividad, se propone que las computadoras que se dejen en un escritorio, se les tenga configurado el tiempo de inactividad lo mas bajo posible, para asi evitar que terceros puedan manipular la información que esta dentro de la misma, así como cuando se le pueda dejar bloqueada a la computadora, se le haga, siempre asegurándose de que cuando se presiono suspender, se quede pidiendo contraseña o para un mas fácil acceso, que se presione la tecla Windows + R para así dejas suspendida la computadora y que esta exija contraseña para desbloquearla.



[Protección de la propiedad intelectual]

En este caso, muchas veces hay ciertas invenciones que se quieren dejar para uso exclusivo de la empresa, para eso se propone el uso de patentes las cuales nos permiten darle exclusividad a algo para uso de la empresa solamente, igualmente se puede usar lo que sería el copyright para los casos que solo se quiera proteger el uso de una idea.



Defensa contra el ransomware

Evitar enlaces spam

- Correos no legítimos
- Direcciones
- Archivos

Eliminando vulnerabilidades

- Actualizaciones de seguridad
- Pruebas de vulnerabilidad

Software de seguridad y vigilancia

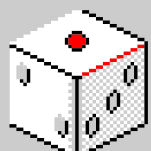
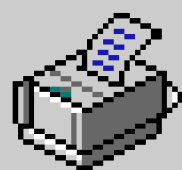
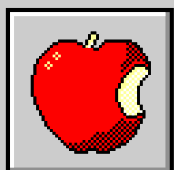
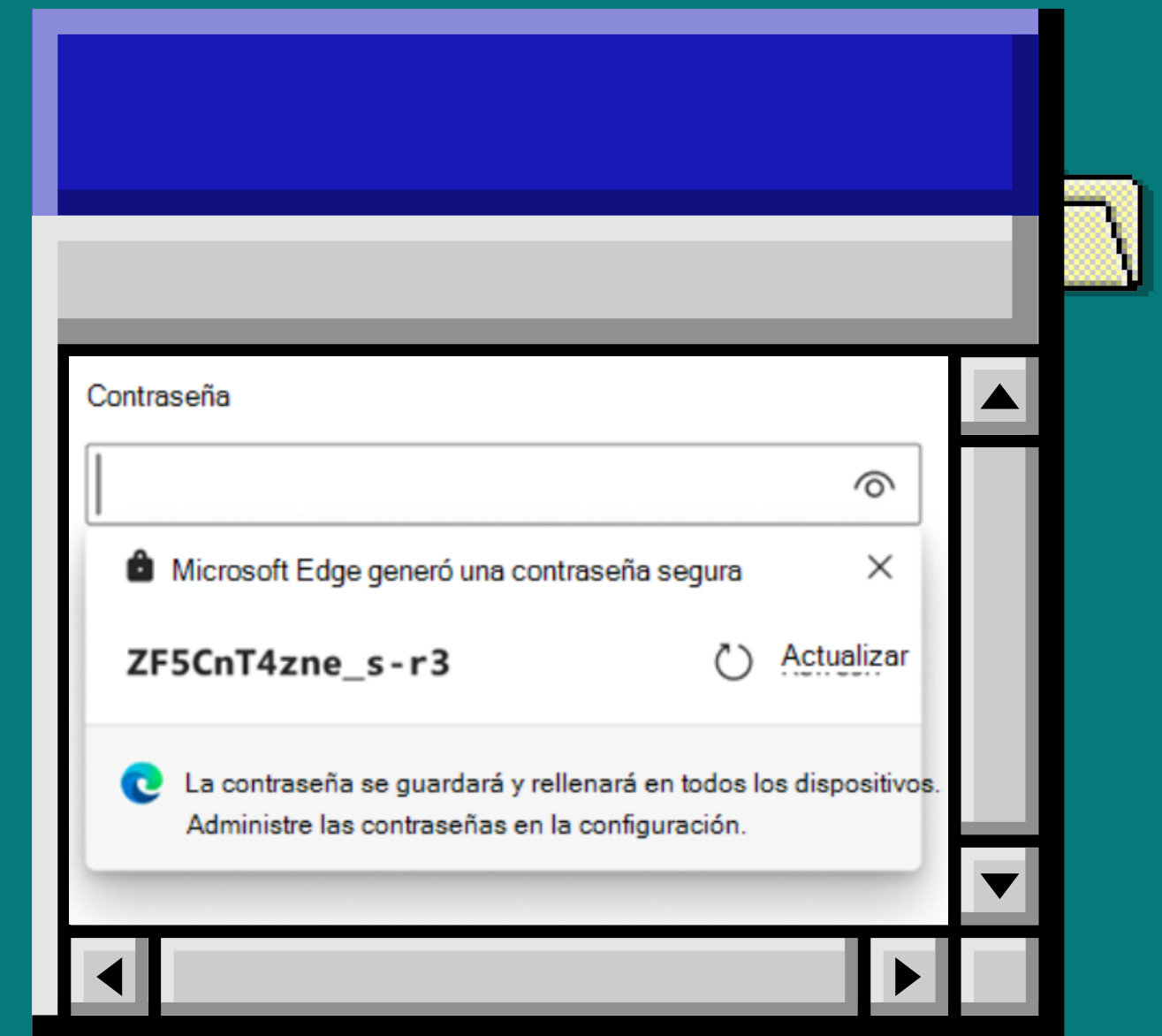
- Software de antivirus

Mejorando defensa de arquitectura

- Software de fuentes confiables
- Autenticadores 2 pasos

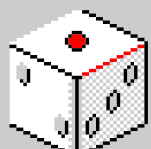
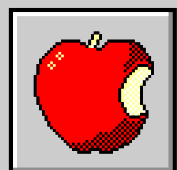
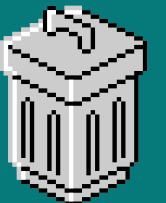
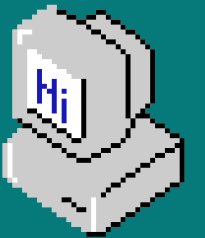
Contraseñas fuertes y autenticadores

- Contraseñas con caracteres alfanuméricos y símbolos
- Autenticadores confiables



- Copias de seguridad completas
- Copias de seguridad diferenciales
- Copias de seguridad incrementales
- Copias de seguridad locales
- Copias de seguridad en línea

Copias de seguridad periodicas



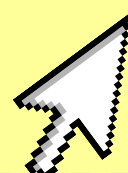


Desactualización de licencia de Windows



Poseer una licencia de Windows desactualizada provoca que no se reciban las últimas actualizaciones del sistema, dando paso a ataques por medio de la explotación de vulnerabilidades, además de no poder parchear estos errores.

[Back to Agenda Page](#)



[Facilidad De Uso]

Monitoreo y evaluación constantes

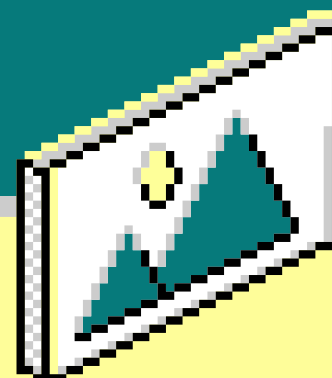
- Buen funcionamiento de los servidores y sistemas de la empresa.
- Tecnologías como monitoreo remoto
- Análisis de registros
- Alertas en tiempo real para problemas críticos
- Monitoreo de Logs

Gestión de contraseñas

- Implementar soluciones de gestión de contraseñas. almacenamiento seguro de contraseñas
- La generación automática de contraseñas complejas.
- Estándares de passwords.

Autenticación de dos factores

- Proteger la información confidencial de la empresa. utilizar dos métodos diferentes para verificar la identidad del usuario
- Contraseña y un código de acceso temporal.
- Tokens de seguridad y aplicaciones móvil



[Capacidad de Aplicación]

Cómo aplicarlos

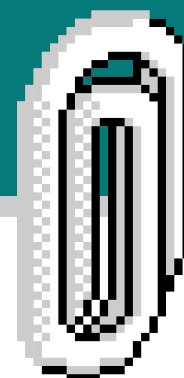
- identificar las áreas que necesitan ser cubiertas por la solución tecnológica
- Selección de una solución escalable.
- Implementación y formación del personal

Qué protege?

- Asegurar que la solución tecnológica pueda adaptarse a las necesidades cambiantes de la empresa
- Proporcionar una protección más completa a largo plazo.
- Inversión de la empresa en tecnología al garantizar que la solución seleccionada pueda seguir siendo utilizada

Tecnologías

- Cloud
- Virtualización
- Automatización
- Inteligencia artificial.



[Políticas de Cifrado]

Como aplicarlo ?

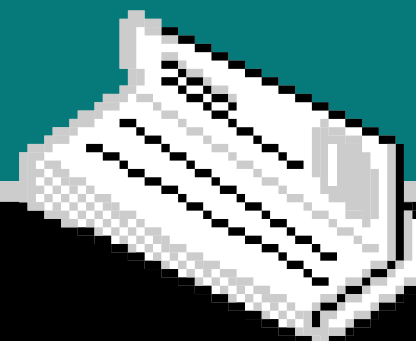
- Uso de software de cifrado de disco que se encargue de cifrar toda la información almacenada en el disco duro del equipo.
- Forma manual, utilizando herramientas de cifrado de disco, o de forma automatizada
- Implementado dentro de los sistemas operativos.

Que protege?

- protege la información almacenada en el disco duro del equipo
- contra el acceso no autorizado. Si un dispositivo se pierde o es robado, el cifrado de disco asegura que la información almacenada en el dispositivo no pueda ser accedida

Tecnologías

- BitLocker de Microsoft
- FileVault de Apple
- VeraCrypt
- Algoritmos de cifrado para asegurar la información almacenada en el disco duro.
- Pueden incluir características adicionales, como la gestión centralizada de claves de cifrado, el soporte para múltiples plataformas



[Monitoreo]

Como aplicarlo ?

- Monitoreo que permitan medir el rendimiento y la disponibilidad de los servidores en tiempo real.
- Enviar alertas en caso de que se detecten problemas.
- Implementar prácticas de evaluación periódicas para medir el rendimiento a largo plazo.

Que protege?

- Permite una respuesta más rápida y efectiva por parte del equipo de TI.
- Evaluaciones periódicas pueden detectar posibles deficiencias en el hardware o software del servidor

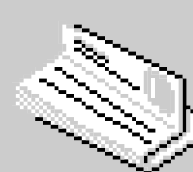
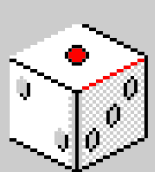
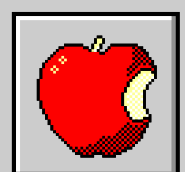
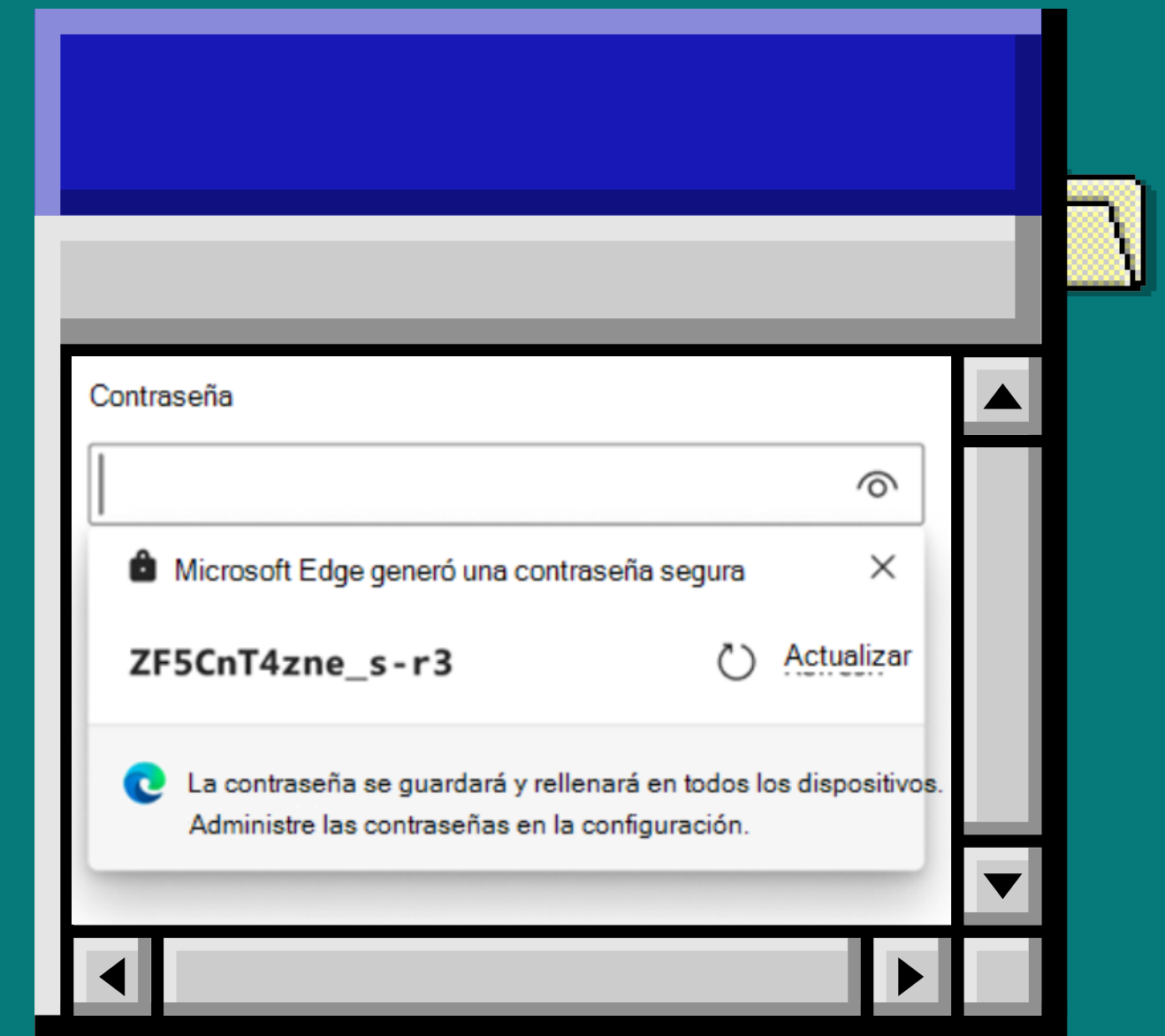
Tecnologias

- Nagios
- Zabbix
- PRTG Network Monitor
- SolarWinds Server & Application Monitor



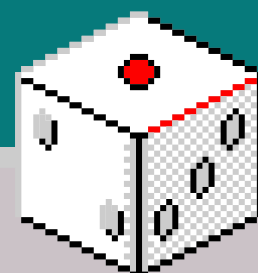
Flexibilidad de almacenamiento

En muchas ocasiones, los mismos dispositivos de almacenamiento externos, como las memorias usb, contienen virus maliciosos para el sistema, el cual nos puede robar información valiosa, por lo que para este caso se propone limitar los dispositivos de almacenamiento que se puedan conectar desactivando los puertos de la computadora y así evitando que estos puedan crear alguna vulnerabilidad dentro del sistema.




[Recuperacion completa desde 0]

Siempre se tiene que tener una fuente confiable de la cual podamos obtener información útil para la empresa, así como un lugar de fiar donde se pueda subir información en estilo backup por si acaso mas adelante se quiere recuperar y para eso se propone contratar un servicio de almacenamiento de información la cual no pueda contener alguna clase de script el cual nos realice algún robo dentro de la computadora.



Copia de seguridad In situ y en otra ubicación.



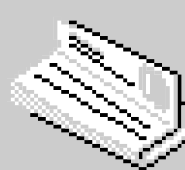
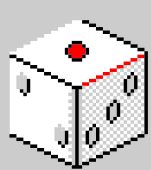
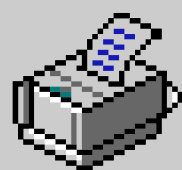
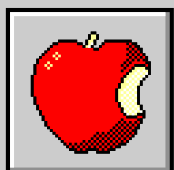
Implementen una solución de almacenamiento en la nube, como Google Cloud Storage, Amazon S3 o Microsoft Azure Blob Storage, para almacenar copias de seguridad en otra ubicación.



Utilice dispositivos de almacenamiento de alta capacidad, como NAS o SAN, para almacenar copias de seguridad in situ.



Configuren la solución de copia de seguridad en tiempo real para sincronizar los datos tanto en la nube como en el almacenamiento local, lo que garantiza la disponibilidad y recuperabilidad de los datos en caso de un incidente.



[Back to Agenda Page](#)

Establecer políticas de seguridad y reforzar sistemas de contraseña

Realicen sesiones de capacitación y pruebas de phishing periódicas para evaluar la conciencia de seguridad y mejorar la resiliencia de los empleados frente a ataques cibernéticos.

Implementen un sistema de bloqueo de cuentas tras varios intentos fallidos de inicio de sesión para prevenir ataques de fuerza bruta.

Implemente la autenticación multifactor para agregar una capa adicional de seguridad, especialmente para cuentas privilegiadas y acceso a sistemas críticos.

- **Las opciones de MFA pueden incluir mensajes de texto, aplicaciones de autenticación como Google Authenticator o Microsoft Authenticator, y tokens de hardware como YubiKey, monitorear y proteger sus recursos de la nube.**

