

STRONG PASSWORDS

Es uno de los tips más mencionados, y de los más **importantes**. Crear una **contraseña segura**, crea una fuerte barrera contra los cibercriminales.



¿CÓMO?

Inicia con una **frase** que tenga un significado para ti, combinado con **números**, **símbolos** y **letras** intercalados, asegurándote de que tenga por lo menos **8 caracteres**.

¡NUNCA UTILIZAR LA MISMA CONTRASEÑA PARA VARIOS SERVICIOS EN LA RED!

¡TERRIBLE IDEA! Porque esto vuelve tus **cuentas un todoterreno** para quien la llegue a adivinar. Ya que si una se logra vulnerar, podrán explotar otra sin ningún problema.



¡LAS CONTRASEÑAS SON VALIOSAS, **APRENDE** A CUIDARLAS!

Las contraseñas representan la primera línea de defensa en la **protección de tu vida digital**, cuídalas porque son un activo importante.

- **No las compartas** con nadie.
- Es recomendable cambiarlas cada **45 días**
- No utilices la misma **para más de un servicio** en la red
- Utiliza **combinaciones** de letras, números y símbolos.
- **No utilices** tu fecha de nacimiento, tu nombre, el de tu mascota o tu dirección para una contraseña.
- Utiliza **el doble factor** de autenticación en los servicios que utilices
- **No los apuntes en papel**, en lugar de esto utiliza un programa para gestión de contraseñas. Estos guardan tus contraseñas puedes utilizar un nombre clave para cada servicio y adicional las guarda protegidas con contraseña.

ZERO TRUST

Zero trust es un modelo de seguridad de red basado en **un proceso estricto de verificación de identidad**. Este marco de seguridad impone que **solo los**



usuarios y dispositivos autenticados y autorizados puedan **acceder** a las aplicaciones y a los datos.

Zero Trust se basa en el principio de **“nunca confié, siempre verifique”**.

El modelo de Zero Trust



Suministra: A los usuarios cualquier dispositivo, con las aplicaciones, las políticas y los perfiles adecuados.

Concede acceso: Basado en un contexto integral. (Usuario, dispositivos, aplicaciones, red, amenaza, tiempo, etc.).

Hace cumplir: Las políticas de seguridad.

Protege: Los datos; encapsulando y eliminando amenazas de dispositivos.

¿Por qué es necesario un modelo de seguridad Zero Trust?



Los usuarios, los dispositivos, los datos y aplicaciones **se están trasladando fuera del perímetro** de la empresa y de la zona de control.



Los **nuevos procesos empresariales** impulsados por la transformación digital incrementan el riesgo a la exposición.

El enfoque **“confiar, pero verificar”** **ya no es una opción**, dado que las amenazas avanzadas ahora **acceden** al perímetro de la empresa.



Los **perímetros tradicionales** son complejos, **incrementan** el riesgo **y ya no son adecuados** para los modelos de negocio actuales.

