CIBERSEGURIDAD PARA ORGANIZACIONES MÁS PEQUEÑAS

LISTA DE COMPROBACIÓN DE LA JUNTA DIRECTIVA: LIDERAZGO DE CIBERSEGURIDAD

FUNDAMENTOS DE LA GOBERNANZA DEL RIESGO CIBERNÉTICO

☐ **Como grupo, evalúe periódicamente si la junta directiva puede responder afirmativamente a las siguientes preguntas:**

- ¿Su organización ha cumplido los requisitos legales y reglamentarios pertinentes, como el RGPD?
- ¿Su organización ha cuantificado sus exposiciones cibernéticas y probado su resiliencia financiera?
- ¿Su organización ha implementado un plan de mejora para garantizar que las exposiciones están dentro de su predisposición al riesgo acordado?
- ¿La junta directiva regularmente discute información concisa, clara y práctica sobre la resiliencia cibernética de la organización proporcionada por la dirección?
- ¿Su organización tiene planes de respuesta a incidentes que se han probado recientemente, incluido a nivel directivo?
- ¿Están las funciones de personas clave responsables de gestionar el riesgo cibernético claras y en sintonía con las tres líneas de defensa?
- ¿Ha obtenido validación y garantía independientes de la postura de riesgo cibernético de su organización, como por ejemplo a través de una prueba, certificación o seguro?

☐ **Si no puede responder de forma afirmativa a una o más de las anteriores preguntas, trabaje con su CEO (Chief Executive Officer [Director ejecutivo]), CISO (Chief Information Security Officer [Director de seguridad de la información]), personal de la organización pertinente o recursos externos para corregir el problema.**

SUPERVISIÓN

☐ **Asegúrese de que la junta directiva es consciente de su papel como titular de la responsabilidad final en cuanto al riesgo cibernético y la resiliencia de su organización.**

☐ **Delegue la supervisión a un comité de junta directiva específico si se considera necesario.**

☐ **Asigne un directivo corporativo, normalmente el CISO, 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.**

☐ **Asegúrese de que este directivo tiene acceso regular a la junta directiva, autoridad suficiente, dominio de la materia, experiencia y recursos para cumplir estas obligaciones.**

☐ **Defina anualmente la tolerancia al riesgo de su organización; garantice la coherencia con su estrategia corporativa y su predisposición al riesgo.**

☐ **Asegúrese de que se realiza anualmente una revisión formal e independiente de la resiliencia cibernética de su organización.**

☐ **Integre la evaluación de riesgos y resiliencia cibernética en la estrategia empresarial general de su organización, gestión de riesgos, presupuestos y asignación de recursos.**

☐ **Revise frecuentemente los riesgos de terceros.**

☐ **Supervise 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 directiva.**

☐ **Revise periódicamente su rendimiento en cuanto a lo anterior y considere asesoramiento independiente para la mejora continua.**

CÓMO MANTENERSE INFORMADO

- ☐ **Cuando una persona se incorpore a la junta directiva, garantice que tenga 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. Planee participar en:**
  - Sesiones informativas periódicas sobre los deberes creados por nuevas normativas y leyes.
  - La planificación conjunta de la junta directiva y el comité ejecutivo y visitas a compañeros y líderes de mejores prácticas y ciberseguridad.
  - Sesiones informativas sobre seguridad en el entorno de amenazas.
  - Intercambios a nivel de junta directiva de información sobre gobernanza e informes.

- ☐ **Deje claro a la gerencia que son responsables 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 directiva.**

- ☐ **Compruebe periódicamente con la dirección y otros miembros del personal relevantes los desarrollos relacionados con los retos sistémicos continuos, como las vulnerabilidades de la cadena de suministro, las dependencias comunes y la brecha en el intercambio de información entre juntas directivas sobre la gobernanza del riesgo cibernético.**

EXPLICACIÓN DEL CONTEXTO

- ☐ **Asegúrese de que el personal de todos los niveles reconoce que cada uno tiene responsabilidades importantes para garantizar la resiliencia cibernética de su organización.**

- ☐ **Supervise el papel de la gerencia en la promoción y el mantenimiento de la cultura del riesgo de su organización. Evalúe periódicamente la eficacia de la cultura del riesgo de su organización, teniendo en cuenta el impacto de la cultura en 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

CarnegieEndowment.org

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP
SWIFT
SWIFT INSTITUTE
FS-ISAC
Standard Chartered
CYBER READINESS INSTITUTE
GLOBAL CYBER ALLIANCE
ICBA
INDEPENDENT COMMUNITY BANKERS of AMERICA®