CIBERSEGURIDAD PARA ORGANIZACIONES MÁS PEQUEÑAS

CEO CHECKLIST: CYBERSECURITY LEADERSHIP

GOBERNANZA

- ☐ **Nombre a un CISO (Chief Information Security Officer [Director de seguridad de la información]) si no existe ninguno.**
- ☐ **Establezca y mantenga una política de ciberseguridad en toda la organización que esté basada en el riesgo y sobre las que informan las normas y directrices internacionales, nacionales y del sector.**
- ☐ **Defina las funciones y responsabilidades para todo el personal involucrado en la ciberseguridad. Trabaje con el CISO para identificar las funciones de ciberseguridad y los derechos de acceso adecuados para todos los niveles de personal.**
- ☐ **Establezca o identifique canales de comunicación claros entre cualquier unidad o personal independiente que trate con distintos aspectos de la ciberseguridad.**
- ☐ **Garantice que el CISO tenga una línea de comunicación clara y directa para comunicar las amenazas de forma oportuna con usted y con la junta directiva.**
- ☐ **Mantenga una invitación periódica para que su CISO u otro personal técnico informe a la alta gerencia.**
- ☐ **Compruebe que las políticas, normas y mecanismos de ciberseguridad son uniformes en toda la organización.**

EVALUACIÓN Y GESTIÓN DE RIESGOS

- ☐ **Realice una evaluación de riesgos de ciberseguridad en colaboración con su CISO u otro personal técnico, que debe incluir:**
  - Describir los activos de su organización y sus diversos niveles de dependencia tecnológica.
  - Evaluar la madurez de su organización y los riesgos inherentes asociados a las dependencias tecnológicas de sus activos.
  - Determinar el estado de madurez deseado de su organización.
  - Comprender dónde se encuentran las amenazas de ciberseguridad en la lista de prioridades de riesgo de su organización.
  - Identificar brechas entre su estado actual de ciberseguridad y el estado objetivo deseado.
  - Implementar planes para alcanzar y mantener la madurez.
  - Evalúe y asigne los fondos para invertir en seguridad y subsanar las lagunas existentes.
  - Reevaluar continuamente la madurez, los riesgos y los objetivos de la ciberseguridad de su organización.
  - Considerar tomar medidas de protección, como adquirir un seguro cibernético.
- ☐ **Analice y presente los resultados a las partes interesadas clave y a la junta directiva.**
- ☐ **Planee supervisar los pasos para aumentar la preparación cibernética y controlar el progreso.**

CULTURA ORGANIZATIVA

- ☐ **Discuta con regularidad el riesgo cibernético y la seguridad en el nivel de liderazgo.**
- ☐ **Asegúrese de que la formación sobre ciberseguridad forma parte de la incorporación de todos los empleados y de que todos los empleados firmen documentos que acepten adherirse a las políticas de ciberseguridad de la organización.**
- ☐ **Establezca formación de ciberseguridad recurrente para todo el personal.**
- ☐ **Asegúrese de que la ciberseguridad siempre se tenga en cuenta cuando su organización evalúe los posibles proveedores y comparta datos con terceros.**
- ☐ **Integre una evaluación de la ciberseguridad de una organización al considerar fusiones y adquisiciones.**
- ☐ **Instituya una revisión anual de las políticas de ciberseguridad de la organización.**
- ☐ **Fomente el intercambio voluntario de información sobre amenazas e incidentes de ciberseguridad entre el personal técnico.**

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

CarnegieEndowment.org