Fomento de la capacidad en materia de ciberseguridad Cuadro de herramientas para organizaciones financieras

Guía para la junta directiva: Liderazgo en ciberseguridad

Fundamentos de la gobernanza del riesgo cibernético

Confirme que puede responder de forma afirmativa a las siguientes preguntas:

1. ¿Su organización **ha cumplido los requisitos legales y reglamentarios pertinentes**?

2. ¿Su organización **ha cuantificado sus exposiciones cibernéticas y probado su resiliencia financiera**?

3. ¿Su organización ha implementado un **plan de mejora** para garantizar que las exposiciones están dentro de su predisposición al riesgo acordado?

4. ¿La directiva regularmente **discute información concisa, clara y práctica sobre la resiliencia cibernética de la organización proporcionada por la dirección**?

5. ¿Su organización tiene **planes de respuesta a incidentes que se han probado recientemente**, incluido a nivel directivo?

6. ¿Están las **funciones de personas clave responsables de gestionar el riesgo cibernético** claras y en sintonía con las tres líneas de defensa?

7. ¿Ha obtenido **validación y garantía independientes** de la postura de riesgo cibernético de su organización?

Supervisión

Como el nivel más alto de liderazgo de su organización, la junta directiva asume la responsabilidad final por el cumplimiento en materia de riesgos cibernéticos y, por tanto, debe supervisar la estrategia, las políticas y las actividades de la organización en esta área. En concreto, la junta directiva debe:

⇒ Asumir la responsabilidad final de supervisar el riesgo y la resiliencia cibernéticos, ya sea como junta completa o por delegación de supervisión a un comité de junta específico.
⇒ Asignar un directivo corporativo, normalmente el CISO (Chief Information Security Officer [Director de seguridad de la información]), para que sea el responsable de informar sobre la capacidad de su organización de gestionar la resiliencia cibernética y el progreso en la implementación de objetivos de resiliencia cibernética. Asegurarse de que este directivo tiene acceso regular a la junta, autoridad suficiente, dominio de la materia, experiencia y recursos para cumplir estas obligaciones.
⇒ Definir anualmente la tolerancia al riesgo de su organización; garantizar la coherencia con su estrategia corporativa y su predisposición al riesgo.
⇒ Asegurarse de que se realiza anualmente una revisión formal e independiente de la resiliencia cibernética de su organización.
⇒ Supervisar la creación, implementación, pruebas y mejora continua de los planes de resiliencia cibernética, asegurándose de que se alineen en toda su organización y de que su CISO u otro directivo responsable informe regularmente sobre ellos a la junta.
⇒ Integrar la evaluación de riesgos y resiliencia cibernética en la estrategia empresarial general de su organización, gestión de riesgos, presupuestos y asignación de recursos, con el objetivo de integrar completamente el riesgo cibernético en el riesgo operativo general.
⇒ Revisar periódicamente su rendimiento en cuanto a lo anterior y considerar asesoramiento independiente para la mejora continua.

Mantenerse informado

La supervisión eficaz del riesgo cibernético de la junta depende del dominio de la materia por parte de los miembros y de que la información esté actualizada.

⇒ Garantice que todas las personas que se incorporen a la junta tengan habilidades y conocimientos actualizados para comprender y gestionar los riesgos planteados por amenazas cibernéticas.
⇒ Solicite asesoramiento habitual de la gerencia sobre la exposición al riesgo actual y futuro de su organización, los requisitos normativos pertinentes y los índices de referencia de la industria y la sociedad para la predisposición al riesgo. Además, participe en sesiones informativas periódicas sobre los últimos desarrollos con respecto al panorama de las amenazas y el entorno normativo, la planificación conjunta y las visitas a colegas y líderes de mejores prácticas en ciberseguridad, así como los intercambios a nivel de junta en la gobernanza y los informes.
⇒ Responsabilice a la gerencia de informar de una evaluación cuantificada y comprensible de los riesgos cibernéticos, amenazas y eventos como un elemento de la orden del día permanente durante las reuniones de la junta.
⇒ Mantenga el conocimiento de los desafíos sistémicos continuos, como las vulnerabilidades de la cadena de suministro, las dependencias comunes y la brecha en el intercambio de información entre juntas sobre la gobernanza de los riesgos cibernéticos.

Explicación del contexto

Junto con la alta gerencia, la junta debe establecer e ilustrar los valores fundamentales de su organización, la cultura del riesgo y las expectativas con respecto a la resiliencia cibernética.

⇒ Promueva una cultura en la que el personal de todos los niveles reconozca sus responsabilidades importantes para garantizar la resiliencia cibernética de su organización. Lidere con el ejemplo.
⇒ Supervise el papel de la gerencia en la promoción y el mantenimiento de la cultura del riesgo de su organización. Promueva, supervise y evalúe la cultura del riesgo, teniendo en cuenta el impacto de la cultura sobre la seguridad y la solidez, y haga cambios cuando sea necesario.
⇒ Deje claro que espera que todo el personal actúe con integridad y que informe rápidamente de los casos de incumplimiento observados dentro o fuera de su organización.

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE · SWIFT INSTITUTE · FS-ISAC · Standard Chartered · CYBER READINESS INSTITUTE · GLOBAL CYBER ALLIANCE