

Compliance Digital

El futuro de la prevención de riesgo



Oscar H. Moratto Santos
Consultor Asociado
omoratto@ricsmanagement.com

Bogotá D.C.
Septiembre de 2020

rics
management

riesgo • inteligencia • cumplimiento • seguridad

Oscar Humberto Moratto Santos

- Ingeniero Civil y Especialista en Finanzas de la Universidad de Los Andes, con estudios de maestría en Economía de la misma Universidad.
- Ex subdirector de Análisis de Operaciones de la Unidad de Información y Análisis Financiero UIAF.
- Certificado ISO 31000 lead risk manager por PECB y entrenador certificado ISO 31000.
- Experiencia en actividades ALA/AFT, Inteligencia de Negocios, metodologías de administración de riesgos (COSO, ISO 31000, estándar australiano), gerencia y coordinación de proyectos, manejo presupuestal y de recursos.
- Experiencia en implementación de modelos analíticos de estructuración de negocios financieros y cuantificación de riesgos, desarrollo de software y gerencia de proyectos en las áreas de finanzas, ingeniería, toma de decisiones bajo incertidumbre y simulación.
- Conferencista nacional e internacional en temáticas de ALM/CTF.
- Consultor Asociado de [rics management](#).



Agenda

- Relevancia de la tecnología en compliance
- Cómo la tecnología apoya procesos de cumplimiento
- Compliance digital vs. Tradicional
- Beneficios de los sistemas de identidad y compliance digital
- Reflexiones
- Conclusiones

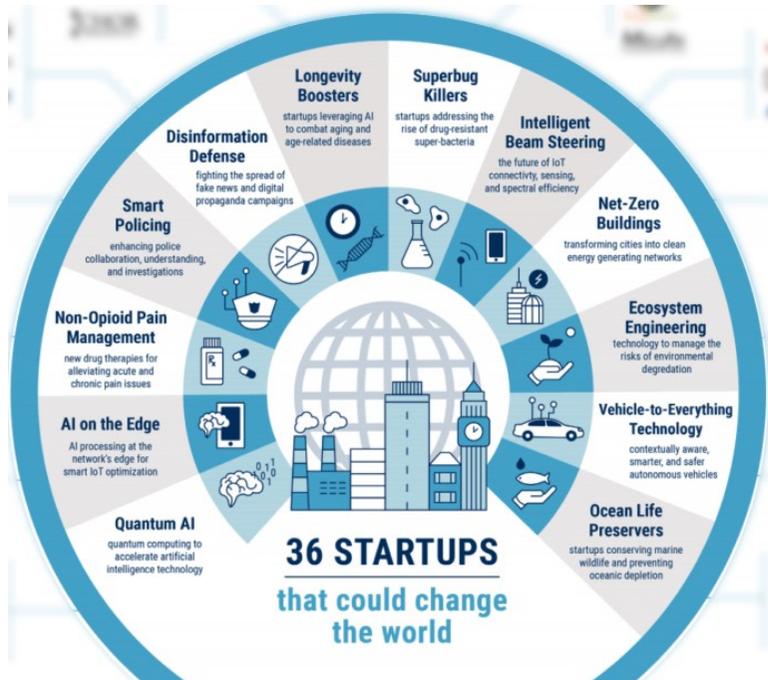
Porqué es relevante el apoyo tecnológico en las labores de compliance?

Era de disrupción digital



70%

* The millennial disruption index. 2019



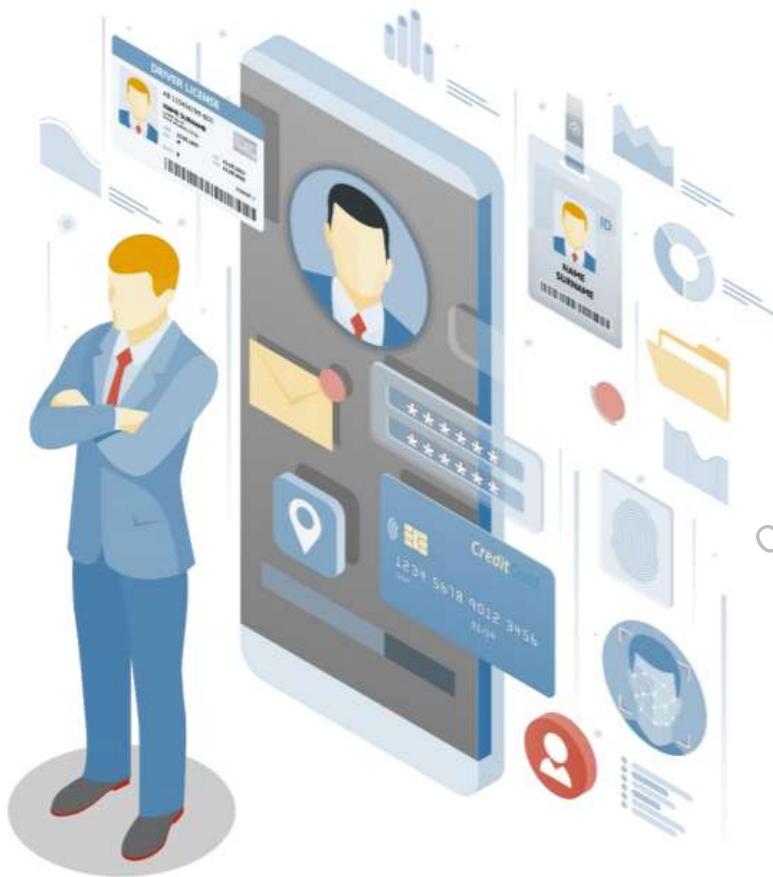
Efectos Covid-19

| Company | Industry | Bankruptcy Date | Assets (\$) |
|-------------------------|--------------------------------|-----------------|-------------|
| Hertz | Travel, Lodging and Leisure | May 22 | 25.8B |
| Latam Airlines | Travel, Lodging and Leisure | May 25 | 21.1B |
| Frontier Communications | Telecoms, Media and Technology | April 14 | 17.4B |
| Chesapeake Energy | Energy | June 28 | 16.2B |
| Ascena Retail | Retail and Restaurants | July 23 | 13.7B |
| Valaris | Energy | August 19 | 13.0B |
| J.C. Penney | Retail and Restaurants | May 15 | 8.6B |
| Whiting Petroleum | Energy | April 1 | 7.6B |
| Avianca Holdings | Travel, Lodging and Leisure | May 10 | 7.3B |

<https://www.bloomberg.com/graphics/2020-us-bankruptcies-coronavirus/>

Porqué es relevante el apoyo tecnológico en las labores de compliance?

Realidades de negocio



- Preferencia por parte de clientes de herramientas tecnológicas para interacción con la entidad.
- Dificultad para realizar relacionamiento comercial (vinculación, mantenimiento, etc.) de manera presencial.
- Necesidad de optimizar costos y hacer más eficientes las operaciones
- Cumplimiento de requisitos regulatorios (p.e ALA/CFT, protección de datos personales, etc.)

Reducir la fricción con clientes

Porqué es relevante el apoyo tecnológico en las labores de compliance?



USD 4
trillones

Transacciones digitales proyectadas para el 2020¹

4300%

Incremento en spam relacionado con Covid desde Febrero²

222M

Denuncias de robo de identidad en la Federal Trade Commission³

Los canales digitales procesan la mayor proporción de transacciones

Transacciones comerciales han cambiado de forma importante

Se mantienen los procesos de gestión de riesgos

[1] <https://www.statista.com/outlook/296/100/digital-payments/worldwide>

[2] <https://www.ibm.com/thought-leadership/institute-business-value/covid-19-action-guide>

[3] <https://public.tableau.com/profile/federal.trade.commission#!/vizhome/FraudReports/SubcategoriesOverTime>

Porqué es relevante el apoyo tecnológico en las labores de compliance?

Adicionalmente

Capacidad de analistas

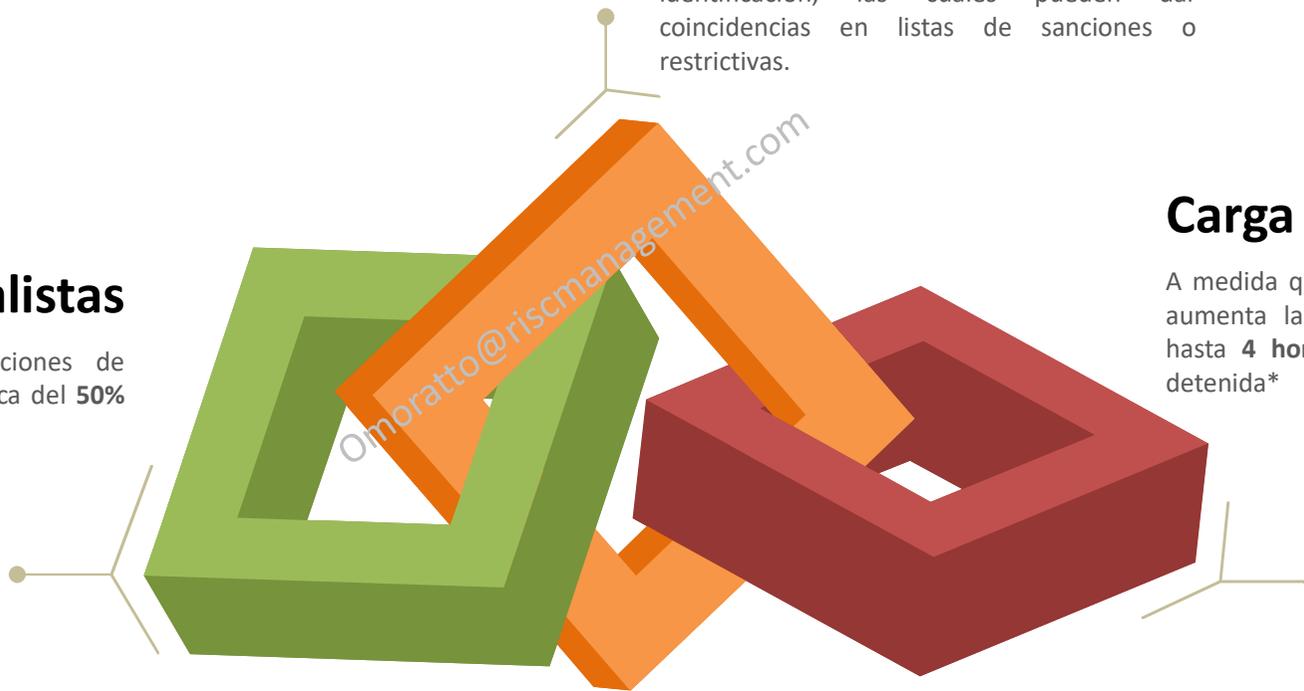
Diversas labores distraen las acciones de analistas, pudiendo llegar a ser cerca del **50% de la productividad** semanal

Facilidad de ocultamiento

En canales digitales, un actor "comprometido" posiblemente no utilizará su nombre real e identificación, las cuales pueden dar coincidencias en listas de sanciones o restrictivas.

Carga operativa

A medida que aumenta el volume de alertas, aumenta la carga operativa – puede llevar hasta **4 horas** analizar una alerta de forma detenida*



Cómo la tecnología apoya los procesos de cumplimiento?

Ejemplo: onboarding de clientes (esquemático)



Validación automática

Anverso

8.5 cm Fondo de seguridad con líneas finas, antifatigante con tintas metálicas

5.5 cm

Información preimpresa

Datos biográficos

Firma del ciudadano

Fotografía a color con una Resolución de imágenes de 640 dpi

Material Tesis (hoja sintética)

Laminación + Políester/poliestireno con copolímero + Holograma tridimensional en el plástico anverso

Composición Tres láminas sintéticas

Datos biográficos

Reverso

Validación dactilar y huella en el sistema AFIS de identificación

Microtexto

Código de barras bidimensional que contiene un algoritmo de seguridad. La información biográfica del ciudadano más la información biométrica de la huella dactilar

Hologramas en el plano de laminación

Reversa estado Registraduría

Información preimpresa

Información de producción del documento

16 / Nuestra Huella Noviembre 2012

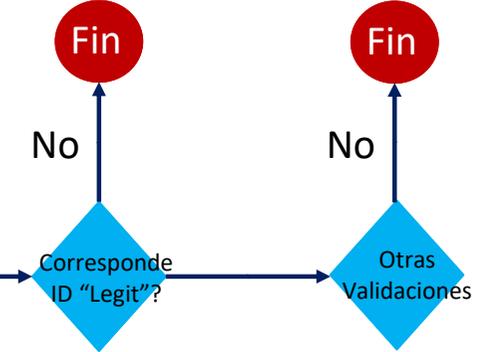
Recolección de información del dispositivo

IP

IMEI

MAC ADDRESS

Windows, Android, Apple



Cómo la tecnología apoya los procesos de cumplimiento?

Ejemplo: onboarding de clientes (esquemático)



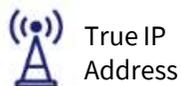
Cómo la tecnología apoya los procesos de cumplimiento?

Otro ejemplo ... monitoreo (GeoFencing)



83%

De las transacciones originadas en Korea del Norte utilizan un proxy o algún otro mecanismo de enmascaramiento de red



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

Enforcement Release: July 8, 2020

OFAC Settles with Amazon.com, Inc. with Respect to Potential Civil Liability for Apparent Violations of Multiple Sanctions Programs

Amazon.com, Inc. ("Amazon"), a Seattle, Washington-based company that provides retail, e-commerce, and digital services to millions of customers worldwide, has agreed to pay \$134,523 to settle its potential civil liability for apparent violations of multiple OFAC sanctions programs. As a result of deficiencies related to Amazon's sanctions screening processes, Amazon provided goods and services to persons sanctioned by OFAC; to persons located in the sanctioned region or countries of Crimea, Iran, and Syria; and to individuals located in or employed by the foreign missions of countries sanctioned by OFAC. Amazon also failed to timely report several hundred transactions conducted pursuant to a general license issued by OFAC that included a mandatory reporting requirement, thereby nullifying that authorization with respect to those transactions. The settlement amount reflects OFAC's determination that Amazon's apparent violations were non-egregious and voluntarily self-disclosed, and further reflects the significant remedial measures implemented by Amazon upon discovery of the apparent violations.

TRADICIONAL

01

Primordialmente Manual

02

Retroactiva

03

Basado primordialmente en identidad física

04

Puede generar fricción con el cliente

Automatización ML, AI

05

Tiempo real

06

Identidad física y digital

07

Mejorar experiencia del cliente

08

NUEVOS RETOS



Ciberseguridad

Creación de identidades falsas (sintéticas)
Explotar (hackear) identidades legítimas (fraude, LA/FT), robo de PINes, Sim card swap, etc



Datos personales

Filtración de datos personales sensibles.
Explotar filtración para acceder a cuentas



Acceso a info

Sistemas complejos puede tener dificultad en acceder a data recolectada.
Altos volúmenes de información que pueden no ser explotados apropiadamente.
Stoppers en el proceso de DD cuando se solicita información complementaria

Fuente. FATF. Digital Identity. March 2020. p. 35



PERSONAS JURÍDICAS?

Fortalecer DD



Mejorar seguridad, privacidad, conveniencia y eficiencia en la identificación de individuos.
Minimizar medidas de control manuales

Experiencia



Mejorar experiencia del cliente
Reducción de costos de onboarding
Reducción fricción con el cliente

Monitoreo



Apoyo en identificación de transacciones inusuales y sospechosas.
Captura de información adicional (IP, etc)

Inclusión



Aumentar la inclusion financiera

Algunas preguntas

- Su negocio actualmente realiza monitoreo del comportamiento online de sus clientes y atributos (p.e. ubicación, actividad de logeo, información de dispositivos, etc.)?
- Su negocio, de manera rutinaria, explota atributos digitales en el proceso de análisis de alertas, operaciones inusuales y los incluye dentro de la información proporcionada la UIF en los ROS? En casos de fraude?
- Se compara la información de KYC proporcionada por el cliente con su comportamiento digital?
- Bloquea interacciones desde ciertas ubicaciones?
- Está en capacidad de identificar si múltiples identidades digitales, dispersas geográficamente, acceden a la misma cuenta?
- Quienes acceden a las cuentas de los PEPs?
- Los patrones atípicos de identidad digital son contrastados contra una muestra mayor de clientes o transacciones?

El compliance digital



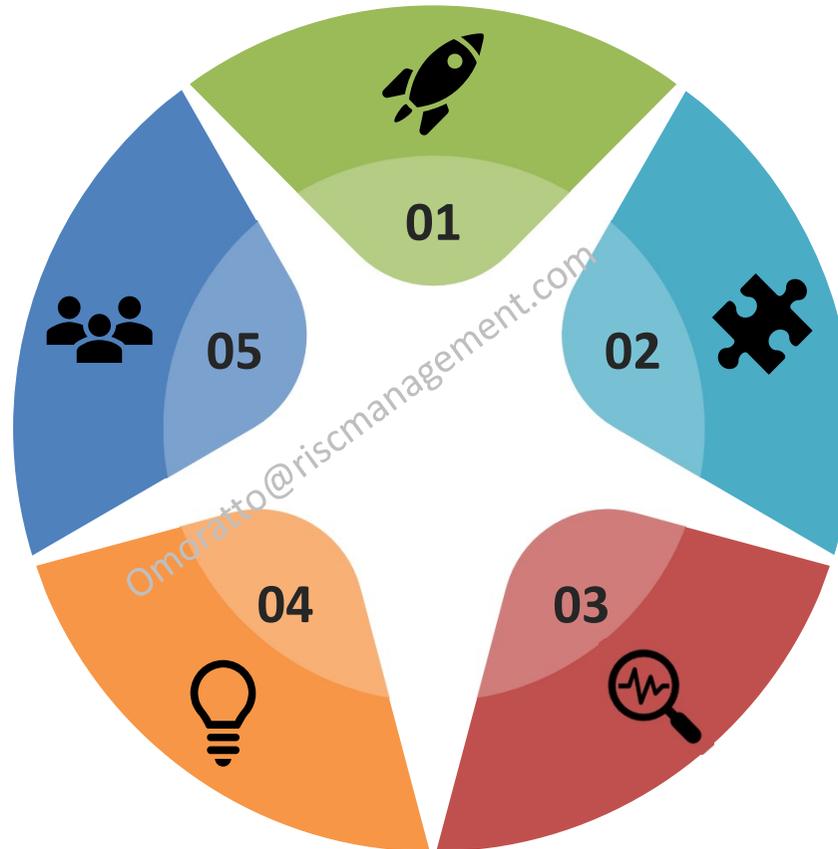
Upgrading

Puede llevar a un siguiente nivel los sistemas de monitoreo, no solo ALA/CFT sino también antifraude



Optimización

Apoya a procesos de optimización de procesos, mejoras de productividad y reducción de costos



Proactividad



Permite reaccionar proactivamente ante amenazas

Información



Utiliza un espectro de información de mayor alcance que el compliance tradicional

Solución?



Se debe tener en cuenta que no soluciona todos los desafíos, en particular, de DD

Device Intelligence Scorecard

A collage of logos for various security and identity management companies. The logos are arranged in several rows. The top row includes e1, BeyondTrust, Callsign, Duo, iovation, and Entersekt. The second row features VerifyMe, BIOCATCH, Cardinal Commerce, ENCAP, evernym, EZMCOM, Folio, and IDOLOGY. The third row contains Centrifify, CounterTack, EASYSOLUTIONS, Entrust Datacard, FORGEROCK, fusionpipe, and InAuth. The fourth row shows Kount, sift science, MAXMIND, MetaStudio, Trustev, SOCURE, neustar, and ThreatMetrix. The fifth row includes onelogin, OneSpan, privaKey, RCDevs, RISK IDENT, RSA, and SECUREAUTH. A watermark 'omoratto@ricsmanagement.com' is visible diagonally across the collage.

Transaction Behavior Scorecard

A collage of logos for various security and identity management companies. The logos are arranged in several rows. The top row includes ca technologies, fst, AuthenWare, BehavioSec, CROSSMATCH, id:analytics, EASYSOLUTIONS, and TeleSign. The second row features ioMetric, EARLY WARNING, miniOrange, NuData Security, Solus, and ThisData. The third row contains FORTER, CREDENCE ID, KeyTrac, sift science, Trustev, and unboxify. The fourth row shows ID R&D, Plurilock, NOPASSWORD, SECUREAUTH, BIOCATCH, aimbrain, Trusteer, and typingdna. The fifth row includes NetGuardians, SECURETOUCH, FICO, BALABIT, and ThreatMetrix. A watermark 'omoratto@ricsmanagement.com' is visible diagonally across the collage.

Gracias