KPMG

BOARD Leadership Center

CYBER SECURITY

#Leaders4Leaders

Cada día hay más ataques y más empresas impactadas tanto en su operación como en su REPUTACIÓN.

Estamos viviendo una situación histórica en el mundo y en el país, cada vez más hay más empresas que fueron **víctimas de ataques cibernéticos.** Los ataques materializados generan pérdidas para las organizaciones, impacto a sus accionistas y así mismo, impacto a los ejecutivos de la alta dirección y de las Juntas Directivas por su **responsabilidad en la gestión adecuada de los riesgos.**

Los ataque más comunes son:

Malware:
Es código malicioso que puede ser descargado en un correo o un acceso web, comprometiendo la confidencialidad, integridad y/o disponibilidad de la información corporativa. Por ejemplo virus o troyanos en archivos.

Ransomware:
Se trata del secuestro de los datos confidenciales o privados, cifrándolos (para impactar la operación), exfiltrándolos de la organización y luego solicitando el pago de un rescate.

Phishing y Spear Phishing:
El atacante intenta que su víctima ingrese generalmente a un vínculo a un sitio web y digite información confidencial.

Distributed Denial of Service (DDoS):
Este ataque bloquea el acceso a los servicios, impactando la operación de las organizaciones y el cumplimiento de sus obligaciones.

Los sectores más vulnerables en Latinoamérica son:

20% Entidades Públicas

16% Industria de Alimentos

16% Empresas de Retail

12% Sector Financiero

12% Sector de Seguros y Salud

15% **de crecimiento en ataques de ransomware en Latinoamérica en 2022. Colombia sigue siendo de los países altamente impactados.**

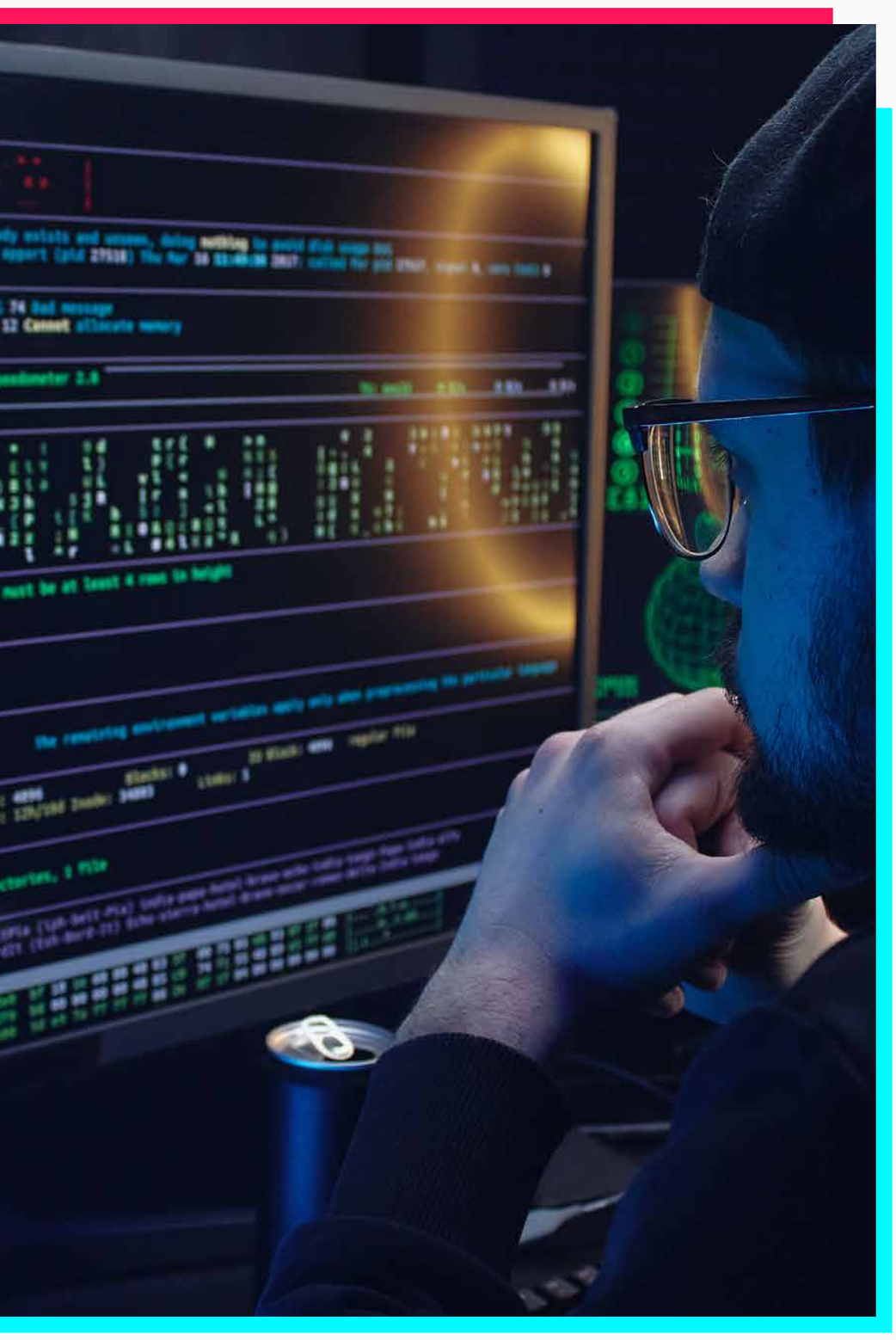
Colombia recibe en promedio **2.898 ATAQUES** cibernéticos al día

Fuente: *Reporte de ciberseguridad en Latinoamérica "ESET Security Report 2022"*

En 2021 los ataques cibernéticos generaron **US$ 6.179 MILLONES** en pérdidas

Fuente: *Datacredito Experian Informe global de Fraude e Identidad 2021*

Cuáles son los **RIESGOS** que enfrentan los directivos y las Juntas Directivas



24% de los CEOs reconocen que están poco preparados ante un ciberataque en 2022 a comparación del **13%** en 2021.

54% de los miembros de Juntas Directivas piensa que el CISO es el último responsable de la ciberseguridad de la organización.

31% de los miembros de Juntas Directivas no comprenden los detalles técnicos de ciberseguridad ni la información que presenta el CISO.

31% de los miembros de Juntas Directivas no considera al CISO como un ejecutivo clave de la organización.

Riesgo en la operación

- Continuidad de la operación
- Impacto en el día a día
- Pérdidas de ingresos

Riesgo Operacional

▲

Riesgo de Ciber Seguridad

Riesgo a la reputación

- Posiblemente el más difícil de reparar
- Es probable que impacte tanto en la organización como al individuo (directivo)

Riesgo Reputacional

Riesgo de litigios costosos

- Impacto Organizacional
- Impacto a los Directivos
- En algunos casos litigios a los miembros responsables de la organizaciones si se alega descuido, negligencia o falta de gestión

Riesgo Legal

KPMG

¿Cómo deberían las Juntas Directivas participar en la gestión de la CIBERSEGURIDAD?

Participación y supervisión de la Junta Directiva

LIDERAZGO Y GOBIERNO

- Reexaminar el resultado de la evaluación de la capacidad de protección de la organización.
- Revisar y aprobar la estrategia y las solicitudes de financiación.
- Métricas: presupuesto ejecutado de iniciativas de protección de la estrategia aprobada vs. Total del presupuesto.

LEGAL Y CUMPLIMIENTO

- Comprender el panorama regulatorio que afecta a la organización.
- Revisar y aprobar la financiación del seguro cibernético (si procede).
- Métricas: revisar las tendencias de litigios.

FACTORES HUMANOS

- Establece el tono de la cultura.
- Comprender los protocolos de capacitación y concientización en ciberseguridad.
- Métricas: revisar patrones / tendencias de incidentes de personal por falta de sensibilización vs. Total de personal sensibilizado.

OPERACIONES Y TECNOLOGÍA

- Comprender la madurez actual de la estructura de control.
- Revisar las métricas de tendencias de incidentes relevantes.
- Métricas:
  – Nivel de madurez actual vs. El objetivo.
  – Incidentes de impacto alto vs. Total de incidentes.

CONTINUIDAD EMPRESARIAL Y GESTIÓN DE CRISIS

- Comprender la capacidad de respuesta actual.
- Revisar el estado de madurez general del plan.
- Participar en ejercicios de mesa (table top).
- Métricas: cantidad de pruebas realizadas satisfactoriamente vs. Cantidad de pruebas planeadas.

GESTIÓN DE RIESGO DE LA INFORMACIÓN

- Revisar y aprobar la tolerancia al riesgo de ciberseguridad.
- Comprender el programa de proveedores externos.
- Métricas:
  – Riesgos mitigados dentro del nivel de tolerancia vs. Total de riesgos.
  – Proveedores externos que cumplen las disposiciones de seguridad de la organización vs. Total de proveedores.

RECOMENDACIONES
para miembros de Juntas Directivas

- Crear simulaciones de ciberataques en las que participe la Junta Directiva con el fin de sensibilizar y entender fácilmente los riesgos de ciberseguridad que pueda experimentar una organización.

- Crear indicadores de gestión de desempeño y de riesgo para que las Juntas Directivas puedan medir las acciones en pro del nivel de madurez objetivo.

- Contar con un manual de gestión de crisis de ciberseguridad socializado, apropiado y aprobado por la Junta Directiva.

Las Juntas Directivas necesitan entender que **la ciberseguridad es tanto su responsabilidad como la de los directivos, colaboradores y áreas de ciberseguridad de la organización.** Si los altos cargos se apropian de esta cultura *top-down* para tratar la ciberseguridad en cascada, la organización también lo hará.

Felipe Silgado
Director Cyber Security Services
KPMG Colombia