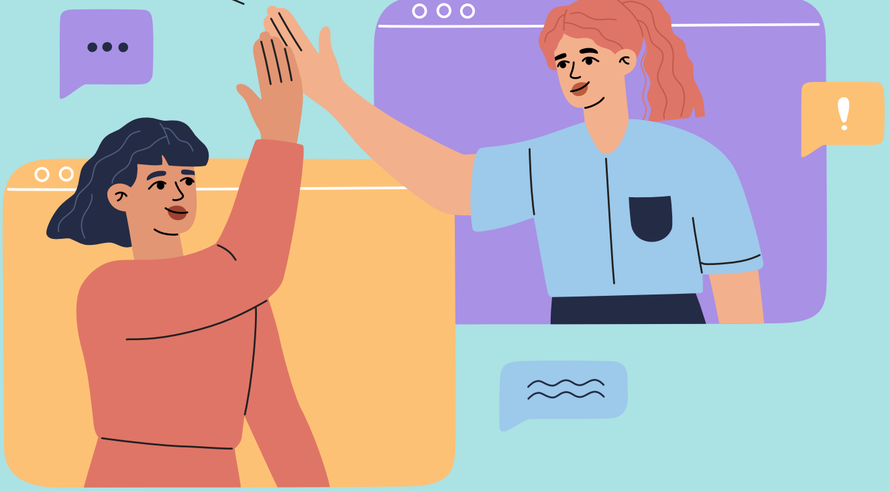
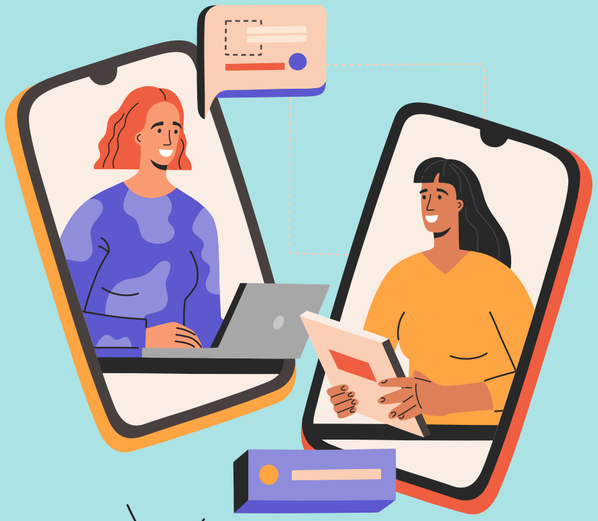
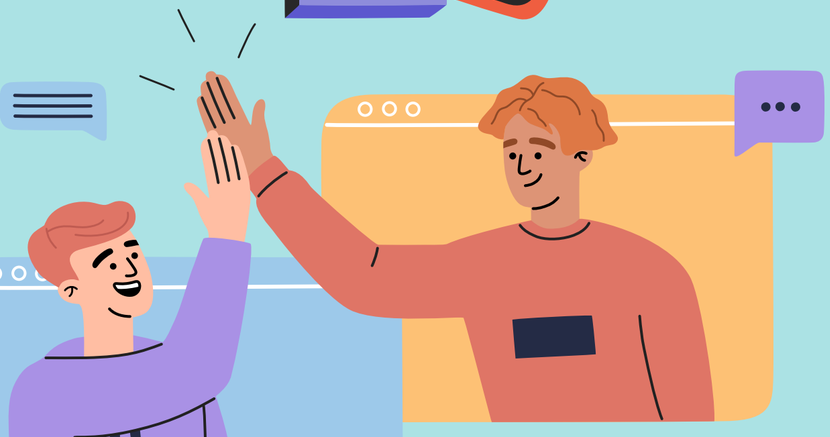


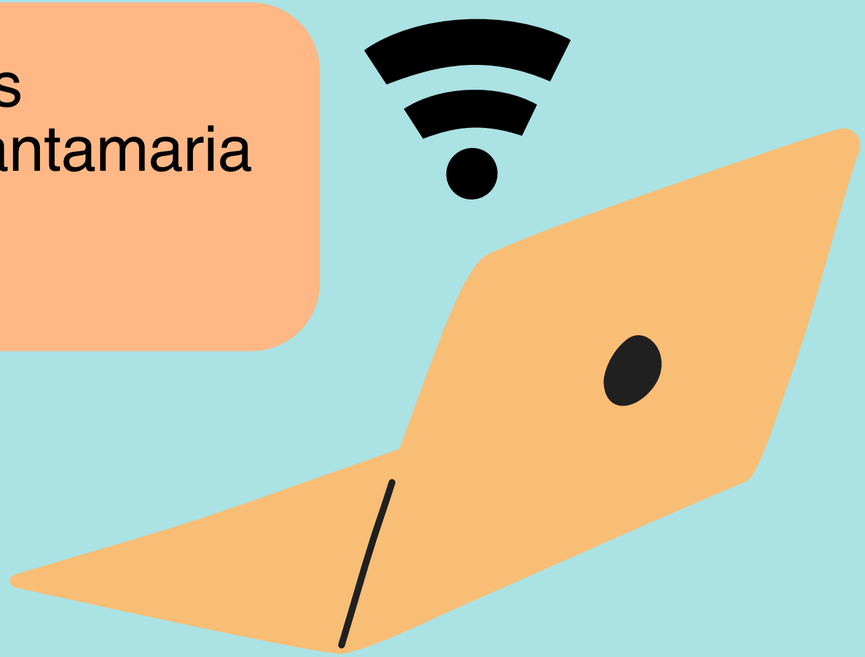




POLÍTICAS DE SEGURIDAD

Josué Abdel Ortiz Deodanes
Brandon Daniel Sanchez Santamaria

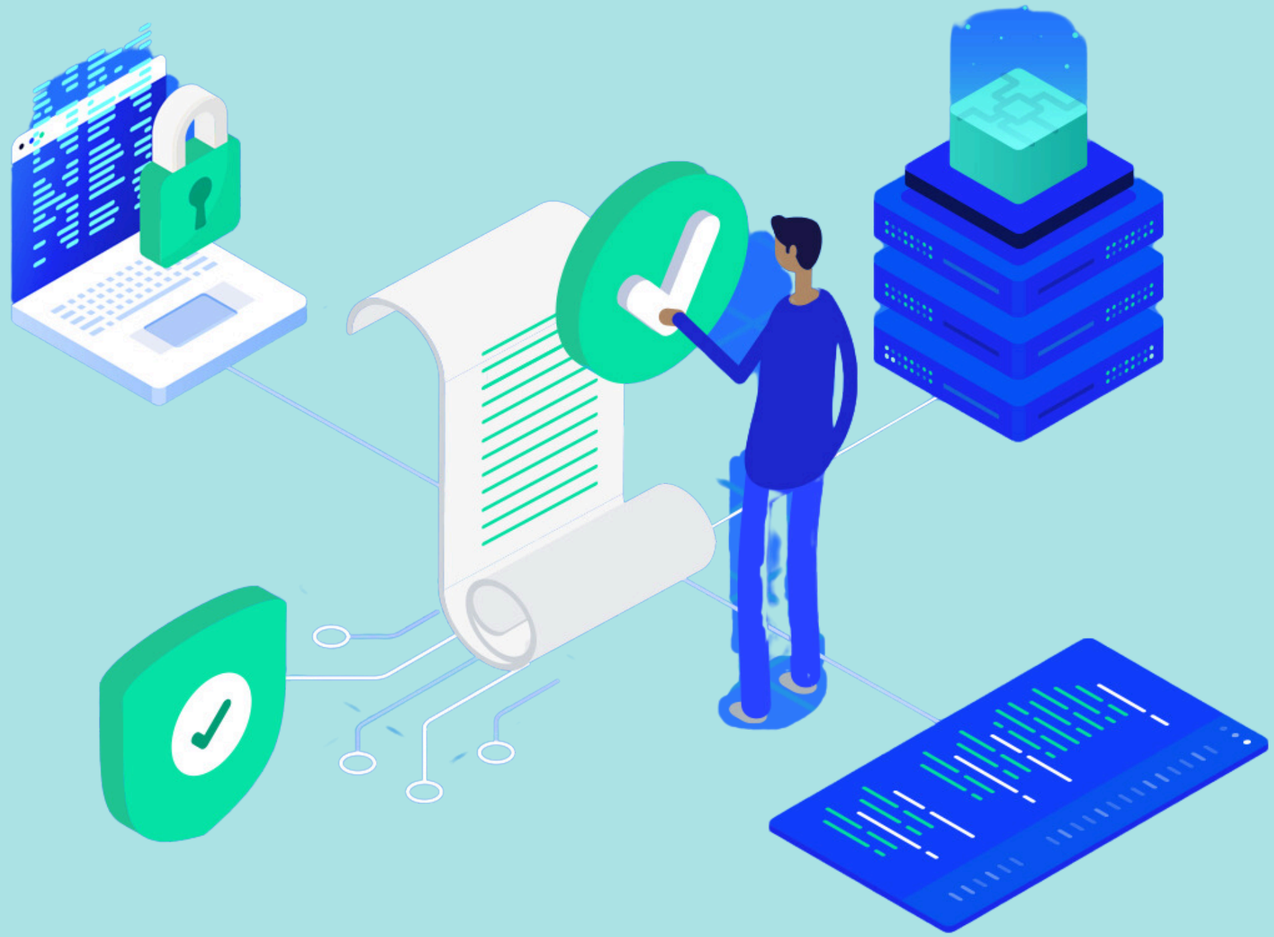
3° Año - 2A



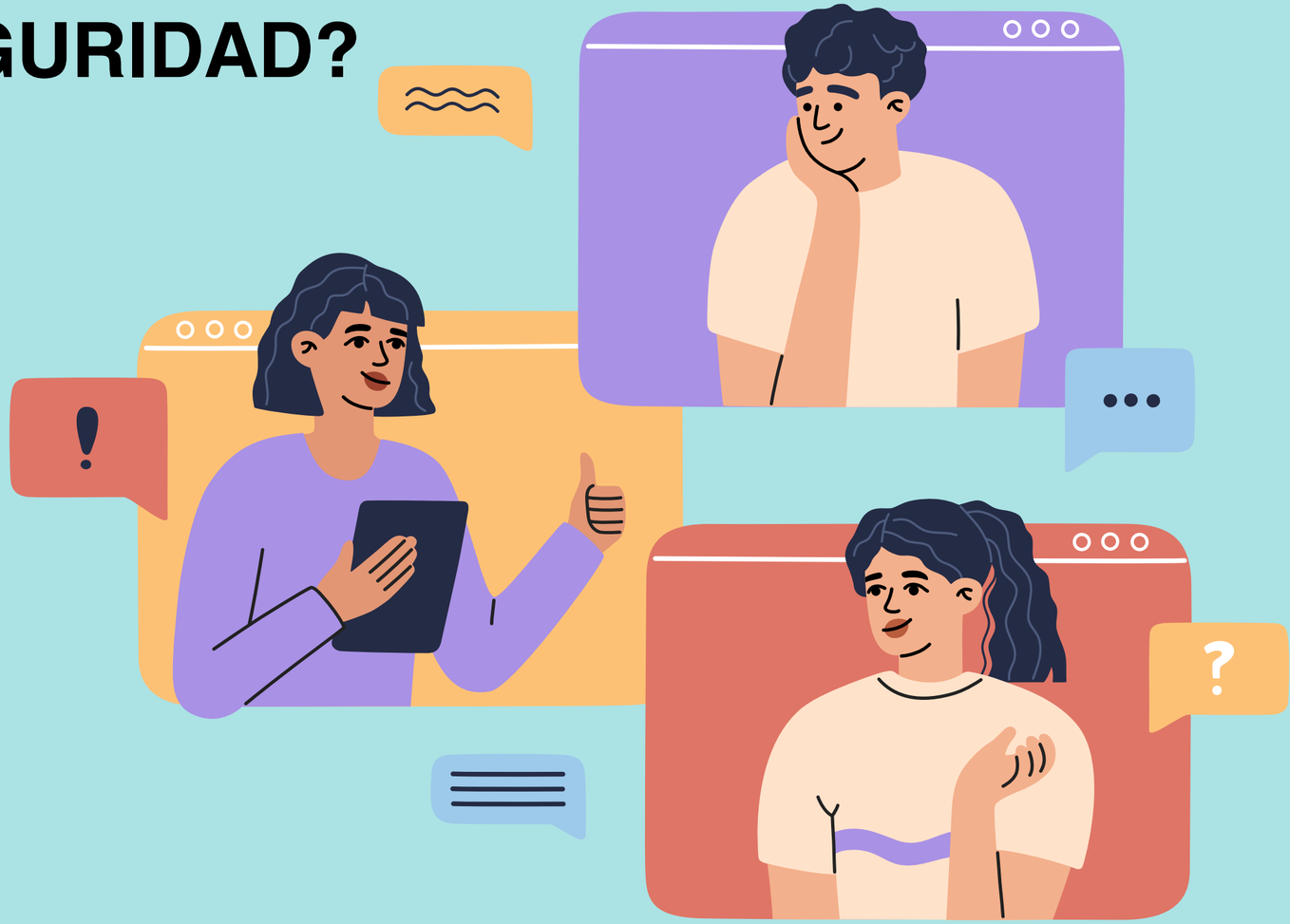
¿QUÉ SON LAS POLÍTICAS DE SEGURIDAD?

Las políticas de seguridad son un conjunto de reglas, directrices y procedimientos diseñados para proteger los datos confidenciales y criticos de una organización.

En otras palabras son formas en las cuales se manejan los posibles riesgos que se puedan enfrentar en una organización al manipular datos, estableciendo medidas que deben tomarse para prevenir accesos no autorizados.



¿POR QUÉ DEBO DISPONER DE UNA ESTRATEGIA DE CIBERSEGURIDAD?

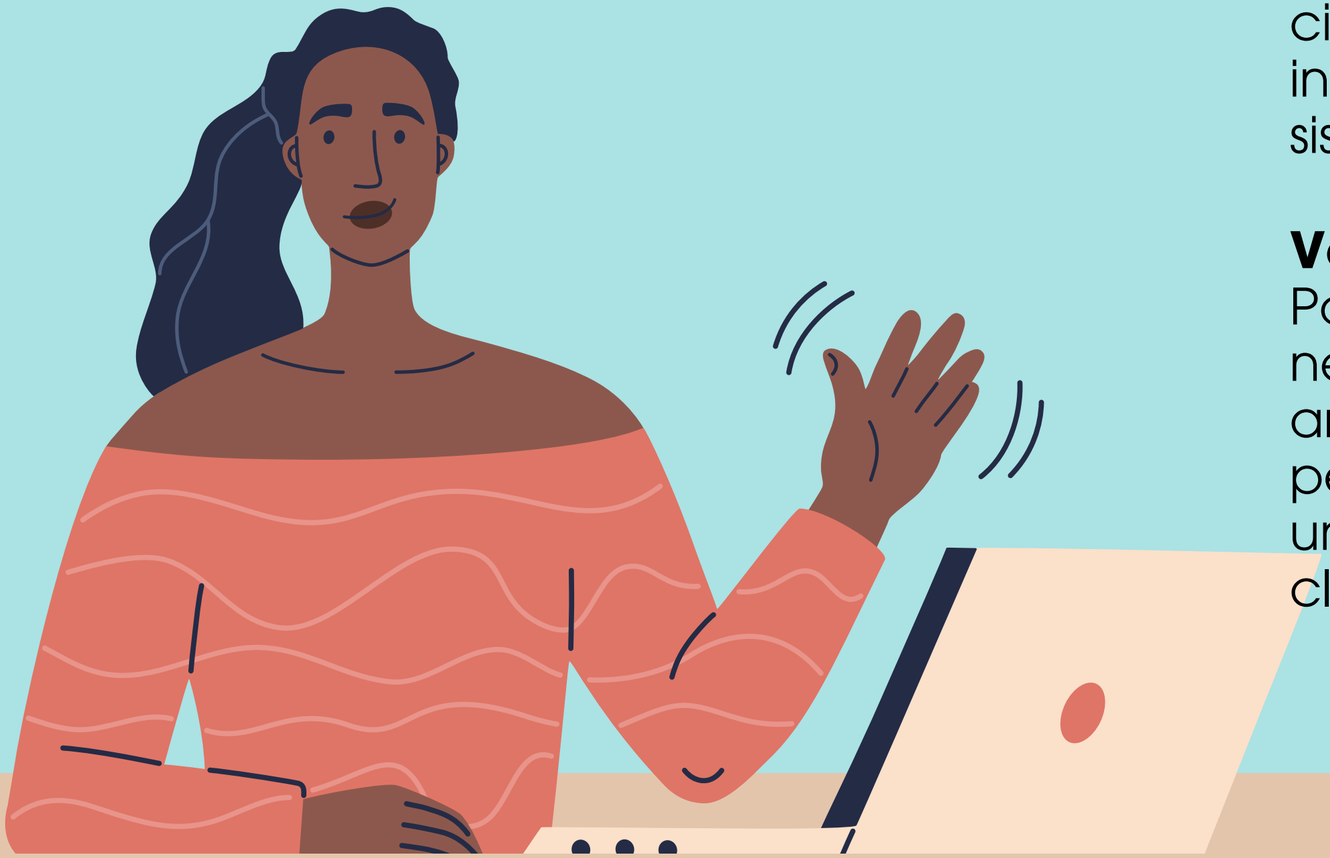


La implementación de estrategias de ciberseguridad es crucial para proteger los activos digitales, la reputación, fiabilidad y confianza de una organización.

Razones clave:

Protección de datos sensibles:
En toda empresa se manejan datos sensibles como datos personales, financieros que son valiosos, por ello una estrategia protege estos datos de robos, fugas y accesos no autorizados, lo escensial.

¿POR QUÉ DEBO DISPONER DE UNA ESTRATEGIA DE CIBERSEGURIDAD?



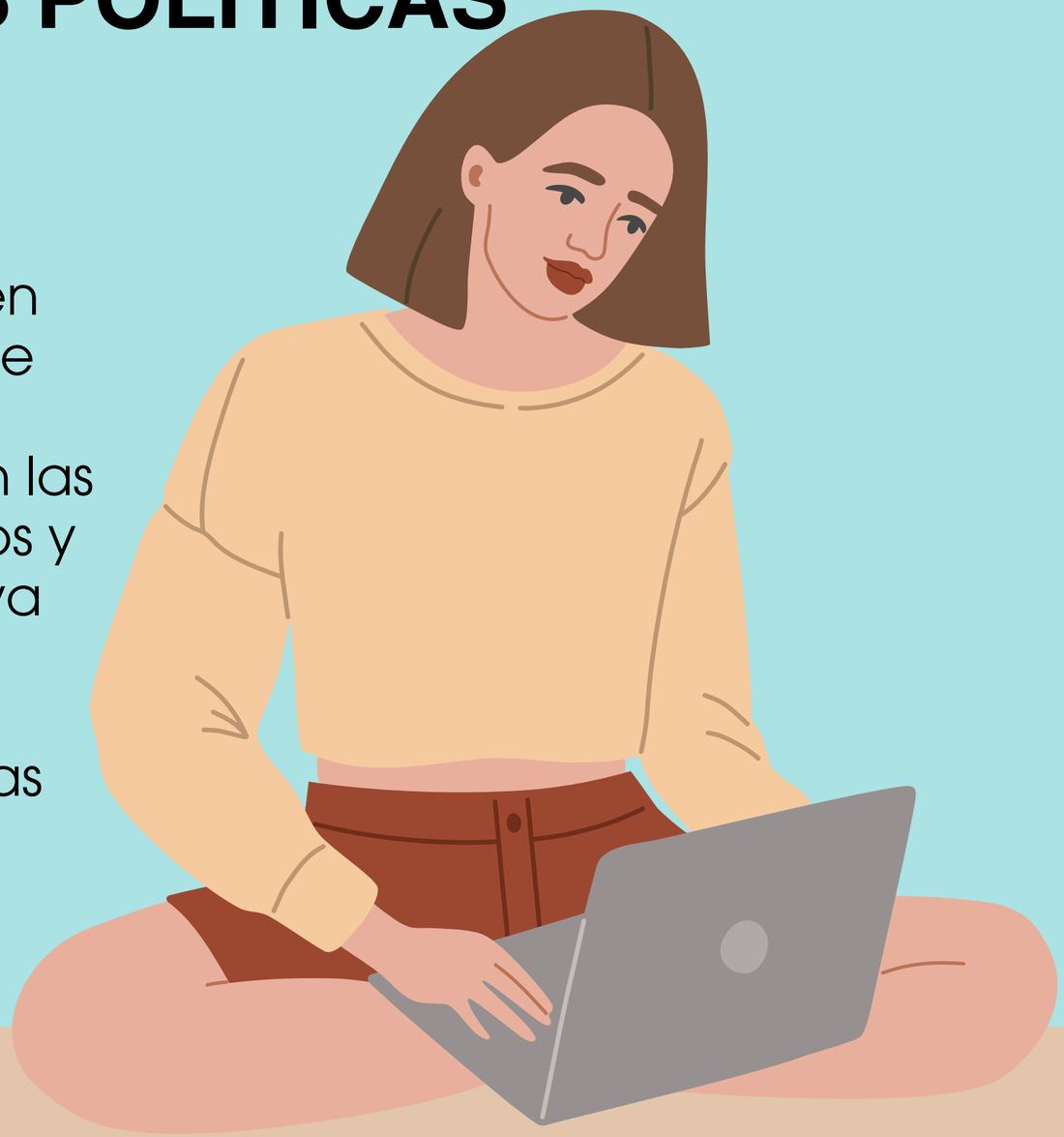
Protección contra amenazas cibernéticas:
Las amenazas cibernéticas, como el malware, ransomware, phishing, y ataques DDoS, están en constante evolución. Una estrategia de ciberseguridad ayuda a proteger la infraestructura de TI, los datos sensibles y los sistemas críticos de estos ataques.

Ventaja Competitiva:
Para destacar entre las demas empresas es necesario mantener una seguridad robusta ante cualquier amenaza que ponga en peligro información valiosa, maneteniendo una buena reputación y compromiso con los clientes.

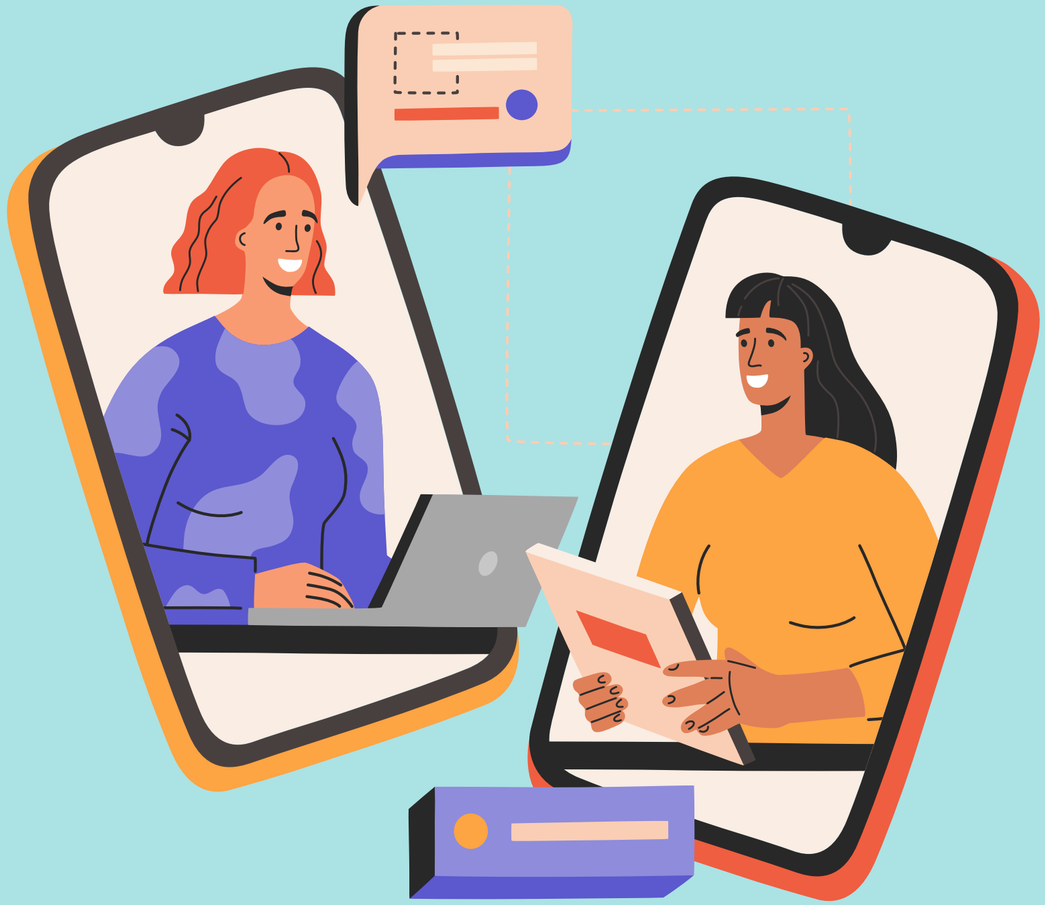
¿PARA QUE ME SIRVEN LAS POLÍTICAS DE SEGURIDAD?

Las políticas de seguridad sirven como herramientas para mantener ciertas medidas en cuanto al manejo de datos, a consecuencia de ello se logra establecer un ambiente seguro y confiable, reduciendo riesgos, cumpliendo con las regulaciones y garantizando que los empleados y sistemas funcionen de manera segura y efectiva

Basicamente funcionan como una guia para proteger los activos, la información y los sistemas de una organización.



CLAVES DE UNA BUENA ESTRATEGIA DE CIBERSEGURIDAD.



1.Evaliacion de riesgos: Es esencial conocer el fluejo de datos así como qué sistemas, datos y procesos son fundamentales en la organización. Una vez identificado sigue **analízar las vulnerabilidades** que existen en la infraestructura de TI.
Evaluación de amenazas y clasificación de riesgos.

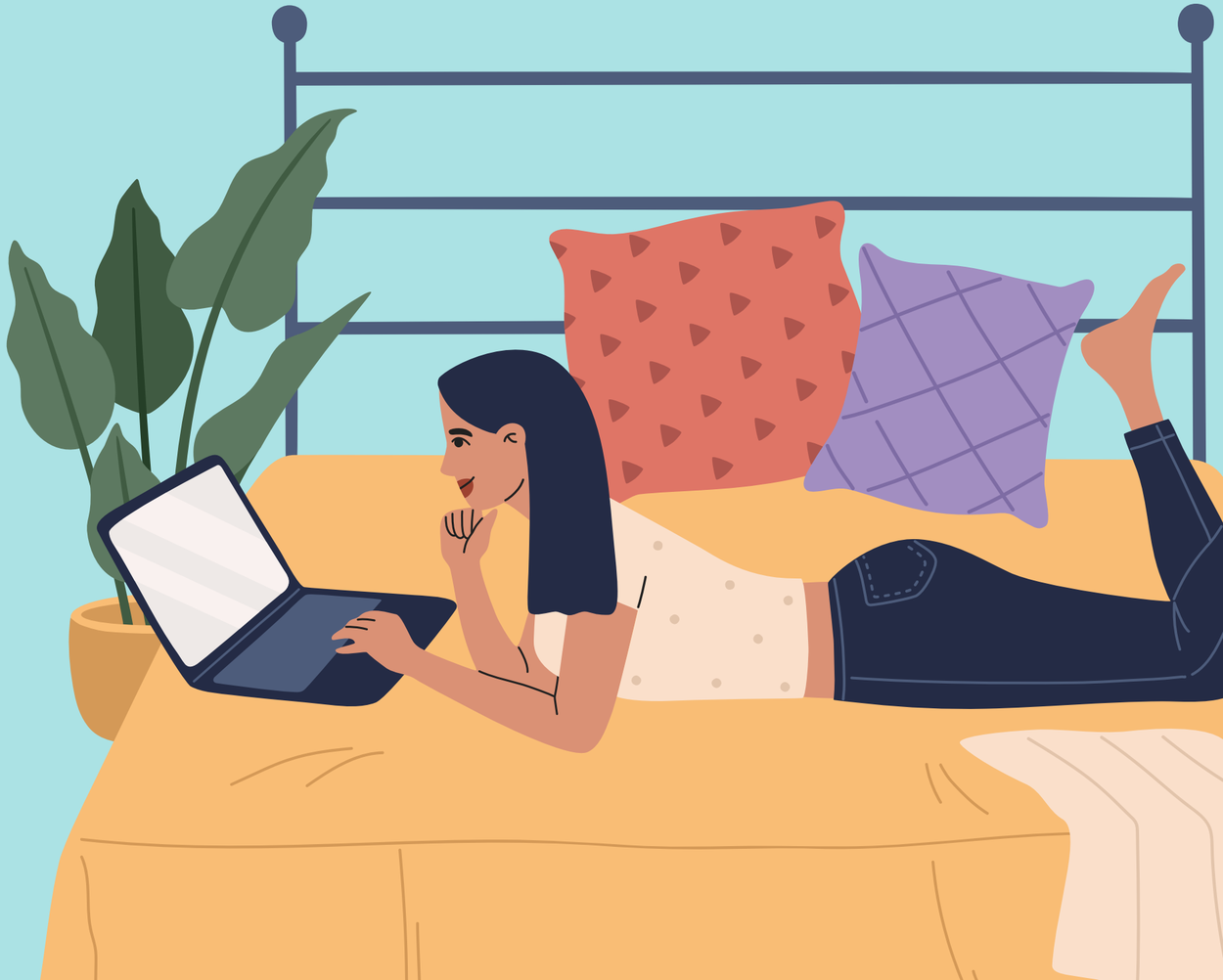
2. Defensa en profundidad: La implementación de múltiples capas de defensa(física, técnica y administrativa) que actúen en conjunto para proteger los sistemas,

3. Capacitación al personal que maneja los datos.

CLAVES DE UNA BUENA ESTRATEGIA DE CIBERSEGURIDAD.

4. Plan de respuesta ante incidentes: Desarrollo y testeo de planes de respuesta ante incidentes que incluyan pasos claros para identiciar, controlar, erradicar y recuperar sistemas afectados por ciberataques.

5. Actualización y Adaptabilidad Constante: La implementación de parches de seguridad y actualizaciones es una buena clave para proteger los sistemas contra nuevas vulnerabilidades.



POLÍTICAS EN MI CASA.

1. Gestión de contraseñas: Todos los dispositivos y cuentas deben usar contraseñas seguras utilizando caracteres especiales (recomendado).

2. Uso responsable de dispositivos: Evitar compatir datos sensibles como datos personales, números o información financiera, al igual evitar acceder a sitios o descargar información de dudosa procedencia,

3. Monitoreo de actividad en línea: Revisa regularmente el historial de navegación y el uso de datos para detectar cualquier actividad sospechosa o no autorizada.

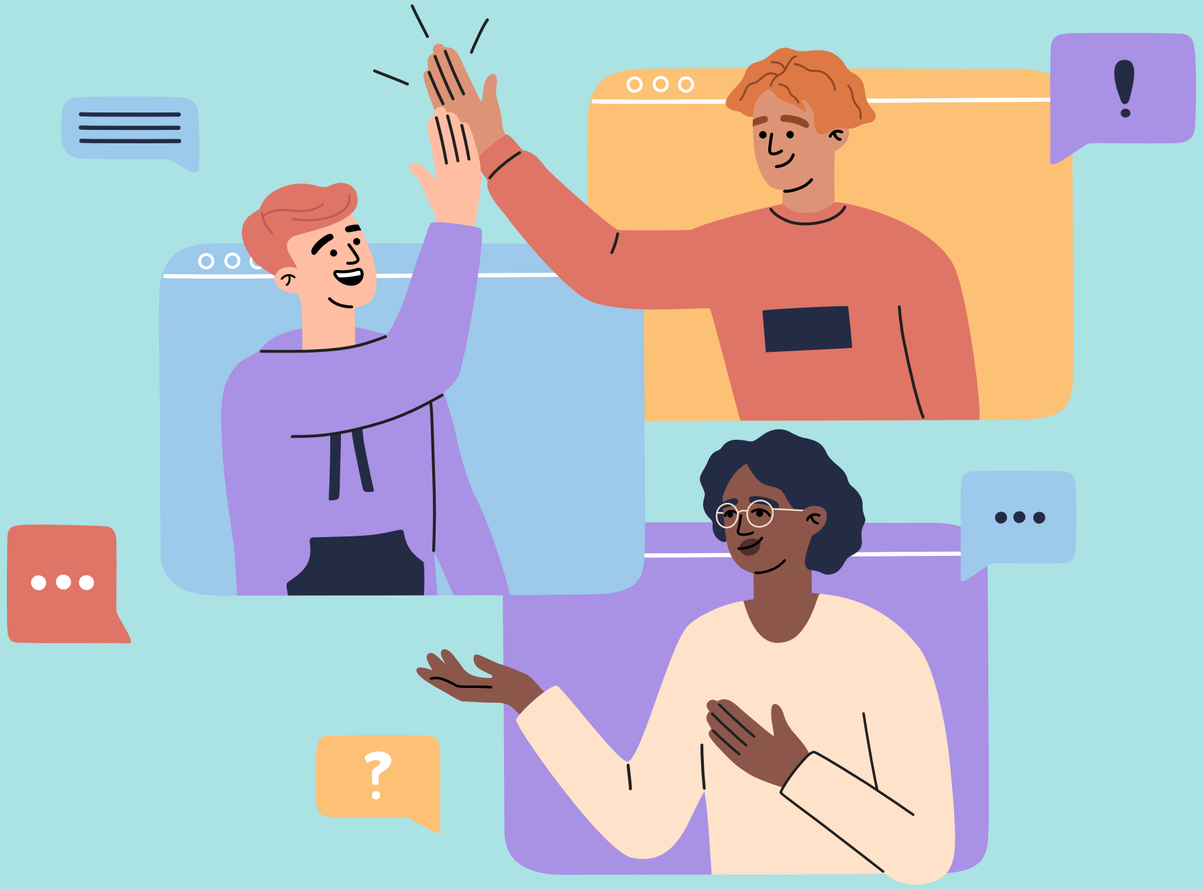
MIS PROPIAS POLÍTICAS

1.Red Wi-Fi:
Cifrado WPA3: Usar cifrado WPA3 en la red Wi-Fi para proteger las comunicaciones.

Cambio de contraseñas predeterminadas: Cambiar la contraseña del router y de la red Wi-Fi, evitando contraseñas simples.

Desactivar el WPS: Esto ayuda a evitar accesos no autorizados a la red.

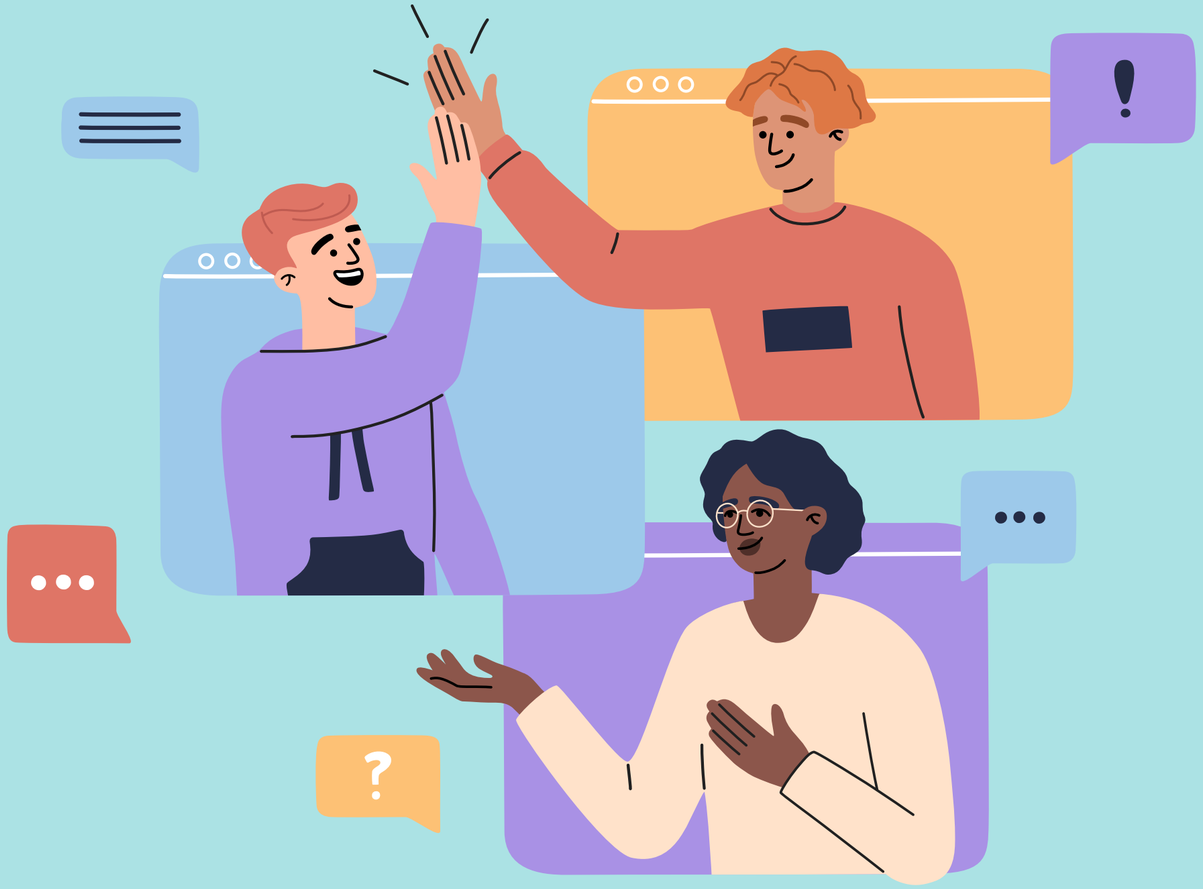
2. Dispositivos (Pc y moviles):
Antivirus y anti-malware: Instalar un software de antivirus confiable y activo en todos los dispositivos.
Contraseñas: Usar contraseñas que no sean faciles de adivinar e implementar el uso de autentificación biométrica,



MIS PROPIAS POLÍTICAS

3. Uso responsable de aplicaciones:
Descarga de contenido: Siempre descargar información, aplicaciones, etc de tiendas oficiales para evitar softwares malignos.
Control de permisos: Revisar y limitar los permisos a las aplicaciones que se descarguen especialmente a las aplicaciones que solicitan este tipo de datos personales.

4. Respaldo de información: Es necesario mantener y realizar copias de seguridad constante en caso de perdida de información.



BIBLIOGRAFÍA

HTTPS://WWW.IBM.COM/DOCS/ES/I/7.3?TOPIC=SECURITY-POLICY-OBJECTIVES

HTTPS://WWW.GLUHINTERNACIONAL.COM/BLOG/5-ESTRATEGIAS-QUE-MEJORARAN-LA-SEGURIDAD-DE-TU-EMPRESA
HTTPS://WWW.CHECKPOINT.COM/ES/CYBER-HUB/CYBER-SECURITY/WHAT-IS-CYBERSECURITY/HOW-TO-DEVELOP-A-CYBER-SECURITY-STRATEGY/