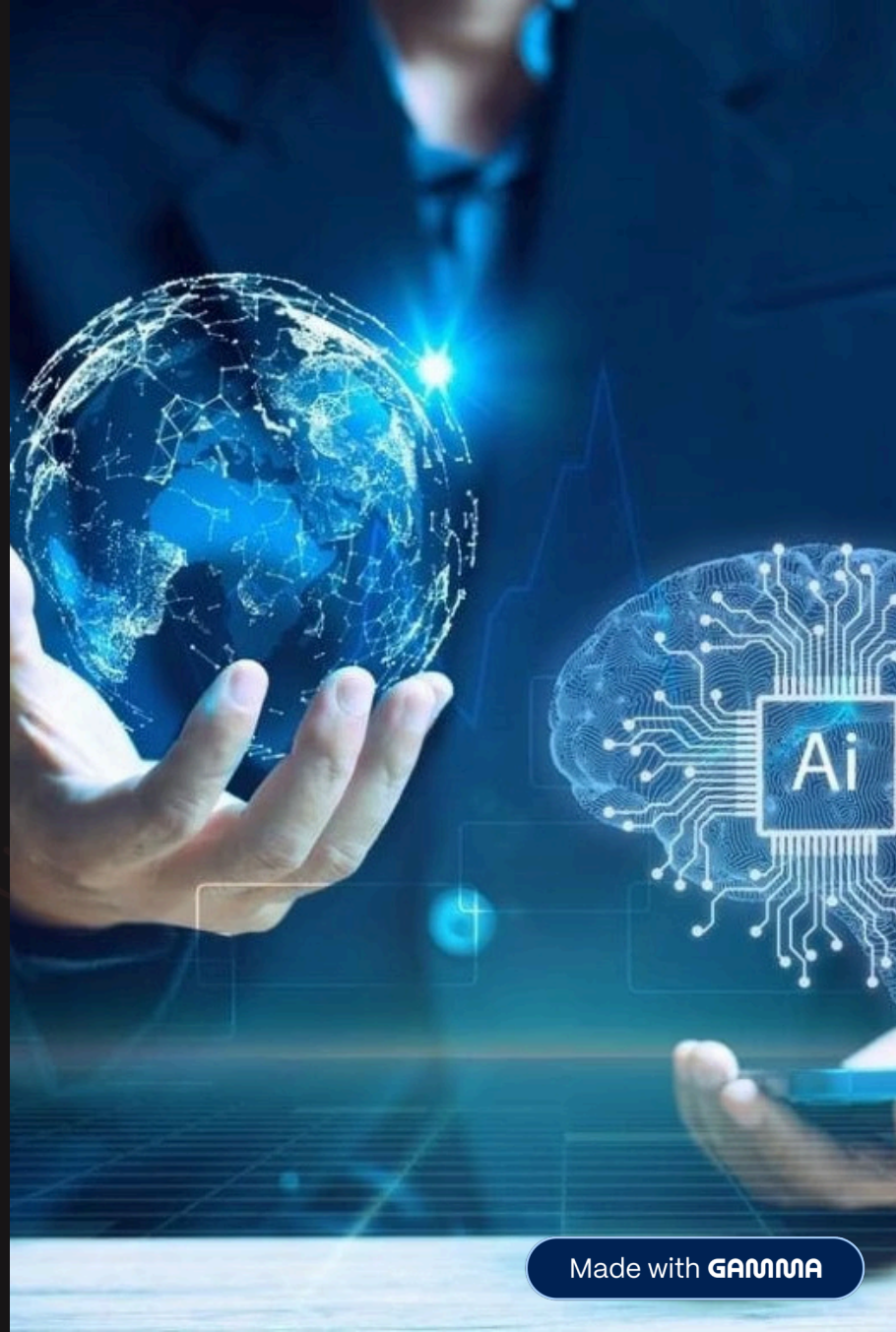
Gestión de Riesgos

Gestión de Riesgos en la Identidad Digital: El Reto de 2026

Integrantes del equipo: Santiago Sahid, Nikolas Hernandez, David Ballesteros, Sebastian Camacho.



Identidad Física vs. Identidad Digital

Concepto Clave: La identidad digital es ubicua, permanente y explotable a escala global.

Identidad Física:

- Controlada
- Tangibilidad corpórea
- Verificación presencial

Identidad Digital:

- Datos distribuidos
- Fácilmente replicable
- Control parcial por terceros

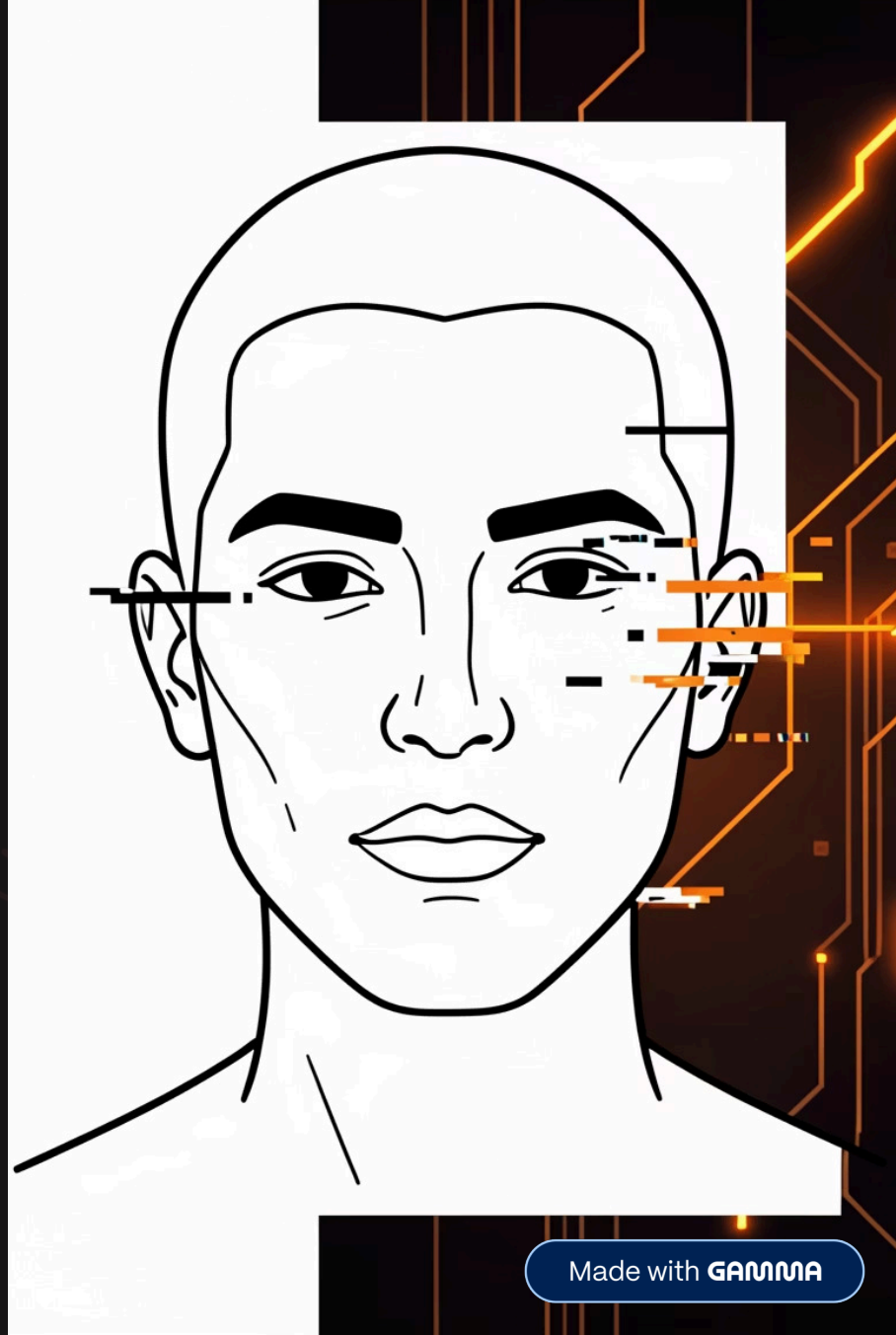
Tipos de Datos: Declarados, Actuantes e Inferidos.

Amenaza Crítica #1 - IA y Deepfakes

El auge del Fraude Impulsado por IA (Proyección 2026)

Datos clave:

- Crecimiento del fraude habilitado por IA estimado en 32% anual.
- Existencia de "Deepfake-as-a-service" y kits de identidad para eludir verificaciones.
- Riesgo sistémico para gobiernos y empresas según Kaspersky.



Amenaza Crítica #2 - Suplantación y Onboarding

Problema: Los métodos tradicionales (Selfie + Cédula) son obsoletos.

Nuevos Vectores:

Identidades Sintéticas: Mezcla de datos reales y ficticios.

Fraude en Fintech: Alto riesgo en créditos instantáneos y pagos en tiempo real en LATAM.

Amenaza Crítica #3 - Pérdida de Privacidad

Pérdida de Control y Filtraciones Masivas

El Ciclo del Riesgo:

- Usuarios sin visibilidad de sus datos inferidos o actuantes.
- Filtraciones que alimentan ataques de "Credential Stuffing".
- Perfilado algorítmico sin consentimiento informado.

Decálogo de Buenas Prácticas (Higiene Digital)

Mitigación y Protección del Usuario

1

Contraseñas fuertes

(>12 caracteres) y Gestores de contraseñas.

2

Autenticación Multifactor (MFA)

en todo (No usar SMS).

3

Desconfianza "Zero Trust"

ante videollamadas (por Deepfakes).

4

Auditoría trimestral

de perfiles y permisos.

La Paradoja de la Seguridad (Gráfico Conceptual)

Concepto Central: La confianza en sistemas tradicionales se ha erosionado.

El Ciclo Paradójico:

- Necesitamos Mayor Verificación para protegernos.
- Pero mayor verificación implica Más Datos Expuestos.
- Más datos expuestos generan Más Oportunidades de Fraude.

Solución Integral y Alineación ISO (Conclusión)

Hacia una Solución Integrada

Tecnología:

- Biometría "Liveness" (prueba de vida)
- IA defensiva.

Regulación y Estándares:

- ISO 31000: Para la gestión estratégica del riesgo.
- ISO 27001: Para la seguridad de la información.

"Ya no basta una contraseña fuerte; necesitas pensamiento defensivo continuo".