Ciberseguridad

SEC - Guía para el reporte de información

Juan Marciales
Manager
Cyber Security Services

CONTENIDO

Ciberseguridad panorama actual

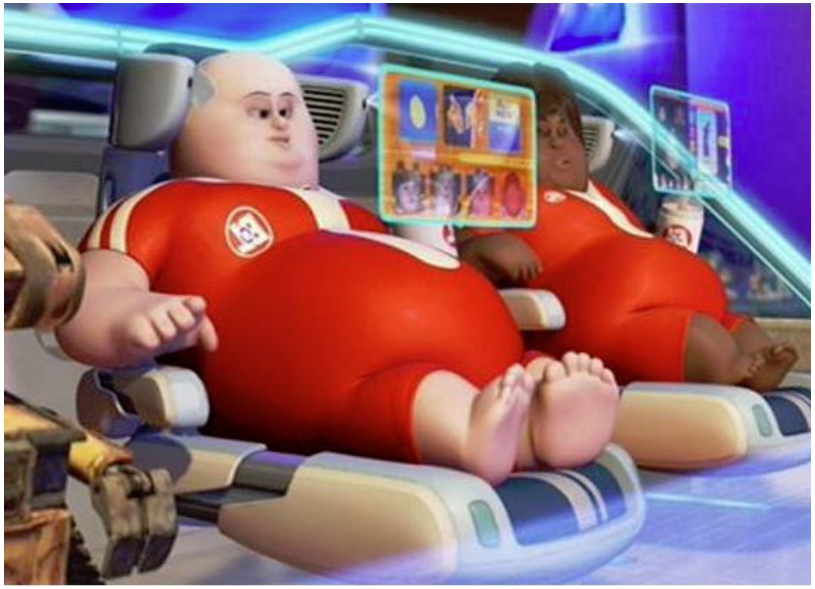
La guía de divulgación

El enfoque de la auditoría

Medidas adoptadas por la SEC

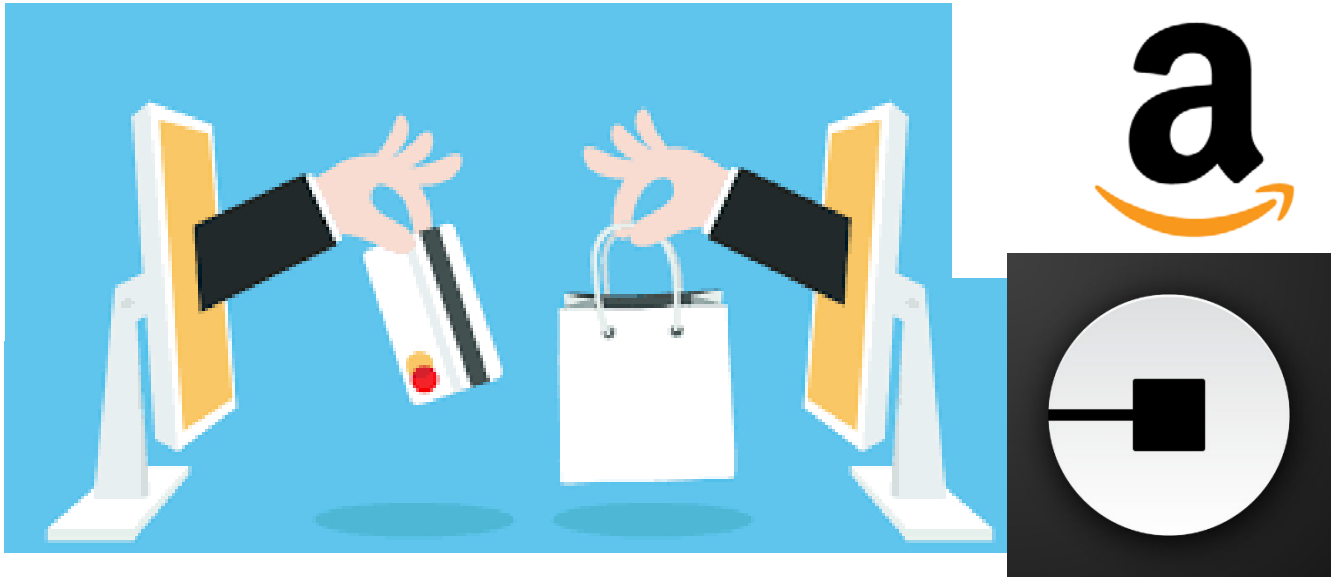
Ciberseguridad
Panorama actual

"Wall-E" una película futurista.....

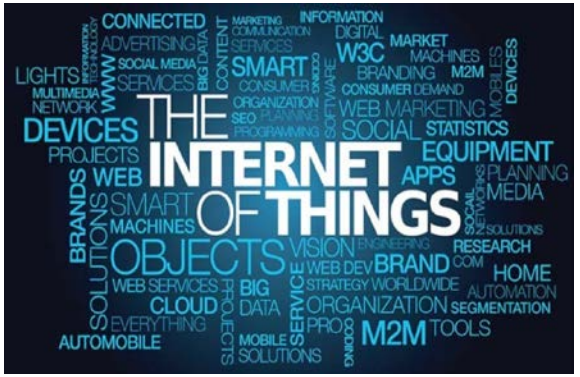


Un cambio fundamental

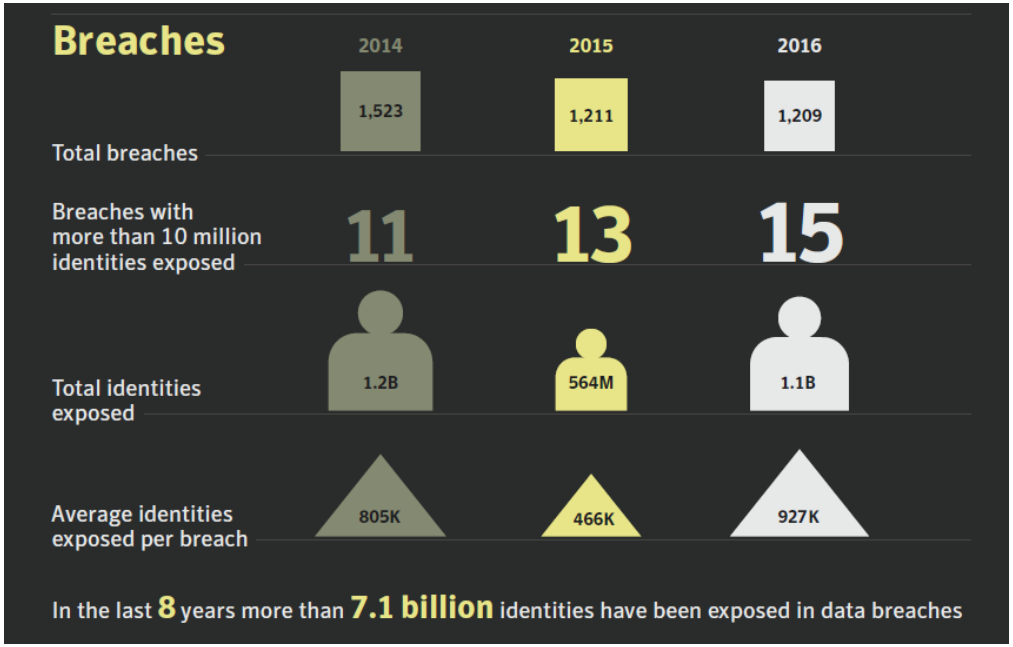
¡La tecnología ya no consiste simplemente en digitalizar y trasladar información. Las Tecnologías Digitales de Negocio están transformando productos y modelos operativos!



La transformación tecnológica impulsa el futuro…



Las estadísiticas no mienten…

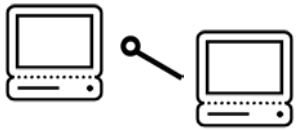


Internet Security Threat Report, April 2017, Symantec

Todas las tendencias principales indican un aumento en el número de ataques

Evolución de la seguridad a través de los años…

Pre-1990	1990-2000	2000-2010	2010-Present	2020
Confidentiality, Integrity and Availability	Non-repudiation, Anti-virus software, Authentication	OWASP, ISO/IEC 27001, Integrated SOC, SIEM, Network/Perimeter Security	Mobile security, Cloud security, IPS, Analytics, IDAM	Threat Intelligence, Self-healing systems, Proactive Monitoring & Response



¿Por qué la seguridad está siempre un paso atrás?

Las amenazas...

Los objetivos...

FINANCIAL INFORMATION

INTELLECTUAL PROPERTY

STRATEGIC ADVANTAGE

INDUSTRIAL CONTROL SYSTEMS

WHAT IS BEING

TARGETED?

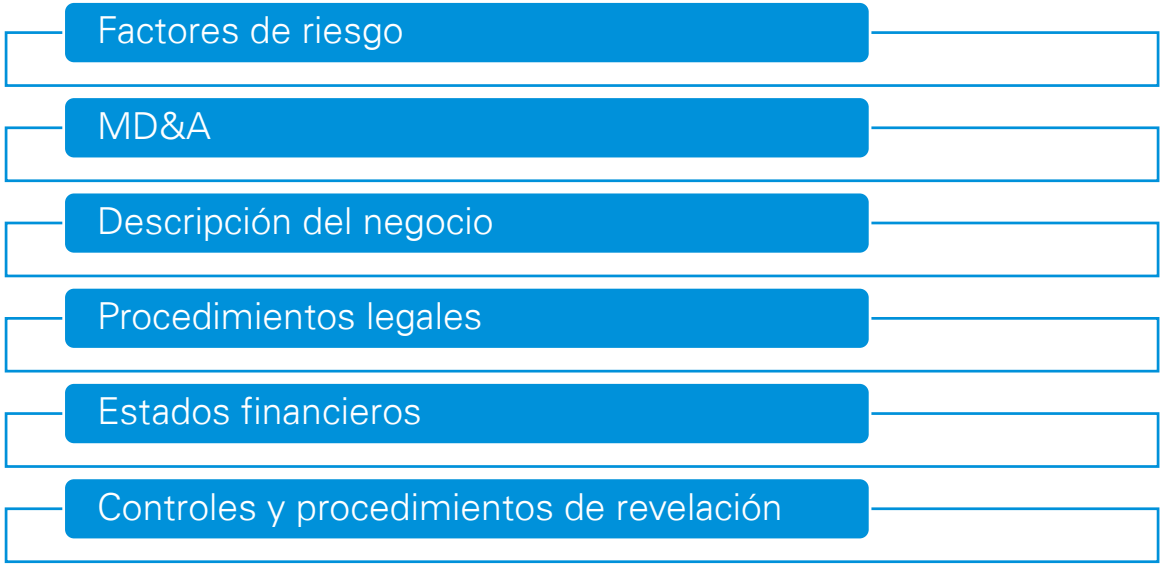
La Guía…

La Guía 2011

CF Disclosure Guidance: Topic No. 2 – Cybersecurity (October 13, 2011)

- **Regulación de la SEC:** Revelar información oportuna, completa y precisa de riesgos y eventos que un inversionista razonable consideraría importante para tomar una decisión de inversión.

- **Obligaciones de revelación de riesgos e incidentes de Ciberseguridad**:



La Guía 2018

Commission Statement and Guidance on Public Company Cybersecurity Disclosures (Rel. No. 33-10459) (February 21, 2018)

Expedida directamente por la Comisión

Refuerzo del enfoque de 2011, con claro sentido de urgencia

Mayor orientación acerca de las revelaciones, mismo marco de reporte.

Nuevo enfoque en políticas y procedimientos

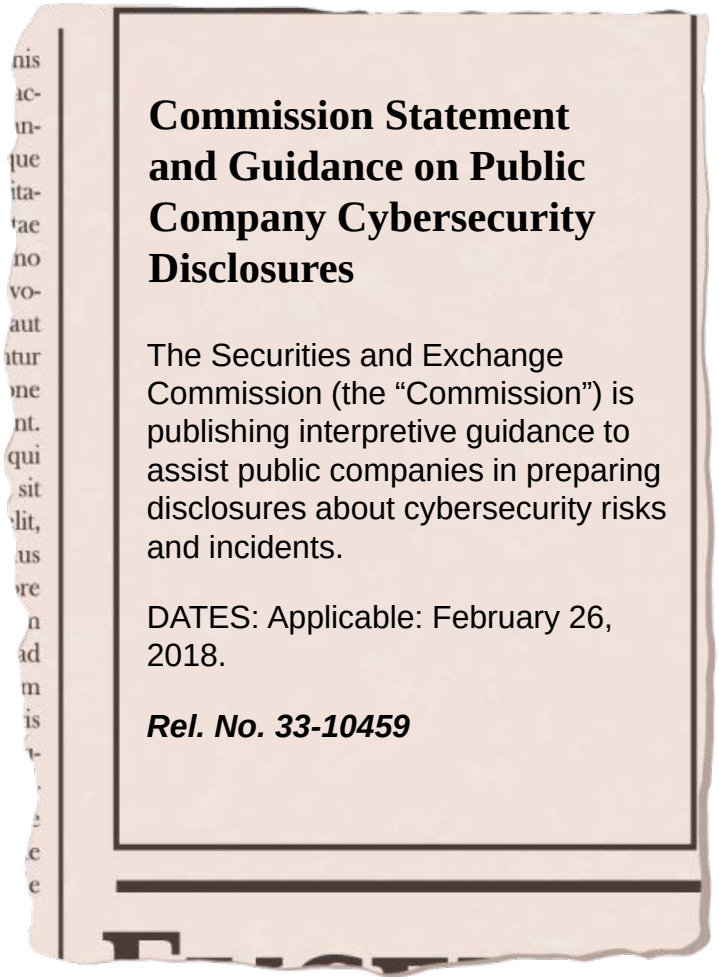
Guía de divulgación de Ciberseguridad 2018

A. Reglas para la revelación de asuntos de ciberseguridad

- Obligaciones de divulgación
- Factores de riesgo
- Materialidad en productos y servicios
- Procedimientos legales
- Supervisión de riesgos por parte de la Junta Directiva

B. Políticas y procedimientos

- Controles y procedimientos de divulgación
- Uso de información privilegiada
- Regulación *Fair Disclosure* y divulgación selectiva



Commission Statement and Guidance on Public Company Cybersecurity Disclosures

The Securities and Exchange Commission (the "Commission") is publishing interpretive guidance to assist public companies in preparing disclosures about cybersecurity risks and incidents.

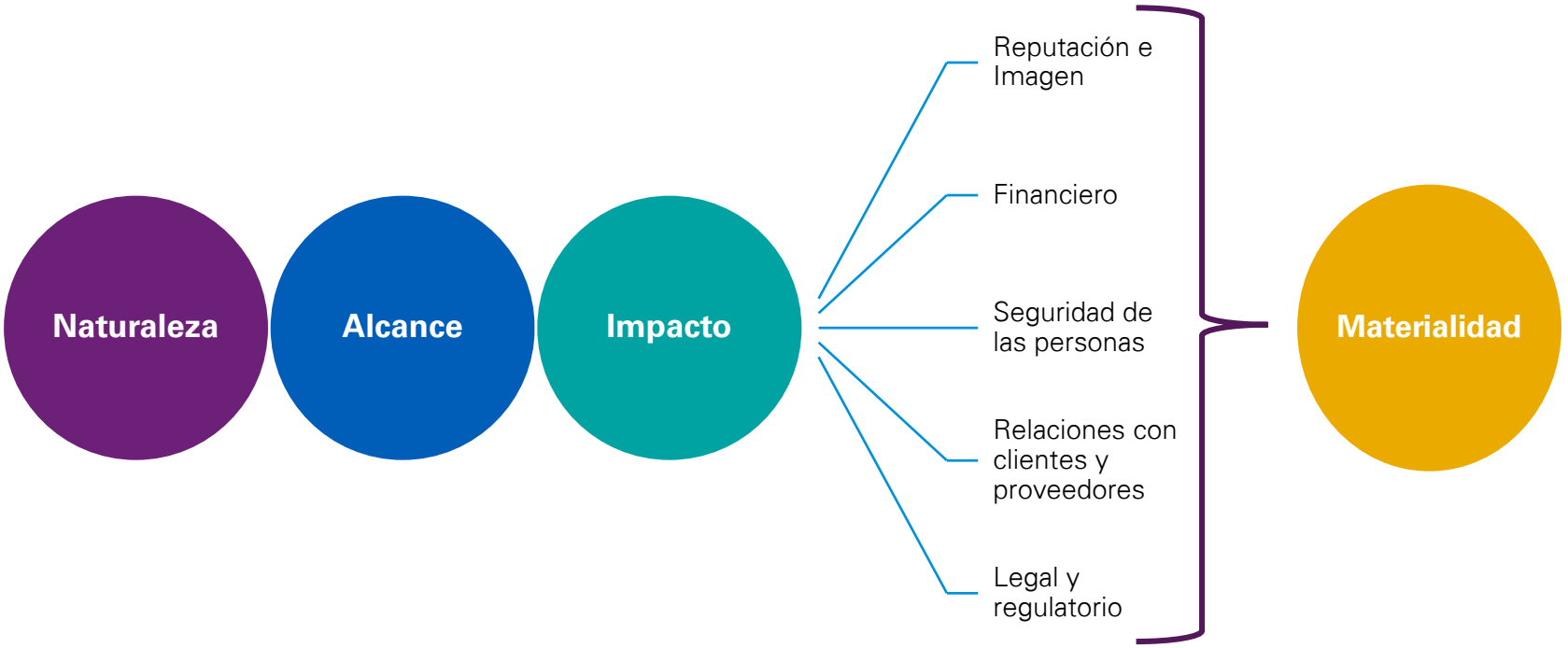
DATES: Applicable: February 26, 2018.

Rel. No. 33-10459

A. Reglas para la revelación de asuntos de ciberseguridad

1. Obligaciones de divulgación (Materialidad)

- El estándar para determinar la divulgación de mantiene: **Materialidad**
- Criterios para determinar la materialidad:



A. Reglas para la revelación de asuntos de ciberseguridad

1. Obligaciones de divulgación (Materialidad)

La información omitida puede ser importante

La materialidad es un "juicio propio"

La información técnica y comprometedora no debe ser divulgada

La SEC podría requerir un análisis cuando una violación "no fue material".

A. Reglas para la revelación de asuntos de ciberseguridad

1. Obligaciones de divulgación (Oportunidad)

La investigación en curso no es razón suficiente para retrasar la divulgación.

Revelación de los incidentes y riesgos previa a la oferta de valores

Uso de reportes actuales, deber de actualizar y corregir

A. Reglas para la revelación de asuntos de ciberseguridad

2. Factores de riesgo (Reg. S-K, Punto 503(c) - Formulario 20-F, Punto 3.D)

- **Incidentes anteriores** de Ciberseguridad (severidad y frecuencia)
- La probabilidad e impacto de futuros incidentes
- Medidas preventivas, incluyendo limitantes
- Situaciones del negocio que aumenten el riesgo (industria, terceros, proveedores)
- Costos de medidas de protección, incluyendo seguros
- Potencial daño a la reputación
- Cumplimiento regulatorio y costos asociados
- Costos legales (litigios, investigaciones, compensaciones)

A. Reglas para la revelación de asuntos de ciberseguridad

3. MD&A (Reg. S-K, Punto 303 - Formulario 20-F, Punto 5)

La Comisión espera que las empresas consideren el impacto de los incidentes en cada uno de sus segmentos declarables:

A. Reglas para la revelación de asuntos de ciberseguridad

4. Descripción del negocio y procedimientos legales
(Reg. S-K, puntos 101 y 103 - Formulario 20-F, punto 4.B)

Evaluar el impacto de riesgos e incidentes de Ciberseguridad en:

- Productos
- Servicios
- Relaciones con clientes y proveedores
- Condiciones de competitividad

Divulgar información de procesos legales

- Proceso legales, incluyendo demandas e investigaciones de ciberseguridad

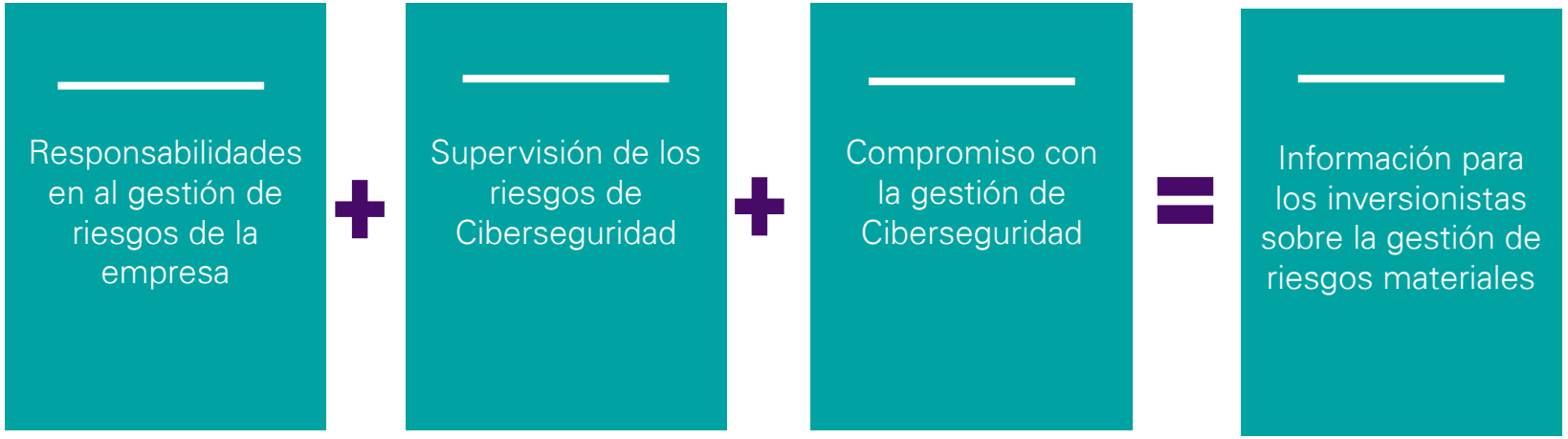
A. Reglas para la revelación de asuntos de ciberseguridad

5. Información a revelar en los estados financieros (Reg. S-K)

La revelación de estados financieros en informes anuales y trimestrales sobre ciberseguridad:

A. Reglas para la revelación de asuntos de ciberseguridad

6. Supervisión de riesgos por parte de la Junta Directiva



B. Políticas y procedimientos

1. Controles y procedimientos de divulgación

Gestión de Ciberseguridad	Políticas y procedimientos de Ciberseguridad y evaluar su cumplimiento.
Reporte y comunicación	Evaluar si disponen de controles y procedimientos de divulgación
Ejemplos	– Seguridad de red – Gobierno de seguridad – Cumplimiento – Gestión de riesgos – Detección y atención incidentes – Continuidad del negocio - Hardening - Desarrollo seguro - Seguridad SAP - Seguridad AD - Seguridad en la nube, SaaS

B. Políticas y procedimientos

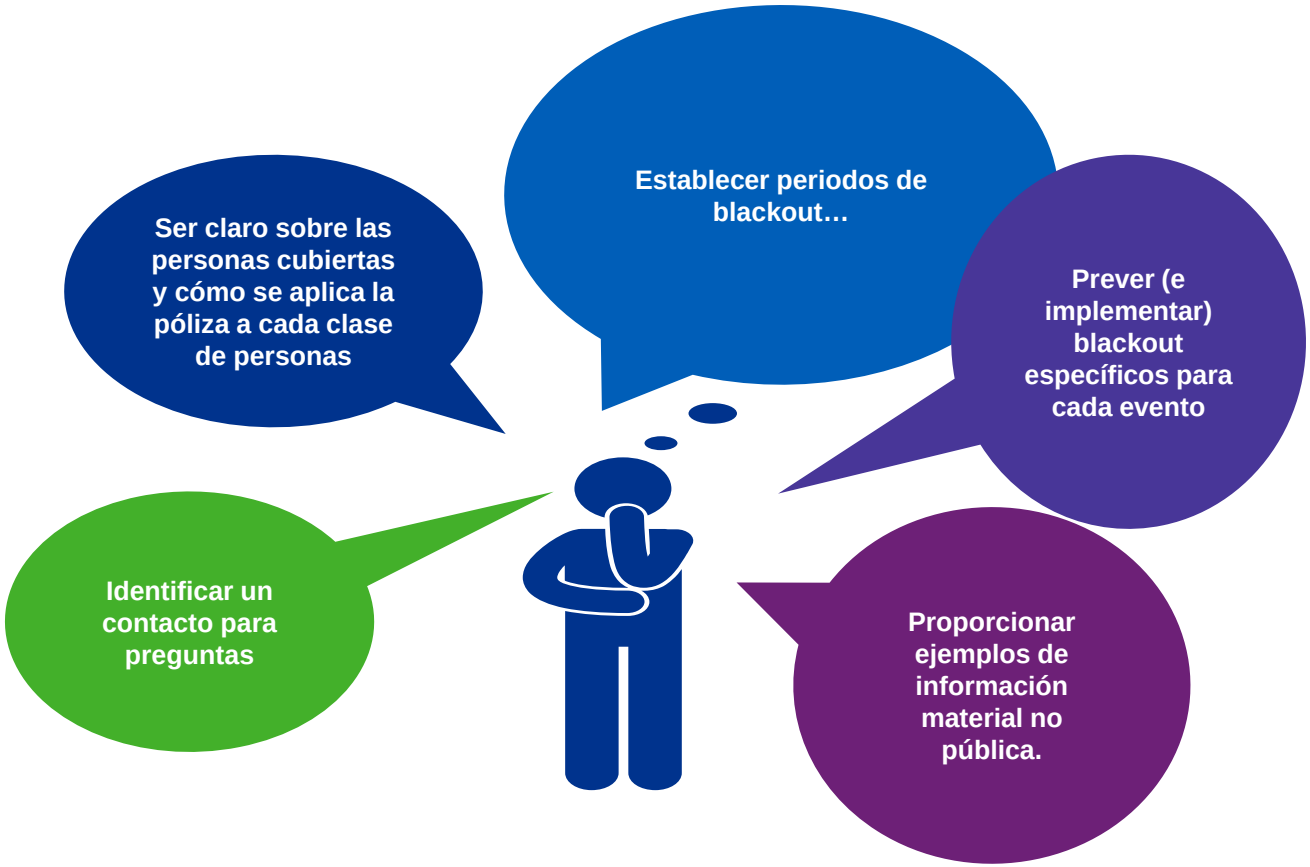
2. Uso de información privilegiada y revelación justa

- Prohibido realizar transacciones sobre la base de información material no pública, incluyendo la de riesgos e incidentes de ciberseguridad

- Se **anima** a las empresas a incluir el tema en sus códigos de ética y la definición de políticas de uso de información privilegiada

B. Políticas y procedimientos

2. Uso de información privilegiada y revelación justa



B. Políticas y procedimientos

2. Uso de información privilegiada y revelación justa

Puntos clave a considerar:

Establecer voceros autorizados

Sea claro acerca de la aplicación y el protocolo en varios entornos

- Comunicados de prensa
- Llamadas
- Comunicaciones del día a día
- Reuniones individuales con los analistas
- Presentaciones
- Medios de comunicación social

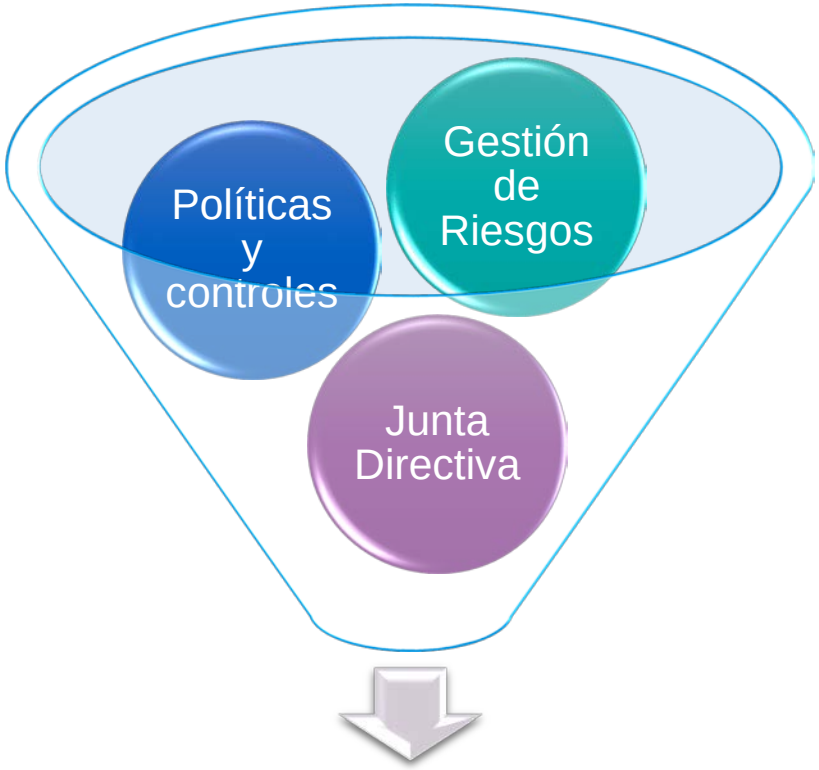
Articular con el rol del departamento jurídico

Proporcionar ejemplos de información material no pública

Proporcionar recordatorios periódicos y capacitación a la gerencia

El enfoque de la Auditoría

El enfoque de la auditoría



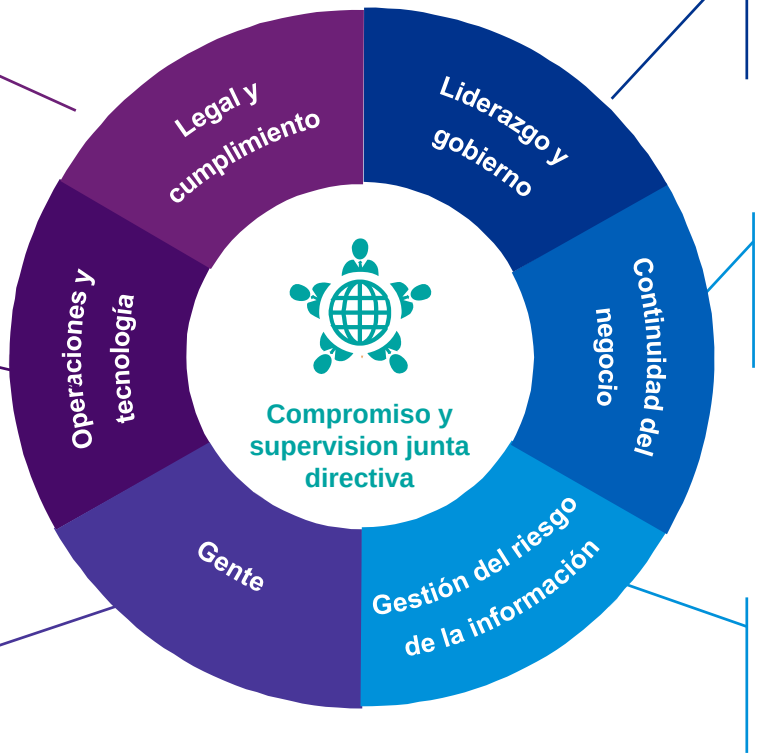
Reportes de riesgos e incidentes de Ciberseguridad

Modelo de madurez de Ciberseguridad

¿Se trabaja en estrecha colaboración con las autoridades y se comparte información en todo el sector?

¿se mitigan adecuadamente las amenazas internas?

¿Qué nivel de riesgo de ciberseguridad se considera aceptable?

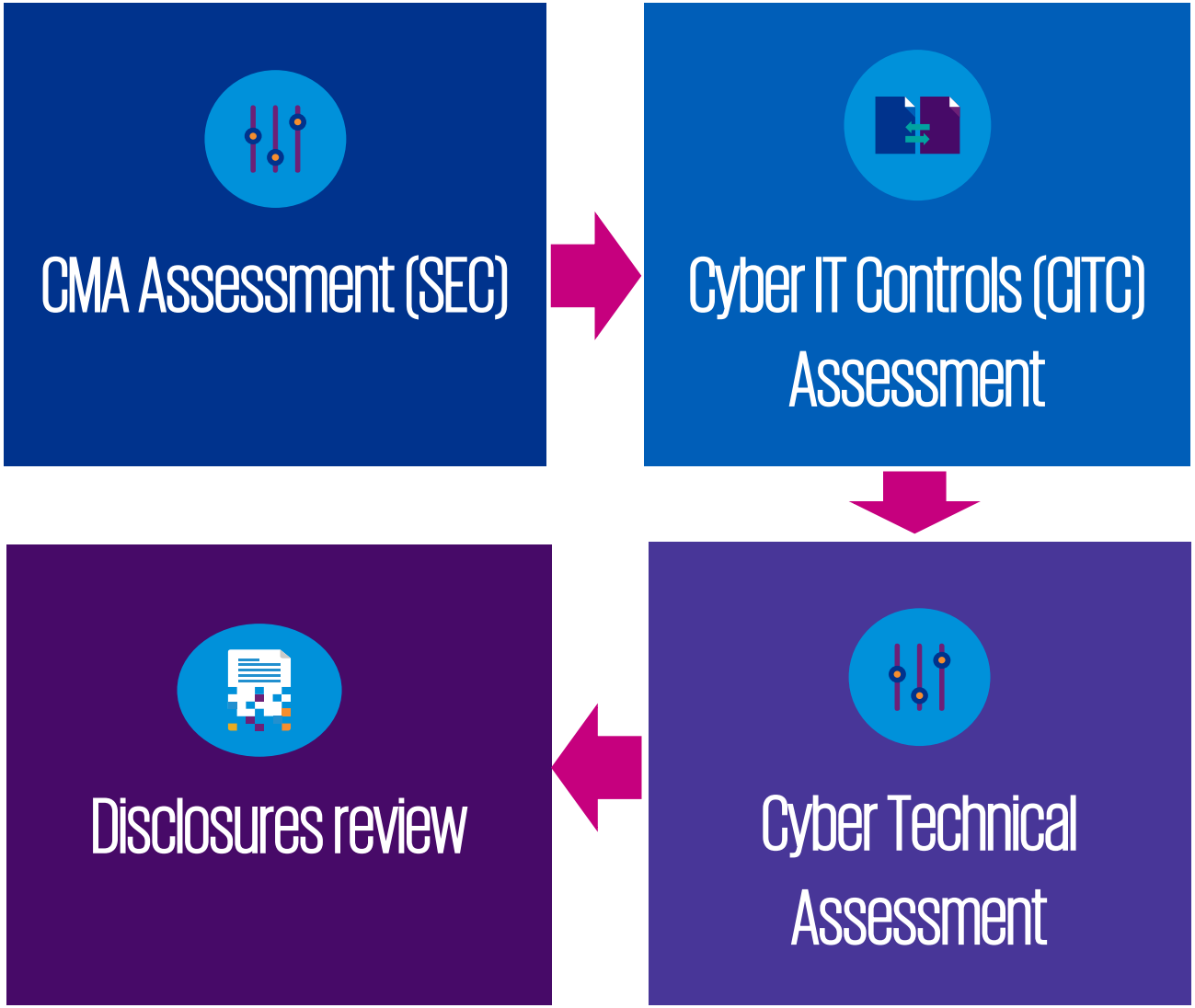


¿Quién es el responsable de Ciberseguridad?

¿se mitigan adecuadamente las amenazas internas?

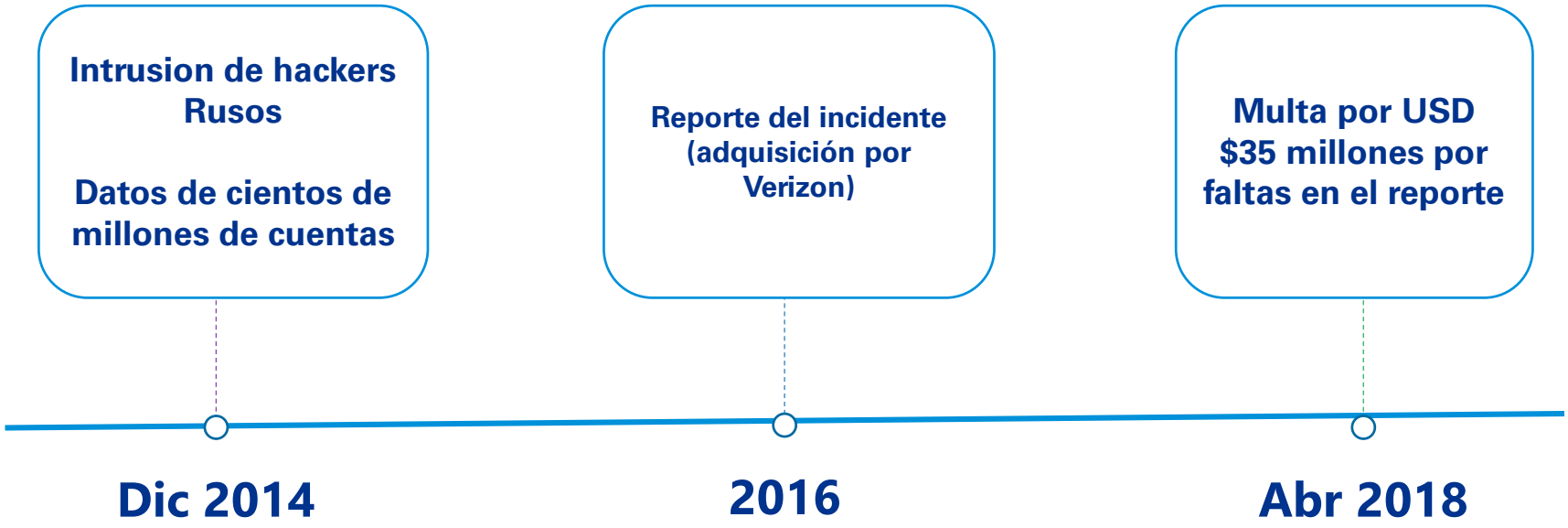
¿Cuáles son los activos clave que requieren protección?

Enfoque de evaluación Ciberseguridad KPMG

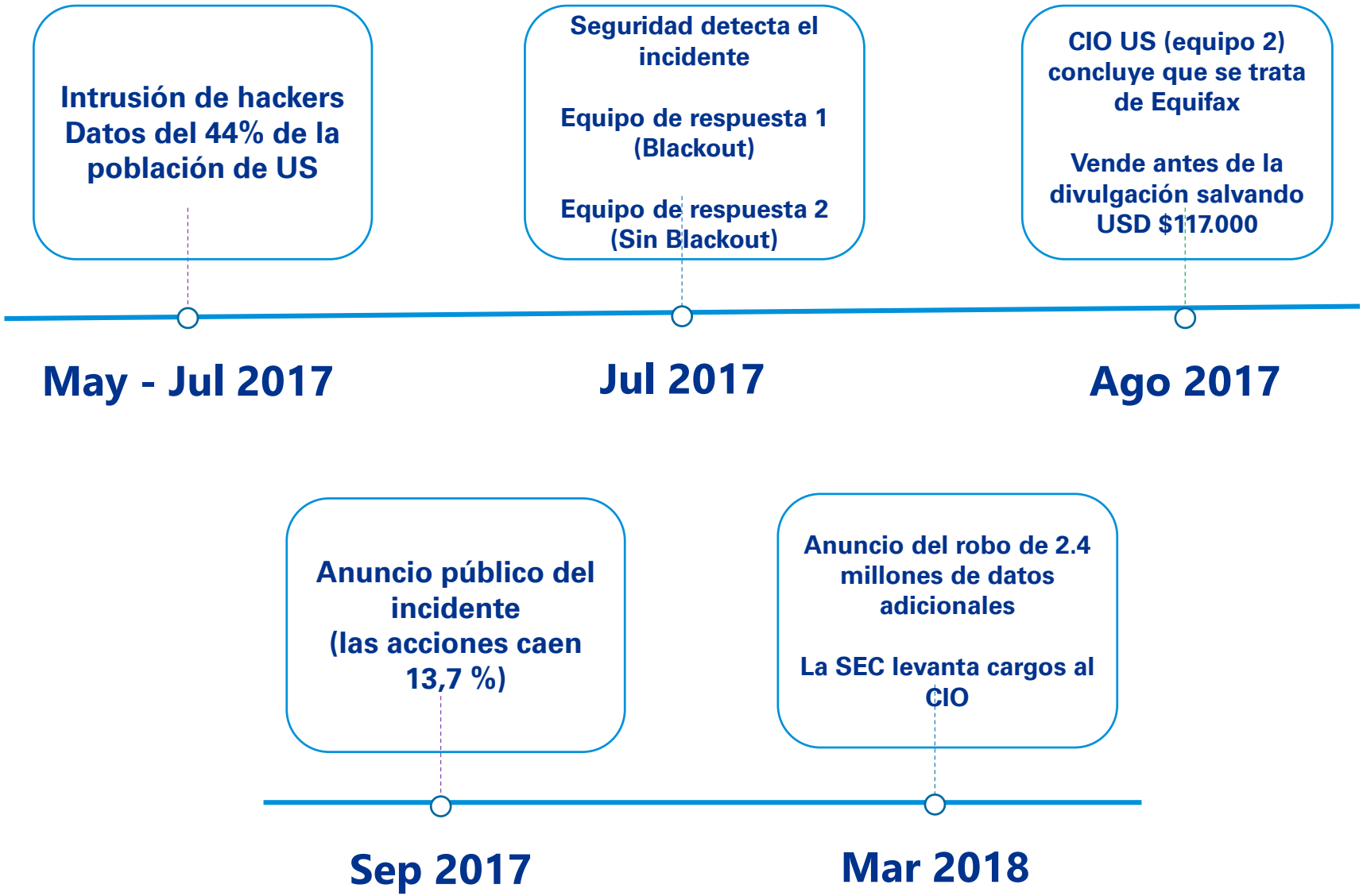


Medidas adoptadas por la SEC

ALTABA (YAHOO)



EQUIFAX



VOYA FINANCIAL ADVISOR

The S.E.C. Dusts Off a Never-Used Cyber Enforcement Tool

The S.E.C. issued a cease-and-desist order against Voya Financial last month for allowing hackers to access social security numbers, account balances and even details of client investment accounts.
Brendan Mcdermid/Reuters

JUAN MARCIALES

Manager

Cyber Security Services

jmarciales@kpmg.com

kpmg.com/socialmedia