Deloitte.

Digitalización, ciberseguridad y Gobierno Corporativo: Cómo proteger los activos digitales de la empresa

Boletín de Gobierno Corporativo

La digitalización ha transformado radicalmente el entorno empresarial, generando nuevas oportunidades de crecimiento, eficiencia y competitividad. Sin embargo, este proceso también ha traído consigo una creciente exposición a riesgos cibernéticos que amenazan los activos digitales de las organizaciones. En este contexto, el Gobierno Corporativo se convierte en un pilar fundamental para garantizar la protección de dichos activos, mediante la implementación de políticas, estructuras y controles que aseguren una gestión responsable y estratégica de la ciberseguridad.

Los órganos de gobierno, como el consejo de administración, los comités de auditoría y riesgos, y los miembros de la alta dirección en su conjunto, tienen la responsabilidad de liderar la transformación digital de manera segura, ética y conforme a las regulaciones vigentes. Su rol no se limita a supervisar, sino que deben participar activamente en la definición de estrategias, asignación de recursos y evaluación de riesgos tecnológicos.

Digitalización y su impacto en la gobernanza corporativa

La digitalización implica la adopción de tecnologías como inteligencia artificial, big data, computación en la nube y automatización de procesos. Estas herramientas permiten mejorar la toma de decisiones, optimizar operaciones y generar valor para los *stakeholders*. No obstante, también generan vulnerabilidades que pueden ser explotadas por agentes maliciosos.

El Gobierno Corporativo de cada organización debe adaptarse a este nuevo entorno, incorporando la gestión tecnológica como parte integral de su estructura. Esto incluye la creación de comités especializados en tecnología, la actualización de políticas de seguridad de la información y la formación continua de los consejeros en temas digitales. La supervisión de la transformación digital debe estar alineada con los objetivos estratégicos de la empresa y considerar los riesgos inherentes al uso de tecnologías emergentes.

Las vulnerabilidades que surgen con la digitalización pueden ser explotadas de varias maneras, dependiendo de la tecnología y el contexto. Algunos ejemplos son:

01. **Inteligencia Artificial (IA)**

- **Manipulación de algoritmos:** Actores maliciosos pueden introducir datos sesgados (ataques adversarios) para alterar decisiones automatizadas.
- ***Deepfakes* y suplantación:** Uso de IA para crear identidades falsas que afectan la reputación corporativa.

02. **Big Data**

- **Robo de información sensible:** Bases de datos masivas son objetivos para ataques que buscan datos financieros, estratégicos o personales.
- **Inferencia indebida:** *Hackers* pueden combinar datos públicos y privados.

03. **Computación en la nube**

- **Acceso no autorizado:** Si la configuración de seguridad es débil, atacantes pueden entrar a sistemas críticos.
- **Secuestro de cuentas** *(Account Hijacking):* Robo de credenciales para controlar recursos en la nube.

La ciberseguridad no es una función exclusiva del área de T.I. Es una responsabilidad transversal que debe ser liderada desde los niveles más altos de la organización.

04. **Automatización de procesos**

- **Explotación de *bots:*** Si los *bots* no tienen controles robustos, pueden ser manipulados para ejecutar transacciones fraudulentas.
- **Interrupción operativa:** *Malware* puede detener procesos automatizados, afectando la continuidad del negocio.

Impacto en la gobernanza corporativa

Estas vulnerabilidades pueden:

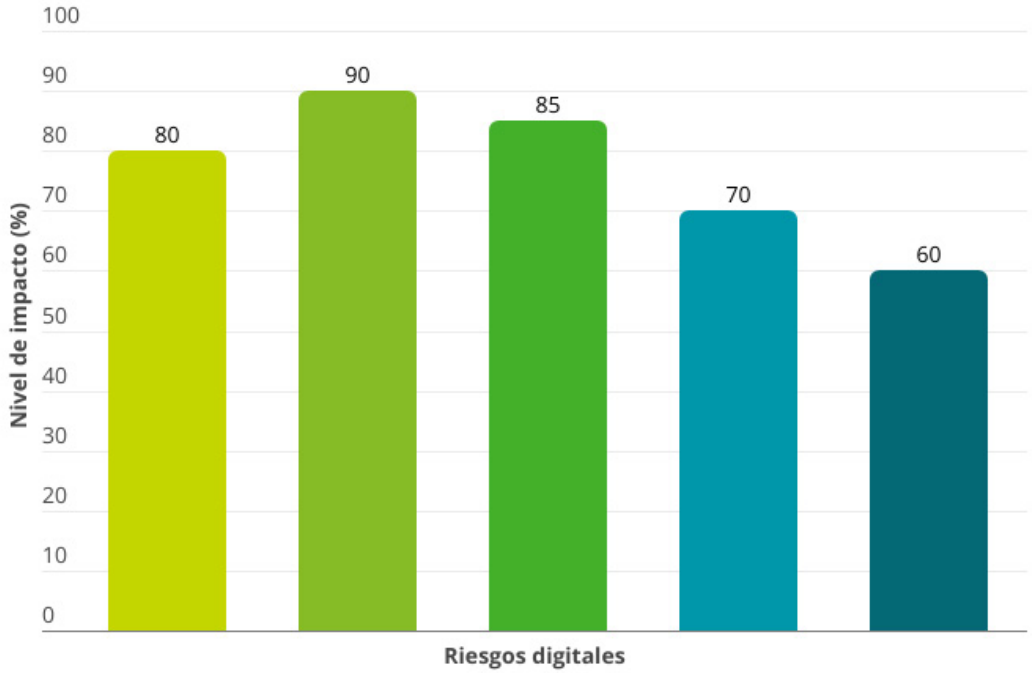
- Comprometer la **confidencialidad** de información estratégica.
- Alterar la **integridad** de decisiones del Consejo.
- Generar riesgos reputacionales y regulatorios.

Ciberseguridad como responsabilidad estratégica

La ciberseguridad no es una función exclusiva del área de T.I. Es una responsabilidad transversal que debe ser liderada desde los niveles más altos de la organización. Según la revisión sistemática publicada en la *Revista Talento*, "las estrategias más efectivas para proteger los activos digitales incluyen la formación continua del personal, la implementación de tecnologías avanzadas y el desarrollo de una cultura organizacional orientada a la seguridad".

Por su parte, los órganos de gobierno deben garantizar que existan mecanismos de control interno robustos, auditorías periódicas, simulaciones de ataques y protocolos de respuesta ante incidentes. Además, deben establecer indicadores clave de desempeño *(KPIs)* para evaluar la madurez de la ciberseguridad en la organización.

A continuación, se muestran los riesgos digitales comunes y su nivel de impacto:



Fuente: Elaboración basada en tendencias de ciberseguridad (Revista Talento, INCIBE)

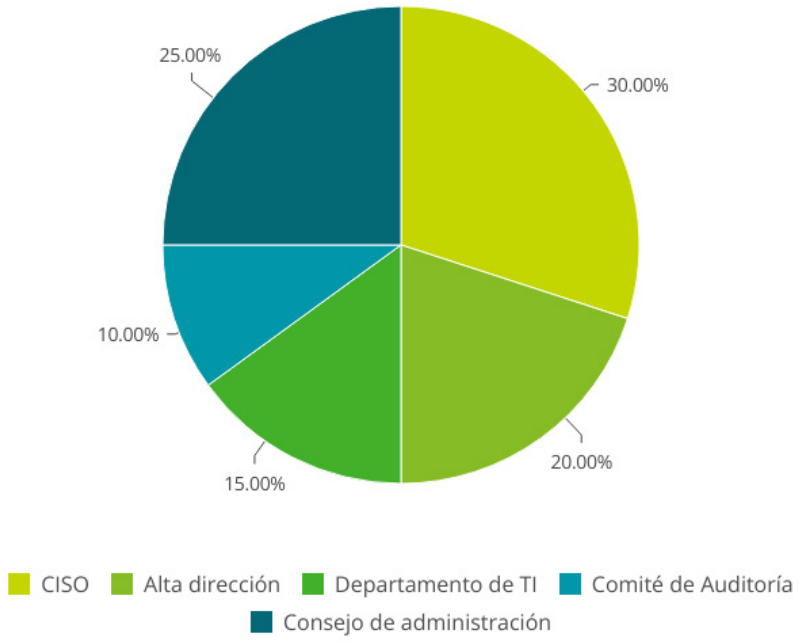
Esta gráfica muestra como uno de los principales riesgos se presenta en el *ransomware*, el cual aparece como el más crítico (90%), seguido por fugas de datos (85%) y ***phishing*** (80%), que son amenazas frecuentes y con consecuencias financieras y reputacionales significativas. Acceso no autorizado (70%) y errores humanos (60%) también representan riesgos importantes, aunque con menor impacto relativo. Con ello se refuerza la idea de que la ciberseguridad debe ser prioritaria en la estrategia corporativa, ya que los riesgos no solo son técnicos, sino que pueden afectar la continuidad del negocio.

El papel de los consejeros y la alta dirección

Los consejeros y miembros de la alta dirección tienen un rol decisivo en la protección de los activos digitales. Su participación en la estrategia de ciberseguridad permite que los riesgos técnicos se mitiguen y puedan convertirse en impactos financieros, reputacionales y/u operativos. Para lograrlo, es fundamental que estos líderes establezcan políticas claras de gestión de riesgos, promuevan la integración de la ciberseguridad en la planificación estratégica y aseguren la asignación de recursos adecuados. Además, deben impulsar la creación de comités especializados y garantizar que la información sobre amenazas y vulnerabilidades llegue al nivel directivo para una toma de decisiones informada.

Adicionalmente, los consejeros y los miembros de la alta dirección deben fomentar una cultura de seguridad mediante campañas de concientización, liderar con el ejemplo en el cumplimiento de normas y promover la responsabilidad compartida entre todos los colaboradores. La implicación del consejo en la supervisión de la ciberseguridad también es clave para garantizar la resiliencia organizacional y la continuidad del negocio.

Distribución de responsabilidades en ciberseguridad



Fuente: Elaboración basada en recomendaciones de gobernanza y ciberseguridad (AESYC, INCIBE)

El Gobierno Corporativo debe integrar la ciberseguridad en la estrategia general del negocio, incluyendo aspectos como la gestión de proveedores, fusiones y adquisiciones, y desarrollo de productos. La falta de implicación puede derivar en sanciones, pérdida de reputación y afectación directa al valor de la empresa.

La gráfica muestra cómo se reparten las responsabilidades en materia de ciberseguridad dentro de la estructura de gobierno corporativo. El *CISO (Chief Information Security Officer)* concentra el mayor porcentaje (30%), ya que es el responsable técnico principal. Le sigue el Consejo de Administración (25%) y la Alta Dirección (20%), quienes tienen un rol estratégico y de supervisión. El Departamento de TI (15%) y el Comité de Auditoría (10%), reflejando que la protección de activos digitales es una tarea compartida y no exclusiva de un área técnica. Esto evidencia la necesidad de una gobernanza integral donde todos los niveles participen activamente.

Marco normativo y responsabilidad legal

Normativas como la Directiva NIS2 (legislación de la Unión Europea que actualiza la Directiva sobre seguridad de redes y sistemas de información (NIS) para reforzar la ciberseguridad en la UE) han elevado el nivel de exigencia para los líderes empresariales, estableciendo que la alta dirección puede ser legalmente responsable en caso de incumplimiento de las obligaciones de ciberseguridad. Esto implica que los consejeros deben estar informados, capacitados y comprometidos con la gestión de riesgos digitales.

El Gobierno Corporativo debe integrar la ciberseguridad en la estrategia general del negocio, incluyendo aspectos como la gestión de proveedores, fusiones y adquisiciones, y desarrollo de productos. La falta de implicación puede derivar en sanciones, pérdida de reputación y afectación directa al valor de la empresa.

Tipos de activos digitales en las empresas

- **Datos sensibles:** Información personal de clientes, empleados y proveedores.
- **Propiedad intelectual:** Patentes, diseños, algoritmos y *know-how*.
- **Infraestructura tecnológica:** Servidores, redes, sistemas operativos y aplicaciones críticas.
- **Plataformas digitales:** Sitios web, aplicaciones móviles y sistemas de comercio electrónico.
- **Bases de datos:** Información financiera, registros de transacciones y análisis de mercado.

Políticas de seguridad y protección de activos digitales

Como mejor práctica, se recomienda que las empresas desarrollen las siguientes políticas:

- **Control de accesos:** Definir roles y permisos para evitar accesos no autorizados a sistemas, programas o documentos.
- Gestión de contraseñas y autenticación multifactor.
- **Protección de datos:** Cifrado, copias de seguridad y anonimización.
- **Gestión de incidentes:** Protocolos claros para detección, respuesta y recuperación.
- **Evaluación de proveedores:** Cláusulas contractuales sobre ciberseguridad.

Proceso para desarrollo, aprobación y monitoreo de políticas:

- Quién las desarrolla: El Departamento de TI junto con el CISO y el área de cumplimiento normativo.
- Quién las aprueba: El Director General las presenta para aprobación al Consejo de Administración o al Comité de Auditoría y Riesgos, asegurando alineación con la estrategia corporativa.
- Quién las monitorea: El Comité de Auditoría, apoyado por auditorías internas y reportes periódicos al consejo.

Este proceso garantiza que las políticas no solo existan, sino que se mantengan actualizadas y efectivas frente a nuevas amenazas.

Conclusión

La protección de los activos digitales en la era de la digitalización requiere un enfoque integral, estratégico y ético, liderado por los órganos de gobierno de las entidades.

La ciberseguridad debe ser vista como una inversión en resiliencia, reputación y sostenibilidad, y no como un gasto operativo.

Los consejeros y miembros de la alta dirección tienen la responsabilidad de garantizar que la empresa esté preparada para enfrentar los desafíos del entorno digital, mediante políticas claras, estructuras de gobernanza eficaces y una cultura organizacional comprometida con la seguridad. En definitiva, el éxito de la transformación digital depende de la capacidad del Gobierno Corporativo para anticipar riesgos, tomar decisiones informadas y proteger los activos que sustentan el valor de la empresa.

Contacto:

Daniel Aguiñaga
Socio Líder de Gobierno Corporativo
daguinaga@deloittemx.com
Tel. +52 55 5080 6000

Rodrigo Badiola
Socio de Gobierno corporativo
rbadiola@deloittemx.com
Tel. +52.55.5080 7587

Fuentes:

1. https://www.pmg-ssi.com/2025/03/cual-es-la-responsabilidad-de-la-alta-direccion-en-nis2/
2. https://aesyc.com/el-rol-del-consejo-en-la-ciberseguridad-estrategia-cumplimiento-y-resiliencia-digital/
3. https://revistatalento.org/index.php/talento/article/view/1479
4. https://www.linkedin.com/pulse/el-rol-de-la-alta-direcci%C3%B3n-en-estrategia-c%C3%A9sar-viteri-tzzbe
5. https://www.incibe.es/empresas

Deloitte.