Gobernanza y seguridad en la información

Para fortalecer la protección y el almacenamiento de la información dentro del marco de gobierno corporativo, es esencial comprender los desafíos actuales y aplicar prácticas de resguardo que respondan a un entorno digital vulnerable. La gestión de la información es hoy una prioridad para la mayoría de las industrias, particularmente en sectores regulados como el financiero, la salud y la tecnología. La digitalización y el incremento en la cantidad de datos generados por las empresas han hecho que su protección sea un pilar para la supervivencia empresarial y la confianza pública.

La seguridad y resguardo de la información hoy en día

- Según un informe de IBM, el costo promedio global de una violación de datos en 2023 alcanzó los 4.45 millones de dólares, lo cual refleja un aumento constante en los últimos cinco años. Los sectores de salud y tecnología suelen ser los más afectados, donde las consecuencias económicas y de reputación pueden ser significativas.

- De acuerdo con un estudio de Kaspersky, el 52% de las empresas han experimentado fugas de datos debido a negligencia interna, como errores humanos o falta de políticas de protección adecuadas. Este dato resalta que los riesgos no solo provienen de amenazas externas, sino también de la necesidad de fortalecer la capacitación del personal y de implementar controles internos efectivos.

- Normativas como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea y la Ley Federal de Protección de Datos Personales en Posesión de los Particulares en México exigen que las empresas adopten medidas estrictas para proteger la información. En 2022, las sanciones por infracciones al GDPR superaron los 1,000 millones de euros, evidenciando la seriedad de los reguladores al abordar el tema de la protección de datos.

Las empresas que buscan mejorar la gestión de la información y mitigar riesgos deben implementar una combinación de tecnología y prácticas de gobernanza efectiva:

1. **Políticas de seguridad sólidas y claras**
   Tener protocolos definidos para el manejo, almacenamiento y eliminación de datos es esencial. Un estudio de PwC indica que el 77% de las organizaciones con políticas de seguridad claras y efectivas enfrentan menos incidentes de seguridad graves.

2. **Control de acceso y autenticación**
   Limitar el acceso a la información confidencial sólo al personal autorizado y con autenticación avanzada.

3. **Fomento de la participación y autonomía**
   Es vital involucrar a los empleados en la toma de decisiones y brindarles la autonomía para ejecutar sus tareas de la mejor manera posible.

4. **Auditorías y monitoreo continuo**
   Realizar auditorías frecuentes para asegurar que los protocolos de seguridad se mantengan actualizados y para detectar posibles vulnerabilidades.

5. **Implementación de infraestructura tecnológica robusta:**
   Soluciones como la encriptación, autenticación de múltiples factores y sistemas avanzados de seguridad (por ejemplo, inteligencia artificial para detección de amenazas) son indispensables. Se estima que para 2025 las empresas aumentarán su gasto en tecnología de seguridad de la información un 15% debido al incremento de los ciberataques.

6. **Almacenamiento en la nube con protección avanzada:**
   La migración de datos a la nube es una tendencia en aumento, y para proteger esta información es necesario recurrir a proveedores confiables que cumplan con normativas como ISO 27001 y ISO 27018, que aseguran la privacidad y protección de datos en la nube.

7. **Cultura de gobernanza y responsabilidad en la información**
   La capacitación periódica del personal sobre los riesgos y mejores prácticas en el manejo de datos es esencial.

La gobernanza en la protección de la información

Una buena gobernanza implica supervisión constante y la creación de controles internos y auditorías regulares en seguridad de la información. Un Comité de Riesgo y Cumplimiento como apoyo al Consejo de Administración puede ayudar a monitorear y mejorar las prácticas de protección de datos, alineándose con los objetivos estratégicos de la empresa.

El Comité de Riesgos y Cumplimiento desempeña un papel crítico en la gobernanza de la protección de la información. Sus funciones incluyen:

Preguntas clave para evaluar su desempeño en el resguardo de la información:

- ¿Qué medidas avanzadas de almacenamiento y protección de datos se están implementando en la empresa?
- ¿Cuál es el papel del Consejo de Administración en la supervisión de la seguridad de la información?
- ¿Qué protocolos están vigentes para proteger los datos personales de clientes y colaboradores?
- ¿Cómo influye el cumplimiento normativo en la estructura de resguardo de datos?

- Evaluación de riesgos: Este Comité debe analizar tanto los riesgos internos como externos, asegurando que la organización esté preparada para responder a amenazas potenciales.
- Desarrollo de políticas: El Comité debe participar en el desarrollo y la actualización de políticas de seguridad de la información, asegurando que sean alineadas con las mejores prácticas de la industria y las regulaciones pertinentes.
- Monitoreo de cumplimiento: Es esencial que el comité supervise el cumplimiento de las políticas de seguridad y que se asegure de que se realicen las capacitaciones necesarias para el personal. Según PwC, las empresas con un fuerte enfoque en la capacitación en seguridad tienen un 70% menos de probabilidades de sufrir un incidente de seguridad .
- Consejo de Administración: El Comité debe proporcionar informes regulares al Consejo de Administración sobre el estado de la seguridad de la información, así como sobre cualquier incidente significativo y las medidas correctivas adoptadas.
- Fomento de la cultura de seguridad: Un comité eficaz también puede promover una cultura de seguridad dentro de la organización. Esto incluye el establecimiento de un código de conducta relacionado con la seguridad de la información y la creación de canales de comunicación abiertos para que los empleados puedan reportar preocupaciones o incidentes sin temor a represalias.