Biometría
Fintechgración

CÁPSULA 4

SEGURIDAD: UN TOQUE HUMANO PARA CADA DISPOSITIVO

LA SEGURIDAD SIEMPRE ES EXCESIVA HASTA QUE NO ES SUFICIENTE.

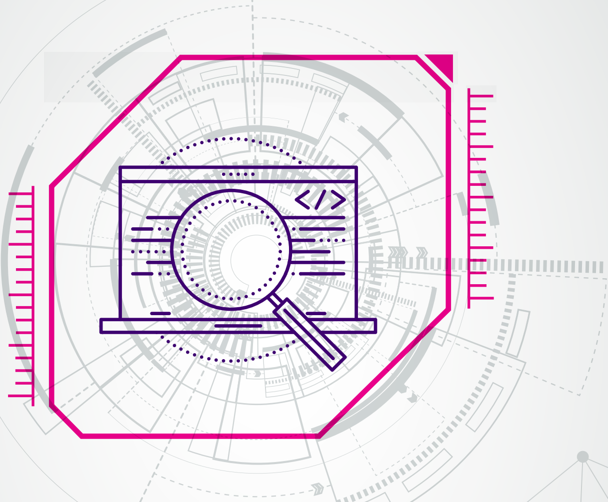
ROBBIE SINCLAIR

SI LAS PRINCIPALES PREOCUPACIONES
EN LA IMPLEMENTACIÓN DE
SISTEMAS BIOMÉTRICOS

POR PARTE DE LAS INSTITUCIONES
SON LOS COSTOS ASOCIADOS Y LA
CONFIABILIDAD DE LA TECNOLOGÍA,

LA PRIMORDIAL PREOCUPACIÓN A
CONSIDERAR POR LOS USUARIOS RECAE
EN LA PRIVACIDAD DE SU INFORMACIÓN.

LOS USUARIOS CADA VEZ SON MÁS
CONSCIENTES DE QUE ES NORMAL QUE SUS
RASGOS BIOMÉTRICOS ESTÉN EXPUESTOS,



A DIFERENCIA DE LAS CONTRASEÑAS,
QUE PERMANECEN SECRETAS.

ESTO FACILITA QUE LAS PERSONAS
PUEDAN SER IDENTIFICADAS
FÁCILMENTE CON O SIN SU PERMISO.

POR EJEMPLO, AHORA ES POSIBLE
ENCONTRAR EL PERFIL DE UNA PERSONA
EN REDES SOCIALES CON SOLO TOMARLE
UNA FOTO Y USANDO UNA APLICACIÓN,

TAL Y COMO SUCEDE EN RUSIA
CON LA APP FINDFACE[1].

1- TheEconomist, 2017. What machines can tell from your face. Disponible en https://www.economist.com/news/leaders/21728617-life-age-facial-recognition-what-machines-can-tell-your-face

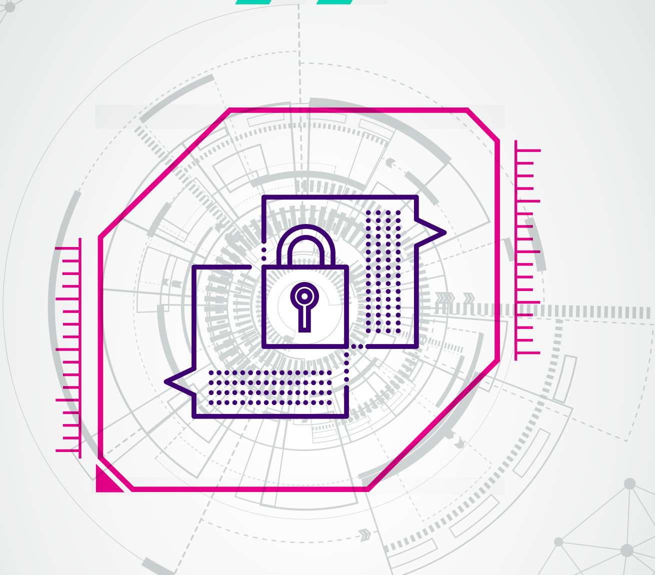
ASIMISMO, FACEBOOK PODRÍA OBTENER IMÁGENES DEL INTERIOR **DE UN CONCESIONARIO E IDENTIFICAR A LOS VISITANTES**

PARA LUEGO ENVIARLES PUBLICIDAD **RELACIONADA CON CARROS.**

POR TAL RAZÓN, PARA QUE **LAS INTERACCIONES MIGREN A LO DIGITAL, LOS USUARIOS DEBEN CONTAR CON DOS GARANTÍAS**

RESPECTO A SUS DATOS:

QUE SON USADOS **CORRECTAMENTE.**



QUE ESTÁN BIEN
PROTEGIDOS.

CON LOS ATAQUES CIBERNÉTICOS
CADA VEZ MÁS SOFISTICADOS,

LAS MEDIDAS DE SEGURIDAD
TAMBIÉN DEBEN SER
MÁS INTELIGENTES.

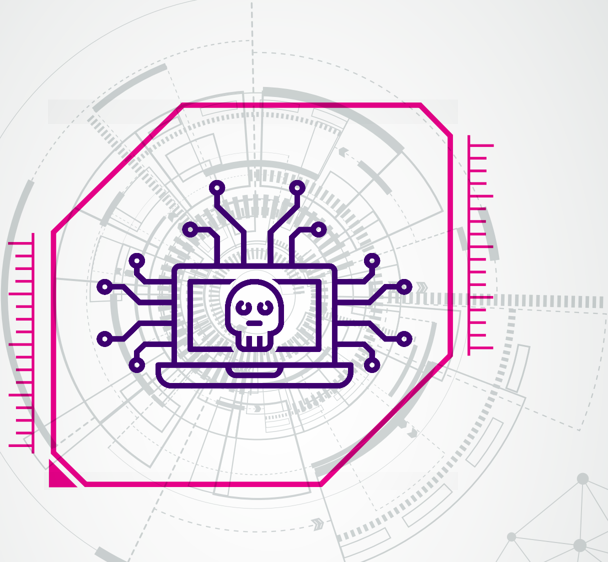
EN TODO CASO, HAY QUE CONSIDERAR **QUE NINGUNA TECNOLOGÍA HA** PROBADO SER INQUEBRANTABLE.

CON EL TIEMPO Y DINERO SUFICIENTES ES POSIBLE VULNERAR **CUALQUIER SISTEMA DE SEGURIDAD.**

INCLUSO BLOCKCHAIN –"LA TECNOLOGÍA MÁS SEGURA" – SE VE AMENAZADA ANTE EL ALCANCE **AÚN DESCONOCIDO DE LA COMPUTACIÓN CUÁNTICA[2].**

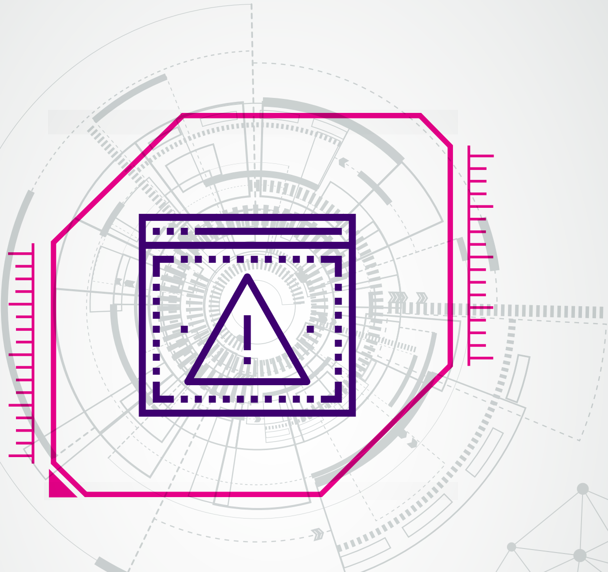
2- SingularityHub, 2017. Is Quantum Computing an Existential Threat to Blockchain Technology?. Disponible en https://singularityhub.com/2017/11/05/is-quantum-computing-an-existential-threat-to-blockchain-technology/#sm.00001qz7us8twhdp2r70d702ehck3

LA ÚNICA MEDIDA PREVENTIVA QUE QUEDA **PARA LA PROTECCIÓN DE LA INFORMACIÓN** ES HACER LA VULNERACIÓN DEL SISTEMA **TAN COSTOSA DE REALIZAR**



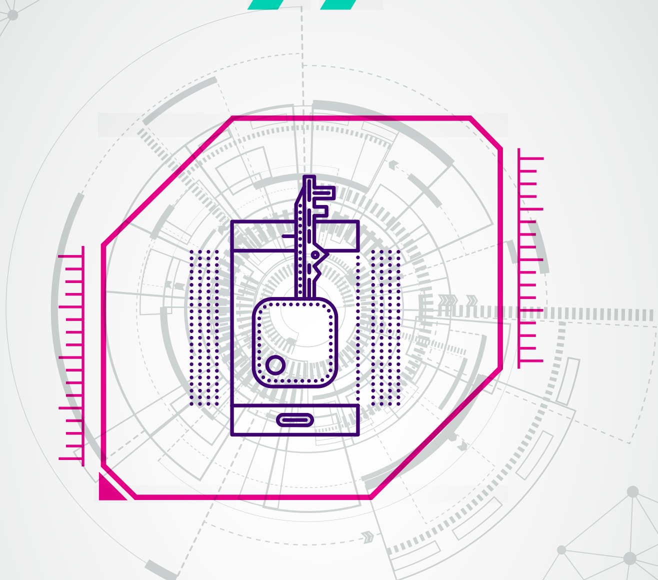
QUE LOS BENEFICIOS DE UN ATAQUE EXITOSO NO VALGAN LA PENA.

PARA AVANZAR EN ESE COMETIDO
HAY QUE ESTAR SIEMPRE ALERTA
FRENTE A NUEVOS RIESGOS



Y, ANTE TODO, CONTAR CON LA
COLABORACIÓN DE TODAS LAS
PARTES INVOLUCRADAS:

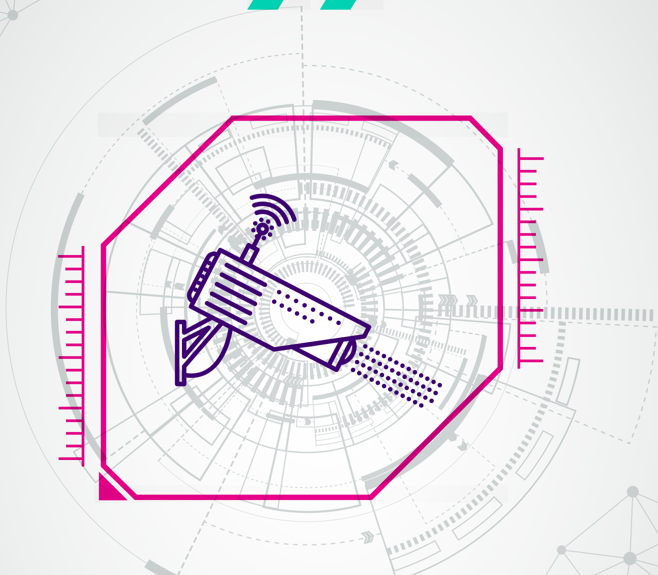
LOS BANCOS Y ORGANIZACIONES, EN RELACIÓN CON LOS SISTEMAS DE **SEGURIDAD IMPLEMENTADOS.**



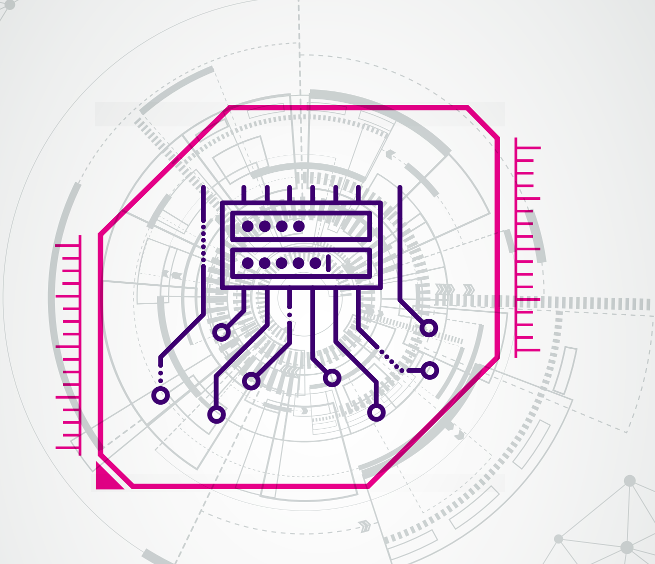
LOS CLIENTES, A TRAVÉS

DEL USO CONSCIENTE DE INTERNET

Y DE SUS DISPOSITIVOS.



LA POLICÍA Y LA LEY, CON AVANCES **EN LA JUDICIALIZACIÓN ADECUADA DE DELITOS CIBERNÉTICOS.**



LOS DESARROLLADORES DE TECNOLOGÍA, EN RELACIÓN CON LA **SOFISTICACIÓN, ESTANDARIZACIÓN Y CONFIABILIDAD DE LA TECNOLOGÍA.**

TAMBIÉN ES IMPORTANTE CONTAR CON BUENAS PRÁCTICAS Y TÁCTICAS QUE PUEDEN INUTILIZAR LA INFORMACIÓN BIOMÉTRICA,

SALVO PARA EL USUARIO GENUINO, UNA VEZ ESTÁ EN MANOS DE LOS DELINCUENTES:

MEJORAR LA DETECCIÓN DE VIDA:

ES IMPORTANTE AVANZAR EN LA SOFISTICACIÓN DE **LA TECNOLOGÍA**

DE TAL MANERA QUE PERMITA **DIFERENCIAR UNA BIOMETRÍA FALSA DE UNA VERDADERA.**

QUE UTILICE ALGORITMOS AVANZADOS ***DE MACHINE LEARNING* (INTELIGENCIA** ARTIFICIAL) Y SE ACTUALICE FRENTE A **NUEVAS AMENAZAS.**

USAR SISTEMAS DE AUTENTICACIÓN MULTI-MODAL Y DE MÚLTIPLES FACTORES:

EN LA MEDIDA QUE SEA PRÁCTICO, LAS **INSTITUCIONES DEBEN CONSIDERAR EL USO** DE MÁS DE UN FACTOR DE AUTENTICACIÓN **PARA DARLES MAYOR SEGURIDAD**

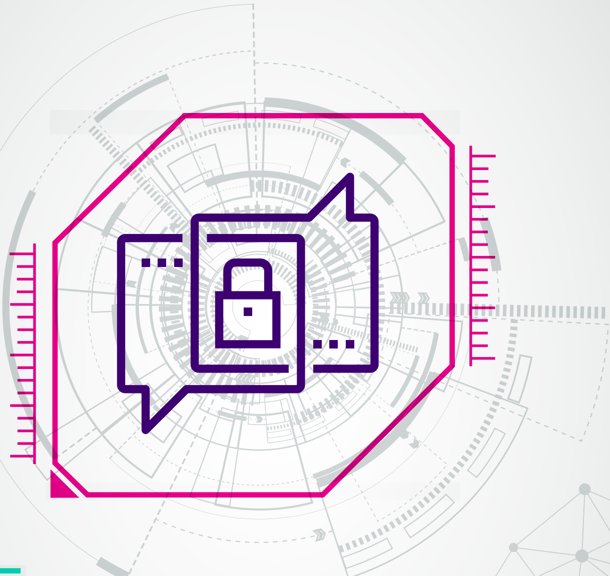
Y MEJOR PROBABILIDAD DE RECONOCIMIENTO A SUS SISTEMAS.

ROBUSTECER LAS PLANTILLAS BIOMÉTRICAS:

TENER UNA PLANTILLA BIOMÉTRICA COMBINADA CON OTRA INFORMACIÓN, COMO **UNA CLAVE DINÁMICA (OTP EN INGLÉS),**

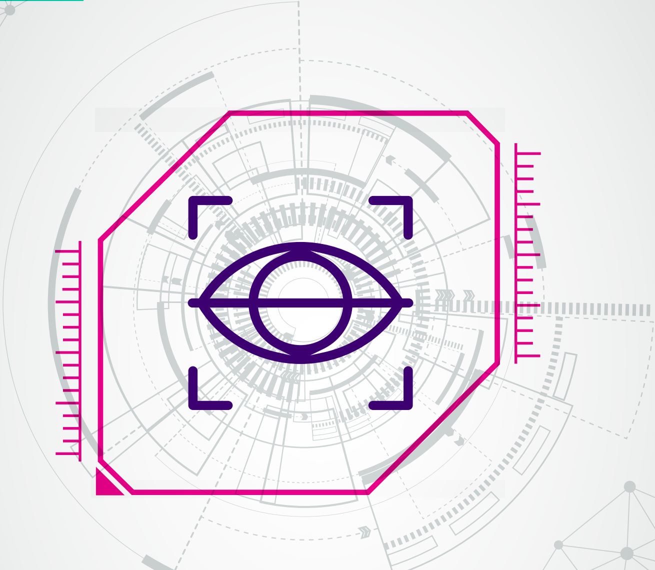
PERMITIRÍA A LOS SISTEMAS RECONOCER Y **RECHAZAR UNA PLANTILLA FRAUDULENTA.**

HACER LA IDENTIDAD MÁS RESISTENTE



TODOS LOS ELEMENTOS INVOLUCRADOS EN LA **CAPTURA Y EL USO DE DATOS BIOMÉTRICOS DEBEN** PODER ENCRIPTARSE Y VOLVERSE RESISTENTES **A TÉCNICAS FRAUDULENTAS.**

POR AHORA, EN UN HORIZONTE DE TIEMPO CERCANO LA AUTENTICACIÓN **DE MÚLTIPLES FACTORES**



(SIEMPRE Y CUANDO INVOLUCRE LA BIOMETRÍA) ES EL MÉTODO MÁS ROBUSTO PARA ACCEDER A DISTINTOS SERVICIOS[3].

3- Gemalto. Ultima vez accedido el 20 de marzo de 2018.
https://safenet.gemalto.es/multi-factor-authentication

EN ÚLTIMAS, EL SECTOR FINANCIERO **TIENE LA GRAN OPORTUNIDAD DE SER** LÍDERES EN EL ALMACENAMIENTO

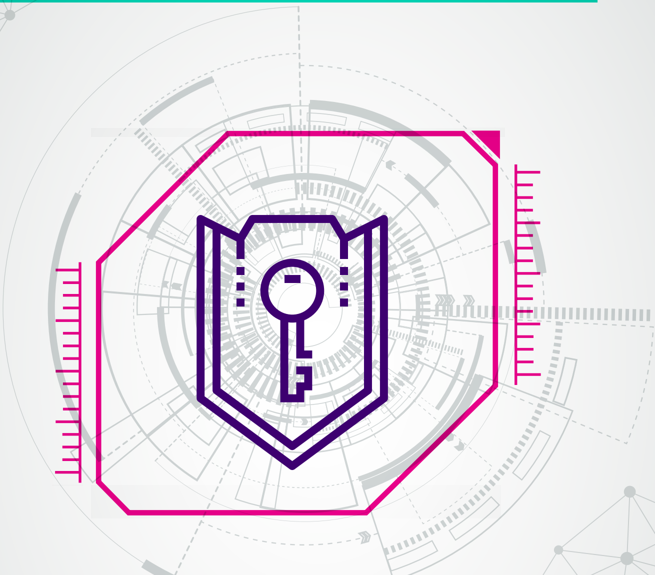
DE LA INFORMACIÓN

DEBIDO A SUS NIVELES DE SEGURIDAD Y ADAPTACIÓN CONSTANTE FRENTE A

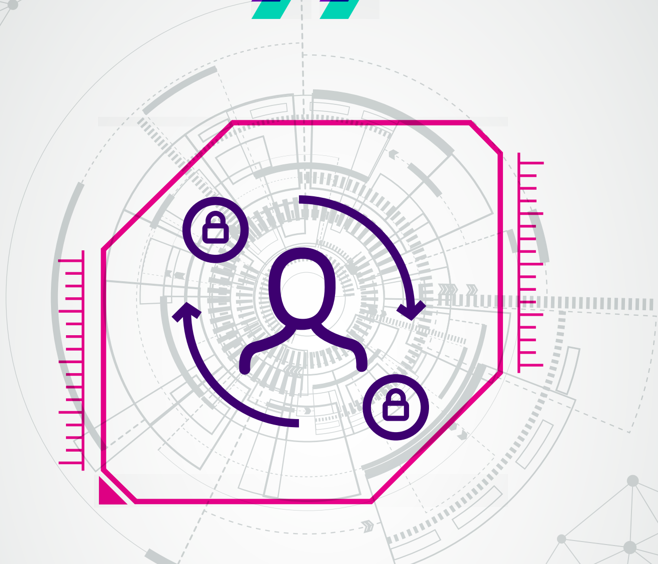
NUEVAS AMENAZAS.

SIN EMBARGO, PARA SEGUIR CONSTRUYENDO

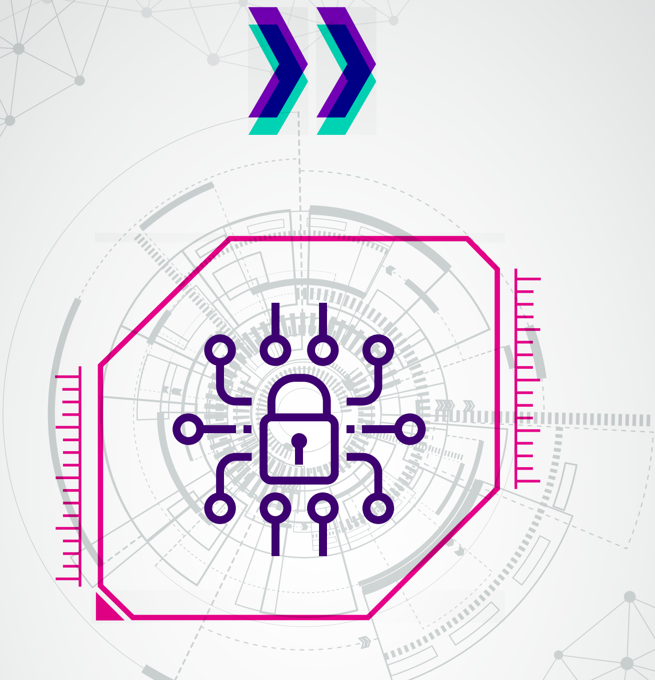
SU REPUTACIÓN EN PRIVACIDAD DE DATOS



Y SEGURIDAD ROBUSTA,
DEBEN SUBIR EL NIVEL EN
DISTINTAS DIMENSIONES:

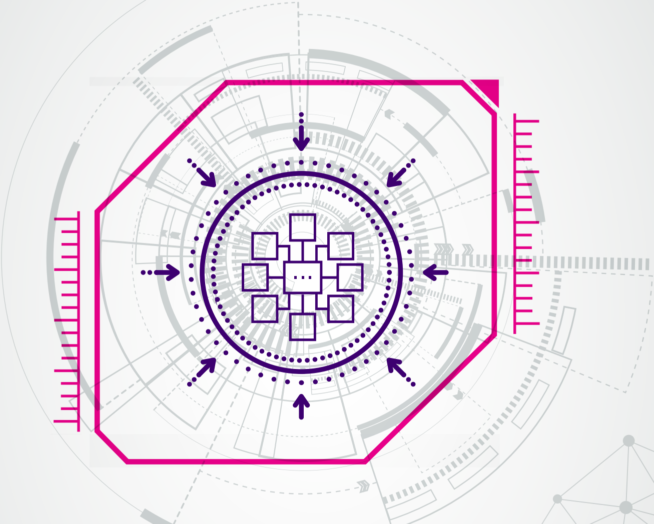


ALINEAR LAS PRÁCTICAS DE CAPTURA Y PROTECCIÓN DE DATOS CON LAS EXPECTATIVAS DE LOS CONSUMIDORES.



ENCONTRAR FORMAS INNOVADORAS DE
PROPORCIONAR SEGURIDAD NO INTRUSIVA
A LOS CONSUMIDORES.

DESARROLLAR LAS CAPACIDADES NECESARIAS PARA MONITOREAR **Y ADAPTARSE A LOS RIESGOS CIBERNÉTICOS EN TIEMPO REAL.**



REVISAR EL MODELO DE **GOBERNANZA DE DATOS.**

AL FINAL, LAS CONSIDERACIONES EN **PRIVACIDAD Y SEGURIDAD DIGITAL** LES OFRECERÁ A LOS BANCOS UNA **VENTAJA COMERCIAL ESTRATÉGICA**

QUE IMPULSARÁ UNA MAYOR ADOPCIÓN DE CANALES DIGITALES **DE MENOR COSTO OPERACIONAL Y ATRAERÁ A NUEVOS CLIENTES**[4].

4- Capgemini, 2017. The Currency of Trust: Why Banks and Insurers Must Make Customer Data Safer and More Secure. Disponible en https://www.capgemini.com/consulting/resources/data-privacy-and-cybersecurity-in-banking-and-insurance/

"La disrupción del sistema financiero no va a suceder, está sucediendo"

Bienvenidos a la Fintechgración