excelia

La ciberseguridad ya está en la agenda del CFO

¿Qué es la Directiva NIS2?

La Directiva NIS2 de la Unión Europea refuerza la ciberseguridad y resiliencia digital en sectores estratégicos como energía, salud, transporte, finanzas, telecomunicaciones y más. Su objetivo es claro:

Prevenir ciberataques, proteger la economía y garantizar la continuidad operativa de las organizaciones.

Obligaciones clave:

- Gestionar riesgos de ciberseguridad en toda la organización y sus proveedores.
- La alta dirección, incluidos los CFOs, debe aprobar y supervisar las medidas implementadas.
- Notificación de incidentes graves de ciberseguridad en un plazo máximo de 24 horas.
- Posibles sanciones económicas y penales en caso de incumplimiento.

Impacto en finanzas

Los ciberincidentes no solo afectan a la tecnología: tienen un impacto directo en las finanzas de la empresa. Desde la tesorería hasta los resultados, pasando por la gestión de contratos y proveedores, el CFO se convierte en una figura clave que debe anticipar riesgos, proteger los activos financieros y asegurar que la organización cumpla con la normativa.

Principales efectos sobre el área financiera:

- Costes directos de ciberincidentes: tesorería, provisiones y resultados.
- El CFO es crucial en la gestión de contratos y proveedores sujetos a controles de seguridad.
- Riesgo legal y reputacional por no cumplir la normativa.
- La cobertura de incidentes en varias pólizas de seguros ya depende del cumplimiento de NIS2.
- El cumplimiento de la normativa será evaluado en auditorías, procesos de due diligence y revisiones regulatorias.

La directiva NIS2 de la UE introduce nuevas exigencias en ciberseguridad que afectan directamente a la función financiera. Esta normativa no solo busca proteger sectores esenciales como el financiero, sino también garantizar la continuidad operativa y la confianza en el ecosistema digital.

Aspectos clave para los CFOs:

- **Gestión de riesgos integral:** es fundamental implementar un enfoque de gestión de riesgos que abarque tanto a la organización como a su cadena de suministro.

- **Continuidad del negocio:** un incidente no gestionado implica interrupciones, pérdida de ingresos y posibles litigios con clientes y/o proveedores.

- **Cumplimiento normativo:** los CFOs deben asegurarse de que la empresa cumpla con las nuevas regulaciones, ya que el incumplimiento puede acarrear sanciones económicas y daños reputacionales.

- **Colaboración interdepartamental:** es esencial fomentar la colaboración entre departamentos para garantizar una respuesta eficaz ante incidentes de ciberseguridad.

- **Planificación financiera:** la asignación de recursos para la ciberseguridad debe ser una prioridad en la planificación financiera, considerando tanto los costes directos como los indirectos asociados a posibles incidentes.

El CFO, la NIS2 y la cadena de suministro

La ciberseguridad ya no termina dentro de la empresa: cada proveedor y socio es un punto crítico de riesgo. Los CFOs deben asegurarse de que toda la cadena de suministro cumpla con estándares de NIS2, porque cualquier fallo puede generar pérdidas financieras y legales.

Exigencias para proveedores:

- Evaluaciones de riesgos periódicas.
- Cláusulas de seguridad en contratos.
- Monitorización y auditorías constantes.
- Planes claros de notificación y respuesta ante incidentes.

Tomar acción y securizar la empresa es un proceso que requiere tiempo. Los CFOs deben iniciar las medidas antes de que NIS2 entre en vigor, para garantizar cumplimiento y evitar sanciones.

Consecuencias de no cumplir NIS2

La NIS2 es una normativa que conlleva obligaciones claras y exigentes para las empresas, que ahora tienen la obligación de informar sobre incidentes graves en un plazo máximo de 24 horas. No es opcional: requiere planificación, supervisión continua y adaptación de procesos para proteger tanto los activos como la continuidad del negocio.

Cómo excelia te ayuda a los CFOs

Excelia es especialista en ciberseguridad, con un equipo altamente experimentado y certificado, preparado para adaptarse a las necesidades y desafíos de cada organización, ofreciendo soluciones prácticas que protegen la operación y la reputación de su empresa.

- Evaluaciones NIS2 con enfoque en riesgo económico.
- Estrategias de gestión de proveedores y contratos.
- Planes de acción prácticos para cumplimiento y reducción de riesgos legales.
- Soporte continuo para proteger estabilidad financiera y reputación corporativa.

La NIS2 no espera.

La ciberseguridad es un proceso: comienza ahora y conviértela en ventaja competitiva.

Habla hoy con un especialista de excelia y asegura el futuro financiero y legal de tu empresa.

info@excelia.com · +34 91 708 05 50

Paseo del Club Deportivo, 1 Edificio 11 - 1ª planta - Parque empresarial La Finca 28223 Pozuelo de Alarcón - Madrid