Boletín Técnico

imef
ejecutivos de finanzas

BOLETÍN TÉCNICO 2025-04

La Ciberseguridad en la agenda del CFO

Diciembre – 2025

Índice

Introducción

En la era de la transformación digital, la ciberseguridad ha dejado de ser un tema exclusivamente técnico para convertirse en una prioridad estratégica para la alta dirección. Las organizaciones se enfrentan, cada vez más, a riesgos cibernéticos que pueden afectar su posición financiera, con impacto en su liquidez, la reputación, continuidad operativa y su valor, representando un riesgo financiero estratégico que debe ser abordado.

Este ensayo explora por qué la ciberseguridad debe figurar de forma explícita en la agenda del CFO, las áreas clave de intervención, marcos de gobernanza, métricas financieras y casos prácticos que ilustran el impacto económico de las amenazas cibernéticas.

1. La ciberseguridad como riesgo financiero estratégico

A) Impacto en el valor de la empresa.

Las brechas de seguridad pueden generar pérdidas directas (robo de datos, fraude, interrupción de operaciones) y costos indirectos (multas regulatorias, costos de remediación, endurecimiento de controles). Estos efectos se traducen en variaciones del costo de capital, depreciación de la marca y menor confianza de inversores.

B) Presupuesto y asignación de recursos

La ciberseguridad debe integrarse en la planificación presupuestaria y en los escenarios de estrés financiero. El CFO, actuando en conjunto con la gerencia de TI y la Administración, está en posición de priorizar inversiones en seguridad en función de su impacto en la liquidez y en el retorno esperado.

C) Indicadores y métricas financieras:

Los riesgos cibernéticos deben observarse a través de métricas integradas en la gestión de riesgos y la valoración de activos intangibles, afectando indicadores como el EP (Economic Profit), EVA, y métricas de aseguramiento (cyber insurance).

2. Gobernanza y responsabilidad

A) Propiedad del riesgo cibernético:

La responsabilidad debe cruzar distintas áreas: TI, seguridad, auditoría interna y finanzas, así como el máximo órgano de la administración. El CFO es un facilitador para articular el perfil de riesgo aceptable y la tolerancia a la pérdida (risk appetite) desde la perspectiva financiera.

B) Programa de ciberseguridad como programa de control:

Integrar controles de ciberseguridad en el marco de control interno y cumplimiento (COSO, ISO 27001) para asegurar la trazabilidad, mitigación y reporte.

C) Informes para la junta directiva y el consejo

Informes periódicos sobre exposición, pérdidas esperadas, probabilidad y plan de mitigación deben ser parte de la agenda de gobierno corporativo.

3. Marco de gestión de riesgos y marcos de referencia

A) Marcos de referencia clave:

- NIST Cybersecurity Framework (CSF): Marco del NIST para gestionar riesgos de ciberseguridad. Se basa en cinco funciones: Identificar, Proteger, Detectar, Responder y Recuperar.
- ISO/IEC 27001 y 27002:
  - ***27001****:* norma para implementar un Sistema de Gestión de Seguridad de la Información (SGSI).
  - ***27002:*** guía de controles y buenas prácticas para aplicar la seguridad definida en 27001.
- CIS Controls: conjunto de controles prácticos del Center for Internet Security para reducir riesgos. Incluye acciones como inventario de activos, gestión de vulnerabilidades y monitoreo continuo.
- COSO Enterprise Risk Management (ERM) y Control Activities:
  - ***COSO ERM:*** marco para gestionar riesgos empresariales alineados con estrategia y objetivos.
  - ***Control Activities:*** políticas y procedimientos para ejecutar acciones que mitiguen riesgos (p.ej., autorizaciones, segregación de funciones).

B) Convergencia con riesgos financieros:

La gestión de ciberseguridad no debe limitarse a métricas técnicas; es fundamental traducir controles y salvaguardas en términos financieros para que los comités y áreas directivas comprendan su impacto real en la organización. Esta convergencia permite integrar el riesgo tecnológico dentro del marco de riesgos financieros, considerando flujos de caja, pérdidas esperadas y requerimientos de capital regulatorio. A continuación, se detallan los componentes clave:

i. **Incorporar métricas financieras específicas**
   a. ***Valor en Riesgo (VaR) cibernético:*** Estimar la pérdida máxima esperada en un horizonte temporal determinado con un nivel de confianza definido, aplicando metodologías similares a las usadas en riesgos de mercado y crédito.
   b. ***Impacto en EBITDA y margen operativo:*** Traducir incidentes cibernéticos en reducción de rentabilidad, considerando costos directos (remediación, sanciones) e indirectos (pérdida de clientes, reputación).
   c. ***Costo de capital adicional:*** Analizar cómo los riesgos tecnológicos incrementan requerimientos de capital regulatorio bajo marcos como Basilea III o Solvencia II, afectando la estructura financiera.

ii. **Relación con flujos de caja**
   a. ***Escenarios de estrés financiero por incidentes:*** Simular cómo un ataque afecta la liquidez, el cumplimiento de pagos a proveedores y el servicio de deuda, incorporando retrasos operativos y costos extraordinarios.
   b. ***Descuentos en valuación:*** Evaluar el impacto en el Valor Presente Neto (VPN) y en la valuación de la empresa ante interrupciones prolongadas o pérdida de confianza del mercado.

iii. **Integración con modelos regulatorios**
   a. ***Capital económico vs. capital regulatorio:*** Ajustar modelos de riesgo operativo para incluir ciber-riesgos, alineando métricas internas con exigencias regulatorias.
   b. ***Cumplimiento normativo:*** Considerar cómo la falta de controles puede derivar en sanciones monetarias significativas bajo marcos como SOX, GDPR, Ley Fintech y otras normativas aplicables.

iv. **Conversión de controles en términos monetarios**
   a. ***ROI de controles:*** Comparar el costo de implementación de medidas de seguridad con la reducción de pérdidas esperadas, justificando la inversión en términos financieros.
   b. ***Costo de oportunidad:*** Analizar qué se gana o se evita perder al invertir en ciberseguridad frente a otros proyectos estratégicos.

v. **Perspectiva aseguradora y exposición residual**
   a. ***Prima vs. cobertura:*** Relacionar el costo del seguro cibernético con la reducción del capital requerido y la mitigación del impacto financiero.
   b. ***Exposición residual cuantificada:*** Expresar en dólares el riesgo que permanece después de aplicar controles y seguros, para una visión completa del riesgo residual.

4. Modelo de valor y coste de la ciberseguridad

A) Coste de control vs. coste de incidente:

Invertir en controles proactivos puede reducir la probabilidad de incidentes y, por tanto, el coste esperado (expected loss). El CFO, en conjunto con el área de TI, debe realizar análisis de costo-efectividad de las medidas de seguridad.

B) Seguro cibernético:

Evaluar pólizas de ciberseguro, limitaciones, deducibles y cobertura frente a breach, ransomware e interrupciones operativas. Integrar primas y reservas en el cuadro financiero.

C) Costo de cumplimiento y multas:

Las regulaciones (GDPR, CCPA/CPRA, LGPD, etc.) pueden generar costos significativos si no se cumplen. El CFO debe anticipar estos desembolsos y su impacto en resultados.

5. Gestión de incidentes y continuidad operativa

A) Relación entre seguridad y continuidad:

Un incidente cibernético puede paralizar operaciones críticas. El CFO debe garantizar la disponibilidad de liquidez para atender incidentes y la continuidad de ingresos ante los distintos escenarios.

B) Plan de respuesta y recuperación financiera:

Establecer procedimientos para estimar pérdidas, comunicar a partes interesadas y activar reservas financieras. Simulacros regulares ayudan a mejorar la resiliencia económica.

6. Métricas y reportes para la dirección

A) Indicadores clave (KPI) recomendados:

i. **Pérdidas por incidentes (en USD):**
   Representa el costo financiero directo ocasionado por incidentes de ciberseguridad, como fraudes, brechas de datos o interrupciones operativas. Se mide en dólares para facilitar comparativos y análisis de impacto.

ii. **Probabilidad ponderada de pérdida (RCSA – Risk/Control Self-Assessment):**
   Es una estimación del riesgo residual considerando la probabilidad de ocurrencia y el impacto económico. Se obtiene mediante evaluaciones internas de riesgos y controles, útil para priorizar mitigaciones.

iii. **Monto de gasto en seguridad como porcentaje de ingresos:**
Indica cuánto invierte la organización en ciberseguridad respecto a sus ingresos totales. Permite evaluar si el gasto es proporcional al tamaño y exposición del negocio.

iv. **Tiempo medio de detección (MTTD) y tiempo medio de respuesta (MTTR):**
   a. MTTD: Tiempo promedio para identificar un incidente desde que ocurre.
   b. MTTR: Tiempo promedio para contener y resolver el incidente.

Son indicadores clave de eficiencia operativa en gestión de incidentes.

v. **Mapeo de controles críticos y su efectividad (SOX-like control effectiveness):**
Consiste en identificar los controles más relevantes para prevenir riesgos y evaluar su efectividad, similar a los estándares de auditoría SOX. Ayuda a garantizar cumplimiento y robustez del marco de control.

vi. **Cobertura de seguro cibernético y exposición residual:**
Mide el alcance de la póliza de seguro frente a incidentes cibernéticos y el riesgo que permanece sin cubrir (exposición residual). Es esencial para entender la protección financiera ante eventos graves.

B) Tablero de control (dashboard) para la junta:

Incluya una vista de alto nivel de exposición financiera, hitos de mitigación, costos de incidentes, y escenarios de impacto en liquidez y valor de empresa.

7. Casos prácticos y lecciones aprendidas

Caso A: Breach con costos de remediación elevados

Una empresa de servicios financieros sufre una brecha que implica exfiltración de datos de clientes. El incidente genera costos directos de 20 millones USD, multas regulatorias y pérdida de ingresos de 5 millones USD, además de 2 años de reputación afectada.

Lecciones: la ciberseguridad debe ser un activo de capital para la continuidad de ingresos y confianza; la reserva de liquidez para incidentes debe ser planificada.

Caso B: Ransomware y continuidad operativa

Una cadena de suministro industrial aplica un plan de resiliencia que minimiza el downtime y reduce el coste de interrupción a minutos en lugar de días.

Lecciones: la inversión en respaldo y recuperación ante desastres tiene un retorno rápido al reducir pérdidas por interrupciones.

Caso C: Cumplimiento y multas

Una empresa con operaciones transfronterizas enfrenta sanciones por incumplimiento de protección de datos.

Lecciones: el control financiero debe incluir revisión de cumplimiento como parte de la gobernanza de riesgos, con costos anticipados de cumplimiento en el presupuesto.

8. Recomendaciones para la integración de la ciberseguridad en la agenda del CFO

1. Incorporar la ciberseguridad en la planificación presupuestaria anual y en escenarios de stress-test**: considerar pérdidas esperadas y requerimientos de liquidez ante incidentes.

2. Asignar un patrocinador dentro de la alta dirección**: un miembro del equipo financiero debe liderar la agenda de ciberseguridad, coordinando con CISO, auditoría interna y operaciones.

3. Desarrollar un lenguaje común entre finanzas y seguridad**: traducir riesgos técnicos a impactos financieros y viceversa.

4. Fortalecer el programa de seguros cibernéticos**: evaluar cobertura, primas y reservas, alineando con la exposición real.

5. Establecer un marco de reporte claro y periódico para la junta**: reportes periódicos con KPI, respuestas a incidentes y planes de mitigación.

6. Desarrollar listas de verificación rápida para ayudar a disminuir el riesgo, por ejemplo: una para la amenaza del Ransomware.

- Copias de seguridad actualizadas y verificadas: garantiza recuperación.
- Sistemas y software con parches aplicados: reduce vulnerabilidades.
- MFA (autentificación multifactorial) activado en accesos críticos: protege accesos críticos.
- Extensiones y macros de Office deshabilitadas por defecto: evita vectores comunes.
- EDR (Endpoint Detection and Response) /antivirus funcionando y actualizado: detección y respuesta.
- Segmentación de red y mínimo privilegio: limita propagación.
- Plan de respuesta a incidentes disponible: asegura reacción rápida.
- Controles de acceso a Backups (copias de seguridad) y datos sensibles: previene exfiltración.

9. Desafíos y consideraciones éticas

- **Protección de datos y derechos de los usuarios**: Equilibrar seguridad con privacidad, cumpliendo normativas y expectativas de clientes.
- **Tolerancia a la incertidumbre:** Los riesgos cibernéticos son dinámicos; el CFO debe liderar una cultura de resiliencia adaptativa.
- **Auditoría y transparencia:** Mantener procesos de auditoría interna y externa para garantizar confiabilidad de la información financiera asociada a riesgos cibernéticos.

10. Conclusión

La ciberseguridad ya no es un tema marginal de TI; es un componente central de la gestión de riesgos y de la creación de valor para la empresa. El CFO, en su rol de guardián de la salud financiera y de la estrategia de valor, debe convertir la ciberseguridad en una disciplina operativa y financiera integrada a la planificación, gobernanza y reporte. Al hacerlo, las organizaciones pueden reducir pérdidas, proteger su reputación y asegurar una continuidad operativa en un entorno cada vez más interconectado y competitivo.

Referencias

- AICPA. EMC? Guías de gestión de riesgos de TI y control interno. Disponible en: https://www.aicpa.org
- CIS. (2023). Critical Security Controls for Effective Cyber Defense. Center for Internet Security. Recuperado de https://www.cisecurity.org/controls/
- COSO. (2017). Enterprise Risk Management—Integrated Framework. Committee of Sponsoring Organizations of the Treadway Commission. Recuperado de https://www.coso.org
- CPRA/CCPA (California Privacy Rights Act). Disponible en: https://oag.ca.gov/privacy/ccpa
- GDPR (Reglamento General de Protección de Datos de la UE). Disponible en: https://gdpr.eu
- Institute of Electrical and Electronics Engineers (IEEE) (2023). Ransomware and business interruption: financial impact. Disponible en: https://ieeexplore.ieee.org
- ISO/IEC. (2013). ISO/IEC 27001:2013 Information Security Management Systems – Requirements. International Organization for Standardization.
- LGPD (Lei Geral de Proteção de Dados, Brasil). Disponible en: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

- NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology. Recuperado de https://www.nist.gov/cyberframework
- PwC, “Global Crypto and Cyber Security” e informes de ciberseguridad corporativa. Disponible en: https://www.pwc.com

Autor

Jorge Ricardo Rendón Blacio
Vicepresidente del Comité Técnico Nacional de Transformación y Economía Digital
rrendon@rendonyasociados.com

En colaboración con:
Sofia Gamboa De La Parra
Presidente del Comité Técnico Nacional de Transformación y Economía Digital
sofiagamboadelaparra@gmail.com
María Gabriela Saavedra
Integrante del Comité Técnico Nacional de Transformación y Economía Digital
Carlos Amtmann Ituarte
integrante del Comité Técnico Nacional de Transformación y Economía Digital