Ciberseguridad

Trabajo Remoto

EnorChile

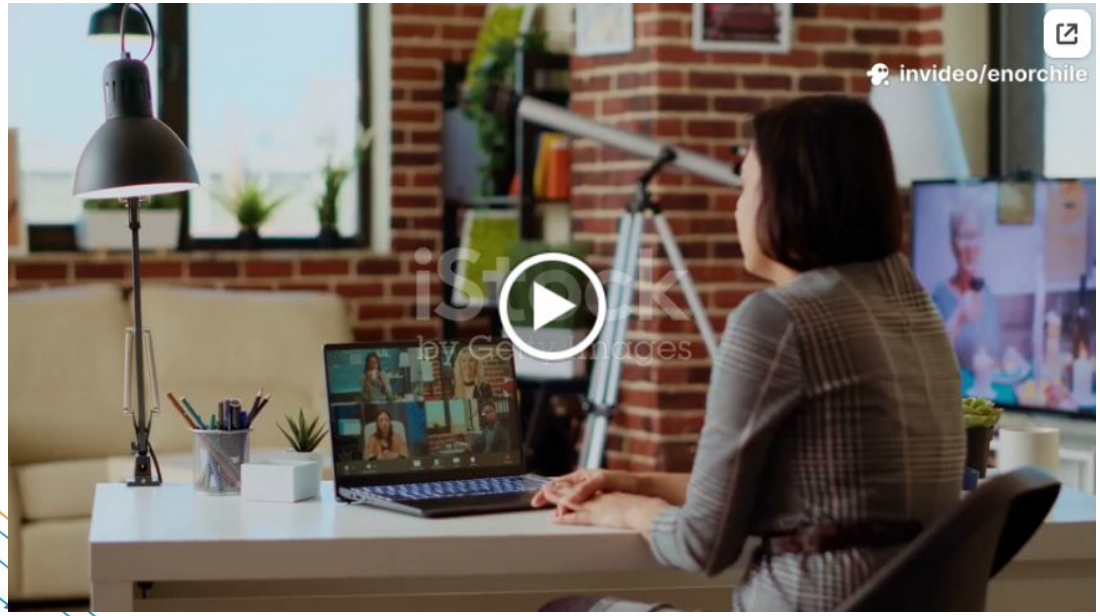
Introducción

¡Vaya! ¿Otra Charla, más de lo mismo?

EnorChile

Trabajo Remoto

Video Explicativo



EnorChile


invideo/enorchile
iStock
by Getty Images

Requerimiento

Anotarse por favor en el chat todos los que están participando de la charla

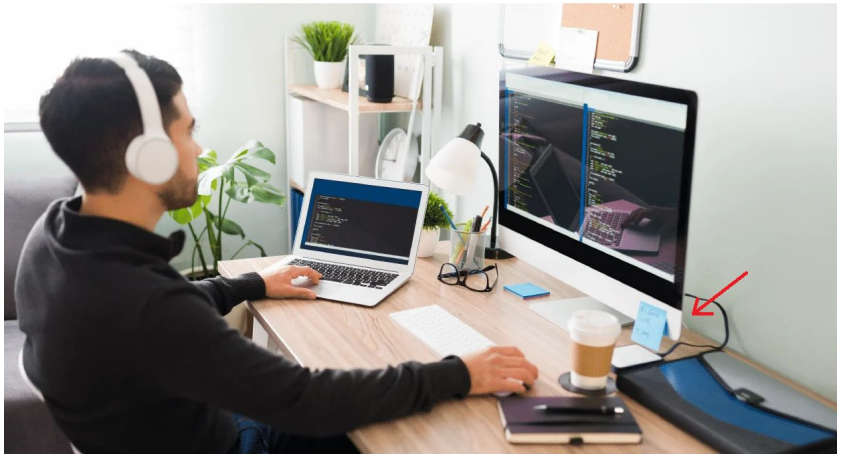
EnorChile

Contraseñas

- **Principales errores en el uso de Claves o contraseñas:**
  - **Utilizar la misma contraseña para distintos servicios.**
  - **Utilizar contraseñas débiles, fáciles de recordar.**
  - **Utilizar contraseñas cortas. (ej: Hola2)**
  - **Utilizar información personal a modo de contraseñas, como la fecha de nacimiento o nombres (ej: pablo123)**
  - **Guardar las contraseñas en webs o en el navegador**
  - **Hacer uso de patrones sencillos. (Hola1234)**

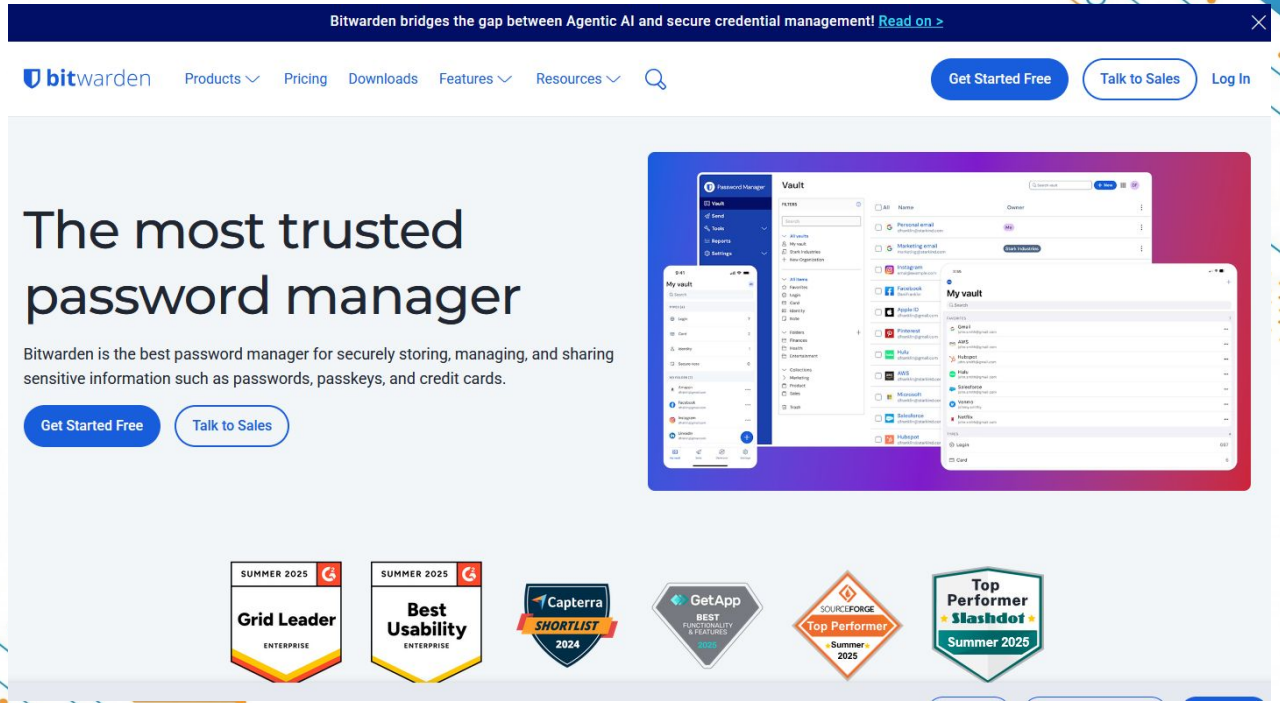
Contraseñas

- **Principales errores en el uso de Claves o contraseñas:**
  - **Apuntarlas en PAPEL o archivos sin cifrar**



EnorChile

Gestor de contraseñas:



EnorChile

Caso Real - 28 Julio 2025

Guerra Ruso - Ukraniana

EnorChile

Caso Real - 28 Julio 2025

Guerra Ruso - Ukraniana

Caso Real - 28 Julio 2025 - Aeroflot

Hackers who hacked Aeroflot revealed that the company uses outdated Windows XP, and the CEO has not changed the password for three years

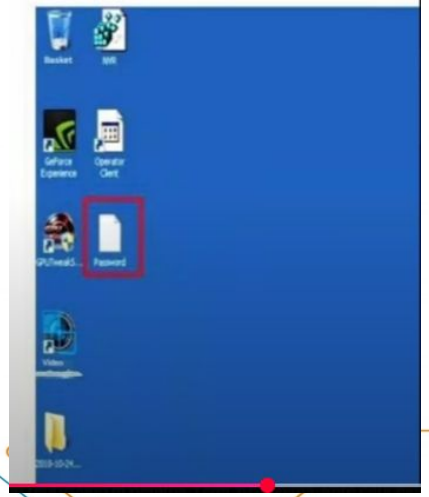
12 minutes ago

some employees of the computer 1 neglect b

CEO Sergei Aleksandrovsky has not

The network uses Windows XP and 2003, whi

their entire infrastructure.



EnorChile

Caso Real - 28 Julio 2025 - Aeroflot

La operación duró **más de un año**, durante el cual los atacantes mantuvieron acceso persistente a los sistemas de Aeroflot hasta el ataque destructivo el dia de ayer lunes 28 de Julio 2025

Los atacantes obtuvieron acceso a prácticamente todos los sistemas principales:

- **Gestión de vuelos** (TRIPULACIÓN, Saber)
- **ERP y CRM** (1C, Sirax, SharePoint, KASUD)
- **Correo electrónico corporativo** (Exchange)
- **Control de pérdida de datos** (DLP)
- **Sistemas de vigilancia e intervención telefónica**
- **Dispositivos terminales del personal**, incluido el director ejecutivo

Datos recopilados:

- **12 TB** de base de datos (historial de vuelos, mantenimiento, pasajeros)
- **8 TB** de recursos compartidos de archivos en red (carpetas internas)
- **2 TB** de correo electrónico
- Audio de interceptaciones y comunicaciones internas
    - Datos de sistemas de monitoreo de personal

Caso Real - 28 Julio 2025 - Aeroflot

Infraestructura comprometida:

- **122 hipervisores**
- **43 entornos ZVIRT (virtualización rusa)**
- Aproximadamente **100 interfaces iLO** para la gestión de servidores físicos
- **4 clústeres Proxmox**
- Acceso completo a miles de máquinas virtuales

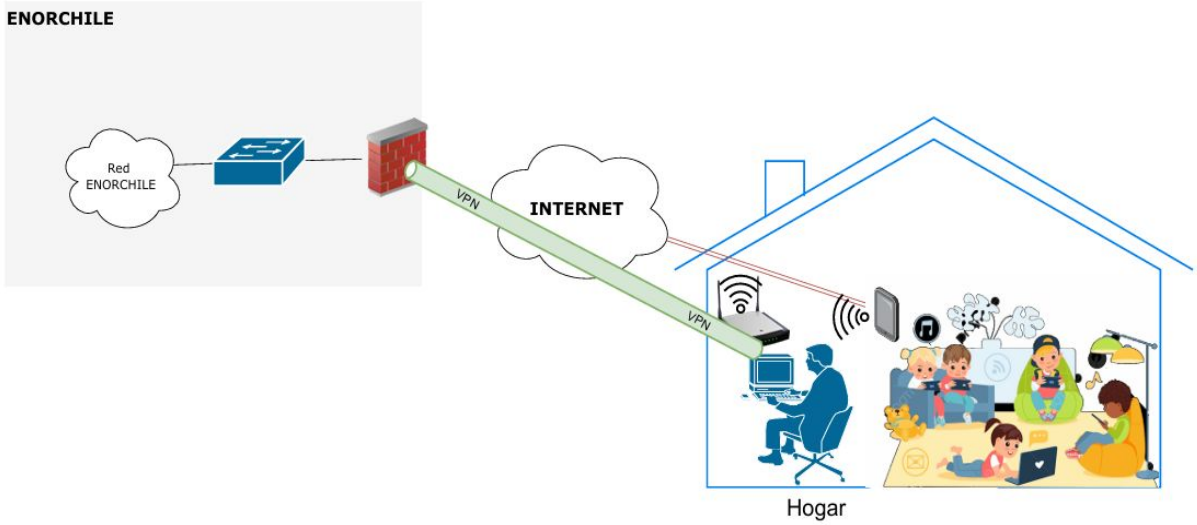
El resultado:

- Eliminación completa de **7000 servidores** (físicos y virtuales)
- La exfiltración de **22 terabytes de datos sensibles**
- **54 vuelos cancelados** solo el 28 de julio
- Interrupciones informáticas a gran escala en aeropuertos rusos
- Información completa de todos los pasajeros

Trabajo remoto

Antivirus & actualizaciones:

- Antivirus en todos los equipos de la casa.
- Actualizar todos los sistemas del hogar.



EnorChile

Trabajo Remoto

Nuevas amenazas:

vector de ataque usando el calendario.

Cuidado a la reunión que estás por entrar.

Resumen:

Desconfiar siempre, Desconfiar Todo

- Desconfiar de paginas WEB desde donde puedes descargar gratis el programa que deseas.
- Desconfiar de email con remitente desconocido.
- Desconfiar cuando la página web te consulta si deseas “aceptar” algo.
- Desconfiar de los Pendrives USB de otras personas.
- Desconfiar del WIFI gratis o Puntos de Acceso.
- Desconfiar del entorno, Bloquea el PC, cuando no lo tengas a la vista.
- Desconfiar del entorno , no coloque claves a la vistas (ej en puestos de trabajo).
- Desconfiar de clientes, proveedores, compañeros … No comparta tu acceso VPN ni tus claves.

EnorChile

Resumen:

Desconfiar siempre, Desconfiar Todo

- Desconfiar de paginas WEB desde donde puedes descargar gratis el programa que deseas.
- Desconfiar de email con remitente desconocido.
- Desconfiar cuando la página web te consulta si deseas “aceptar” algo.
- Desconfiar de los Pendrives USB de otras personas.
- Desconfiar del WIFI gratis o Puntos de Acceso.
- Desconfiar del entorno, Bloquea el PC, cuando no lo tengas a la vista.
- Desconfiar del entorno , no coloque claves a la vistas (ej en puestos de trabajo).
- Desconfiar de clientes, proveedores, compañeros … No comparta tu acceso VPN ni tus claves.

EnorChile