62. La Ciberseguridad como Pilar Estratégico: Más Allá del Cumplimiento

Cómo integrar la seguridad de la información en la estrategia corporativa, evitando que sea solo una respuesta reactiva a incidentes.

En los últimos años, la Ciberseguridad ha dejado de ser un tema exclusivo de las áreas de TI. Hoy, es un factor determinante para la continuidad operativa, la confianza del cliente y la reputación de cualquier organización. Sin embargo, en muchas empresas sigue predominando una visión reactiva: se actúa solo cuando ocurre un incidente o cuando una nueva ley exige cumplir ciertos requisitos.

Esta aproximación es insuficiente. La experiencia demuestra que la Seguridad de la Información debe ser parte integral de la estrategia corporativa, al mismo nivel que las decisiones financieras, comerciales o de innovación.

Del Cumplimiento a la Estrategia

Cumplir con las leyes y regulaciones —como la Ley Marco de Ciberseguridad y la Ley de Protección de Datos Personales en Chile— es, sin duda, un paso necesario. Pero limitar la gestión de la Seguridad al cumplimiento mínimo equivale a proteger el perímetro sin mirar lo que ocurre dentro de la organización.

La Ciberseguridad estratégica no busca solo evitar multas o sanciones: apunta a proteger los activos críticos del negocio, asegurar la continuidad de las operaciones y fortalecer la confianza de clientes, colaboradores y socios.

Incorporar esta mirada implica que la Seguridad deje de ser vista como un costo o una carga administrativa, para transformarse en un **inversor de confianza**, un **habilitador de negocios** y un **elemento diferenciador** frente a la competencia.

Las empresas que logran esto no solo responden a incidentes: los anticipan y se preparan para operar incluso en escenarios adversos.

Figure 1 - Visión 360º

Tres Niveles de Madurez

Podemos distinguir tres enfoques que reflejan distintos niveles de madurez organizacional:

1. **Nivel Reactivo:**
   La empresa actúa ante un incidente o cuando una autoridad lo exige. Las medidas son puntuales y no se mantienen en el tiempo.
   Ejemplo: cambiar contraseñas solo después de una filtración.
2. **Nivel Preventivo:**
   Se implementan controles básicos, políticas internas y capacitaciones. Hay una mayor conciencia del riesgo, pero la seguridad aún depende de iniciativas aisladas.
   Ejemplo: disponer de antivirus, firewalls y planes de respaldo, sin integración con la estrategia global.
3. **Nivel Estratégico:**
   La Ciberseguridad forma parte del gobierno corporativo. Se define un marco de gestión, se evalúan los riesgos de negocio y se invierte en capacidades sostenibles.
   Ejemplo: contar con un Comité de Seguridad, indicadores de desempeño, y políticas alineadas con la continuidad operativa y los objetivos estratégicos.

El desafío actual es pasar del nivel preventivo al estratégico. Para ello, la alta dirección debe asumir un rol activo en la toma de decisiones y en la priorización de inversiones en Seguridad.

La Información como Activo Crítico

Toda empresa —sin importar su tamaño o sector— maneja información sensible: datos personales, financieros, operativos o estratégicos. Esa información tiene valor económico y reputacional, y su pérdida o exposición puede tener consecuencias graves. Por eso, las organizaciones deben aprender a **gestionar la información como un activo más**, igual que gestionan sus recursos financieros o su infraestructura física. Esto implica clasificar los datos según su criticidad, establecer controles de acceso, definir responsables y monitorear permanentemente los riesgos.

Una cultura de Seguridad efectiva se construye cuando todos —desde el directorio hasta los colaboradores— comprenden el valor de la información y el impacto que tendría perderla. La Seguridad deja entonces de ser tarea del área TI, para convertirse en una responsabilidad compartida.

El Factor Humano y la Cultura Organizacional

Estudios internacionales estiman que más del 80% de los incidentes de seguridad tienen origen humano: errores, descuidos o malas prácticas.

Por eso, las políticas y tecnologías deben acompañarse de **programas de sensibilización y formación continua**.

No se trata solo de capacitar, sino de generar hábitos: verificar correos sospechosos, proteger contraseñas, actualizar equipos, y actuar con sentido de responsabilidad digital. Una empresa segura es aquella en la que las personas entienden que cada acción puede fortalecer o debilitar la protección colectiva.

Tecnología, Procesos y Gobernanza

La Ciberseguridad efectiva se apoya en tres pilares:

- **Tecnología:** herramientas de detección, monitoreo y respuesta (antivirus, EDR - - - *Endpoint Detection and Response*, SIEM -*Security Information and Event Management,* cifrado, autenticación multifactor, etc.).
- **Procesos:** políticas, procedimientos y protocolos que estandarizan la gestión del riesgo y la respuesta a incidentes.
- **Gobernanza:** estructura de roles, responsabilidades y métricas que permiten mantener la Seguridad como parte del gobierno corporativo.

Solo cuando estos tres elementos se combinan bajo una visión estratégica, la organización puede anticiparse a las amenazas, minimizar impactos y sostener la confianza de su entorno.

Mirando Hacia Adelante

La digitalización de los negocios, el uso de la nube, la inteligencia artificial y el trabajo remoto han ampliado la superficie de ataque. En este contexto, la Ciberseguridad debe evolucionar al mismo ritmo que la Transformación Digital.

Las empresas que **integran la seguridad desde el diseño** —en sus procesos, sistemas y contratos— estarán mejor preparadas para enfrentar los desafíos que vienen.

Adoptar la Ciberseguridad como **pilar estratégico** no significa gastar más, sino **invertir mejor**: priorizar los riesgos relevantes, fortalecer la cultura interna y asegurar que las decisiones tecnológicas estén alineadas con los objetivos de negocio.

En Síntesis

Más allá del cumplimiento, la Ciberseguridad es una condición esencial para la sostenibilidad de las organizaciones modernas.

Es el puente entre la confianza y la innovación, entre la gestión responsable y la competitividad.

Convertirla en parte del ADN corporativo no solo protege a la empresa: **la fortalece, la hace más confiable y más preparada para un futuro digital seguro.**

Información Adicional

Cyber security beyond compliance: Why resilience is the new boardroom imperative

https://www.computerweekly.com/opinion/Cyber-security-beyond-compliance-Why-resilience-is-the-new-boardroom-imperative

Beyond compliance: new Joint Standard boosts cyber resilience for financial Institutions

https://www.ey.com/en_za/services/cybersecurity/beyond-compliance--new-joint-standard-boosts-cyber-resilience-for-financial-institutions

Cybersecurity dominates concerns among the C-suite, small businesses, and the nation

https://www.ibm.com/think/insights/cybersecurity-dominates-concerns-c-suite-small-businesses-nation