



CONFIANZA DIGITAL

CONSTRUYENDO UN FUTURO TECNOLÓGICO SEGURO

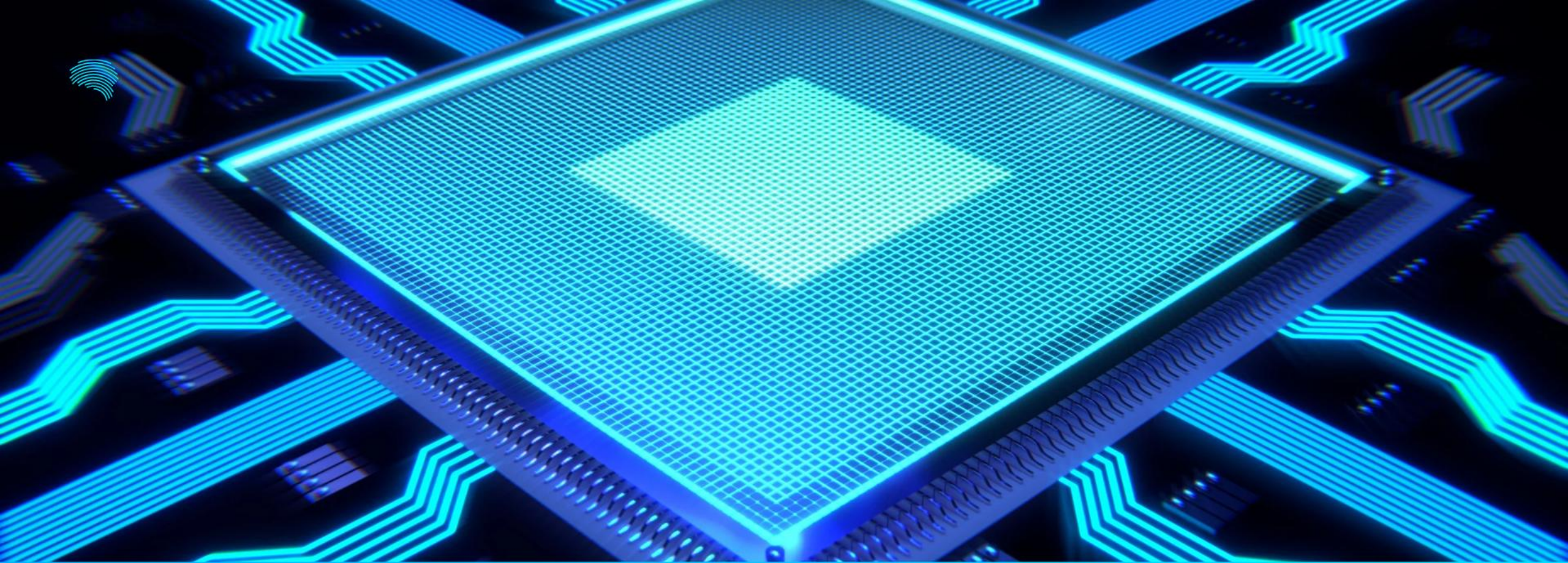
AGENDA

- ❑ QUÉ ES CONFIANZA DIGITAL
- ❑ BOMBARDEO DE INFORMACIONES
- ❑ MUNDO DIGITAL
- ❑ SEGURIDAD - PRIVACIDAD - EDUCACIÓN - CONCIENTIZACIÓN
- ❑ PROTECCIÓN DE PRIVACIDAD
- ❑ PROBLEMAS QUE AFECTAN LA CONFIANZA DIGITAL
- ❑ PROTECCIÓN DE LA PRIVACIDAD EN LÍNEA
- ❑ EDUCACIÓN TECNOLÓGICA
- ❑ CONCIENTIZACIÓN TECNOLÓGICA
- ❑ ENTORNO DIGITAL - PROTECCIÓN RESILIENTE
- ❑ BUENAS PRÁCTICAS CON IMPACTO INMEDIATO
- ❑ CONFIANZA DIGITAL EN TU ENTORNO



LA GRAN PREGUNTA

¿Por qué Confianza Digital?



CONFIANZA DIGITAL

Se refiere a la seguridad y fiabilidad que sienten al interactuar con tecnologías digitales y servicios en línea.

Este concepto abarca varios aspectos:

1. Protección de datos personales
2. Seguridad cibernética
3. Transparencia en el uso de la información
4. Integridad de las transacciones digitales.





En un mundo cada vez más digitalizado, la confianza digital es crucial para fomentar la adopción de nuevas tecnologías y servicios. Ya que las empresas y organizaciones deben implementar medidas robustas de seguridad y privacidad para ganar y mantener la confianza de sus usuarios.

Esto incluye el uso de encriptación, autenticación multifactor, políticas claras de privacidad y la respuesta rápida a incidentes de seguridad.



Además, la confianza digital también implica la educación y concientización de los usuarios sobre las mejores prácticas de seguridad en línea, como la creación de contraseñas seguras y la identificación de posibles amenazas cibernéticas.

Puntualizamos estos datos:

1. Seguridad ☒
2. Privacidad ☒
3. Educación ☒
4. Concientización ☒

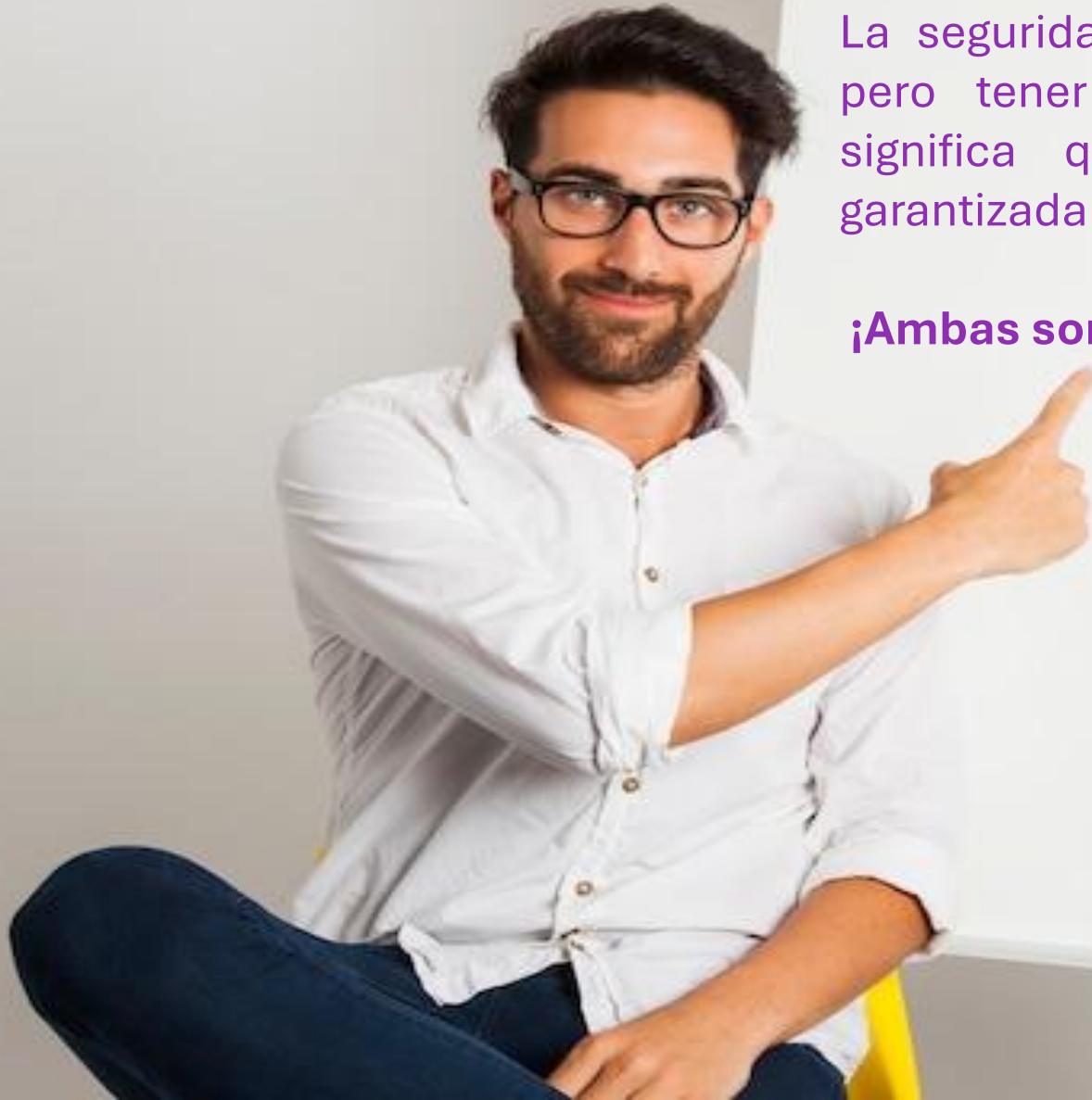




PIENSEN ESTO

La seguridad protege la privacidad, pero tener seguridad no siempre significa que tu privacidad esté garantizada.

¡Ambas son esenciales!



Proteger tu privacidad es clave en un mundo digital lleno de riesgos. Aquí te muestro algunas de las mejores prácticas para mantener tu información personal segura.

1. Usa contraseñas seguras y únicas
2. Activa la autenticación en dos pasos
3. Ten cuidado con la información que compartes
4. Revisa y ajusta configuraciones de privacidad
5. Utiliza redes seguras y evita el Wi-Fi público
6. Mantén tus dispositivos y aplicaciones actualizados
7. Desconfía de enlaces sospechosos y correos desconocidos
8. Limita el rastreo en línea
9. Revisa permisos de aplicaciones
10. Borra datos y cuentas que ya no uses



APLICAR ESTOS CONSEJOS TE AYUDARÁ A MANTENER EL CONTROL DE TU INFORMACIÓN PERSONAL Y EVITAR POSIBLES RIESGOS



PROBLEMAS COMUNES QUE AFECTAN DIRECTAMENTE LA CONFIANZA DIGITAL

- Phishing
- Malware
- Robo de identidad
- Ataques de fuerza bruta
- Fugas de datos
- Fraude en compras en línea
- Secuestro de cuentas
- Spyware
- Ataques DDoS (Denegación de servicio distribuido)
- Exposición excesiva en redes sociales

Proteger la privacidad en línea es fundamental y es un compromiso de todos

1. VPN (Red privada virtual)
2. Navegadores enfocados en privacidad
3. Bloqueadores de rastreadores y anuncios
4. Administradores de contraseñas
5. Autenticación en dos pasos (2FA)
6. Servicios de correo electrónico privados
7. Motores de búsqueda privados
8. Sistemas de almacenamiento cifrado
9. Extensiones de privacidad para navegadores
10. Mensajería cifrada de extremo a extremo



- En el ámbito tecnológico, educación y concientización trabajan juntas para crear una sociedad digital más segura, informada y responsable.

Educación Tecnológica

Proporciona conocimientos y habilidades sobre el uso de herramientas digitales, programación, ciberseguridad y más. Por ejemplo, aprender sobre la importancia de las contraseñas seguras o cómo proteger datos personales en línea es parte de la educación digital.

Concientización Tecnológica

Va más allá del aprendizaje técnico; busca sensibilizar a las personas sobre los riesgos y responsabilidades del uso de la tecnología. Un ejemplo es la concientización sobre los peligros del phishing.

No basta con saber usar la tecnología, también es esencial entender sus efectos y actuar de manera ética y segura.

ENTORNO DIGITAL – PROTECCION RESILIENTE

Mantener un entorno digital seguro es fundamental para evitar amenazas y proteger datos personales.

1. Seguridad en Dispositivos y Redes

- ✓ Mantén software actualizado
- ✓ Usa antivirus y firewall
- ✓ Redes seguras

2. Protección de Cuentas y Datos

- ✓ Contraseñas seguras y únicas
- ✓ Encriptación de datos
- ✓ Copias de seguridad

3. Concientización y Educación Digital

- ✓ Reconocer riesgos
- ✓ Evitar enlaces y archivos sospechosos
- ✓ Configurar privacidad en redes sociales

4. Buenas Prácticas en Empresas y Organizaciones

- ✓ Políticas de seguridad informática
- ✓ Capacitación continua
- ✓ Monitoreo de actividad sospechosa

**LA PROTECCION DIGITAL, VA MAS ALLA DE PONER CANDADOS....
ES CONOCER Y SABER COMO ACTUAR**

Aplica buenas prácticas **CON IMPACTO INMEDIATO**

Comprende el impacto real de la desinformación, la pérdida de datos y las barreras a la transformación digital desde una perspectiva integral.

1. Riesgos en la Seguridad Digital

- ✓ Ataques cibernéticos facilitados por información falsa
- ✓ Phishing y fraudes
- ✓ Manipulación de percepciones

2. Impacto en la Privacidad

- ✓ Exposición de datos personales
- ✓ Robo de identidad
- ✓ Seguimiento y perfilado indebido

3. Consecuencias Sociales y Tecnológicas

- ✓ Pánico y decisiones erróneas
- ✓ Debilitamiento de la confianza en plataformas digitales
- ✓ Desestabilización de procesos democráticos

Verificar la autenticidad de la información, usar fuentes confiables y oficiales, fomentar la educación digital, DEBE SER UN PRINCIPIO, NO UNA ACCIÓN.

Confianza Digital EN TU ENTORNO

Fomentar la adopción de tecnologías emergentes a través de la construcción de entornos seguros y transparentes. GENERA CONFIANZA

- ✓ **Cumplir con normativas de protección de datos**
- ✓ **Desarrollar plataformas resilientes**
- ✓ **Explicar claramente cómo funcionan las tecnologías**
- ✓ **Políticas de privacidad accesibles**
- ✓ **Mostrar los beneficios y riesgos**
- ✓ **Capacita a tu entorno**
- ✓ **Crear documentación clara**
- ✓ **Fomentar la cultura digital**
- ✓ **Retroalimentación Constante**
- ✓ **Involucrar, Ajusta estrategias**
- ✓ **En las pruebas, hazlo parte y muéstrale las soluciones**
- ✓ **HAZLO PARTE DEL CAMBIO**

INVOLUCRAR A TODAS LAS PARTES, ES TENER UN GRAN EQUIPO



Muchas Gracias!

