Informes de ciberseguridad para la alta gerencia: lo que los CISOs deben saber

Edición 2025

La presentación de informes sobre riesgos cibernéticos es un componente crítico para la supervisión efectiva por parte de la alta gerencia, particularmente a medida que las amenazas cibernéticas impactan cada vez más la estrategia empresarial, el rendimiento financiero y la reputación. Las juntas directivas buscan actualizaciones concisas y libres de jerga que conecten claramente los riesgos cibernéticos con los resultados del negocio. Muchas de ellas ahora confían en cuadros de mando o **scorecards** cibernéticos. Cuando se estructuran de manera consistente y se vinculan con el impacto estratégico, estas herramientas ayudan a los ejecutivos a evaluar el riesgo, rastrear inversiones y anticipar amenazas emergentes.

Sin embargo, algunas organizaciones pueden no cumplir con estas expectativas. Las barreras comunes incluyen el uso inconsistente de indicadores clave de riesgo, desafíos para agregar y analizar tendencias de datos entre sistemas, y comprensión limitada del impacto de estos riesgos a nivel de unidad de negocio. Las lagunas en inteligencia de amenazas externa y la dificultad para alinear los informes internos socavan aún más la claridad. Para satisfacer las necesidades de la junta directiva, los responsables de seguridad de la información (CISOs) deben estandarizar los informes de ciberseguridad, vincular las métricas al impacto empresarial y presentar el riesgo en un formato que permita la supervisión y la toma de decisiones informadas. Bien hecho, el informe de ciberseguridad se convierte en una herramienta estratégica, no solo en un ejercicio de cumplimiento.

¿Qué información resulta esencial para la junta directiva?

Los directores pueden enfocar su supervisión en materia de ciberseguridad —y sus conversaciones con la administración— a partir de las siguientes preguntas clave:

1. ¿Cuál es nuestra exposición al riesgo?
2. ¿Qué estamos haciendo al respecto?
3. ¿Estamos haciendo lo suficiente para abordar nuestros riesgos?
4. ¿Estamos preparados para una brecha material o un ataque de ransomware?
5. ¿Cumplimos con las últimas normas y regulaciones?

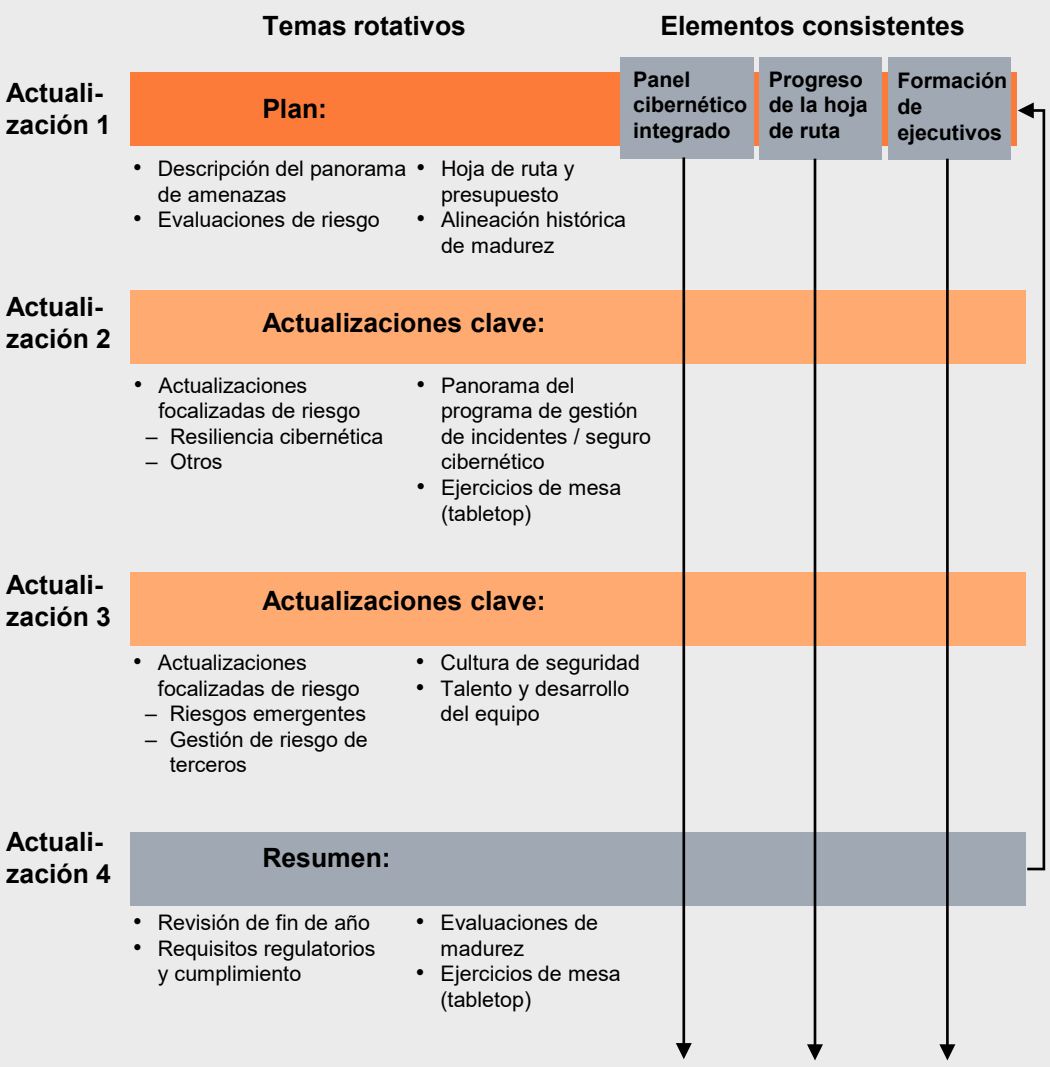
Esta lista no es exhaustiva, pero ofrece a los directores un punto de partida para entender los riesgos clave y cómo la empresa los gestiona. Al planificar materiales previos a la reunión y al presentar comentarios en las sesiones, los CISOs deben considerar cómo su contenido responde a estas cinco preguntas.

Dato: 64% de los comités de auditoría del S&P 500 supervisan la ciberseguridad.

¿Con qué frecuencia debería un CISO reportar a la junta directiva?

Las prácticas varían, pero muchas empresas proporcionan informes consistentes, generalmente trimestrales y, por lo común, al comité de auditoría. Utilizar un calendario anual para definir los temas de cada reunión puede ayudar a establecer expectativas. Programar los temas de esta manera también aclara qué informes recibirá la junta directiva de forma regular y cuáles serán de manera periódica.

Ejemplo de calendario cibernético anual para facilitar la supervisión



¿Qué información debe proporcionar un CISO?

No existe una plantilla universal para los informes de ciberseguridad. Cada empresa es diferente y tiene necesidades de información únicas. Sin embargo, lo que está claro es que el riesgo cibernético está compuesto por una variedad de riesgos que pueden afectar diferentes partes del negocio de distintas maneras. Los informes a la junta directiva deben reflejar este enfoque matizado, detallando cómo se gestionan y monitorean los riesgos significativos a nivel de unidad de negocio. Además, aquí hay algunos componentes que un CISO podría considerar incluir:

Los materiales de informes consistentes podrían incluir:

Descripción del panorama de amenazas (corto y largo plazo), incluyendo los sistemas de monitoreo y gestión de la empresa.

Información sobre cualquier brecha exitosa en la empresa o en proveedores críticos

Información sobre brechas de alto perfil en otras compañías y lecciones aprendidas para la empresa

Evaluación del programa de la empresa con una evaluación de madurez del programa cibernético frente a un marco industrial (p. ej., el Instituto Nacional de Estándares y Tecnología

Mapa de calor o resumen de los riesgos cibernéticos clave

Métricas para monitorear y reportar regularmente eventos y programas de seguridad de la información, incluyendo amenazas relevantes, brechas que incrementen riesgos por unidad de negocio (p. ej., pérdida de datos) y el estado en acciones de remediación.

Estado de proyectos de cumplimiento regulatorio

Perspectivas externas o materiales educativos

Los temas de los informes rotativos y de análisis profundo podrían incluir:

Una visión general de la estrategia de seguridad de la empresa y de las políticas de seguridad de la información que respaldan el programa integral de seguridad.

Cobertura de seguros cibernéticos

Gestión de riesgo de terceros

Tecnologías emergentes y cómo el programa de ciberseguridad de la empresa está incorporando o gestionando cualquier cambio en la postura de riesgo

Gestión de crisis, incluyendo respuesta a incidentes, continuidad del negocio y protocolos de recuperación ante desastres, así como la fecha de la última prueba realizada y los aprendizajes obtenidos.

Leyes, políticas y programas de privacidad/ciber aplicables

Asignación de recursos — financiación y personal

Un informe cibernético efectivo no tiene por qué ser complejo. Cada trimestre, los directores deben recibir una visión transparente del riesgo de la empresa, así como de su seguimiento y gestión. Con esa consistencia, las juntas directivas pueden comprender mejor las tendencias, posibles brechas y prioridades para mantener seguros los datos y sistemas de la empresa.

Contactos:

Bismark Rodríguez
Socio Líder Regional de Consultoría
bismark.rodriguez@pwc.com

Edwin Orrico
Gerente Senior de Ciberseguridad y Privacidad
edwin.orrico@pwc.com

Susana Pino
Socia Líder Regional de Risk Assurance Services (RAS)
pino.susana@pwc.com

Isaac Rodríguez
Gerente Senior de Ciberseguridad y Privacidad
isaac.rodriguez@pwc.com

pwc.com