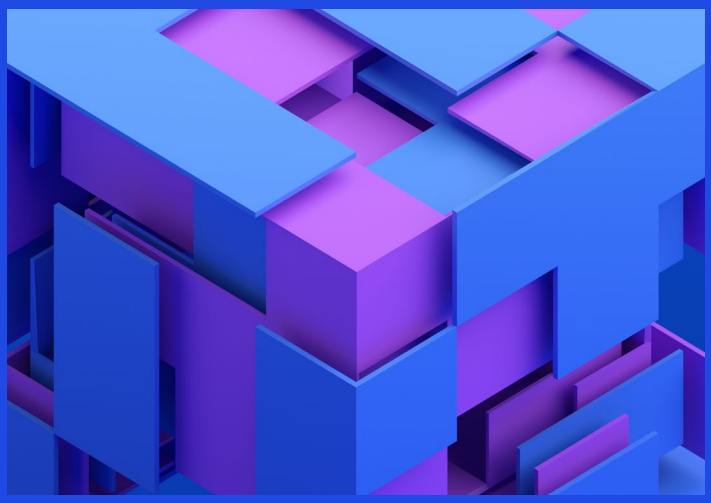
Cumpliendo con las buenas prácticas

Código de Buen Gobierno de la Ciberseguridad



Riesgo de ciberataques

El incremento de las amenazas en el ciberespacio y de la superficie de ataque en las organizaciones han generado un aumento notable de los ciberataques, cada vez con mayor regularidad e impacto.

Muchas organizaciones han tomado la decisión de buscar adecuarse a estándares de seguridad de la información reconocidos en el mercado (ISO 27001, NIST CSF, etc.) para hacer frente a este reto y, adicionalmente, cumplir con las diferentes regulaciones en seguridad de la información en las que se ven desbordadas.

Recomendaciones de ciberseguridad

El 13 de Julio de 2023, la Comisión Nacional del Mercado de Valores (CNMV) publicó en nota de prensa el Código de Buen Gobierno de la Ciberseguridad, elaborado por el seno del Foro Nacional de Ciberseguridad donde, a su vez, también ha participado la CNMV.

El objetivo del Código es proponer, a cualquier tipo de organización —independientemente de su tamaño, sector, actividad o incluso grado de madurez de su ciberseguridad— las prácticas dirigidas a sustentar el modelo de buen gobierno en esta área, con el objetivo de facilitar la gestión de la seguridad de las redes y los sistemas de información y, a su vez, contribuir a mejorar el proceso de toma de decisiones por parte de los órganos de gobierno de las organizaciones y, en especial, por el órgano de administración.

El seguimiento de estas recomendaciones podría interpretarse como una señal de madurez de ciberseguridad y sirve de guía para el cumplimiento de las obligaciones que pudieran requerir los distintos organismos de supervisión de las compañías.

El Código plantea un enfoque de 13 principios definidos como el conjunto de valores, experiencias y normas que orientan y regulan el buen gobierno de la ciberseguridad. El 1º es el de la proporcionalidad, donde las recomendaciones se aplicarían a las organizaciones teniendo en cuenta su propia complejidad, tamaño, riesgos a los que estén sometidas, recursos con los que cuenten y el resto de circunstancias aplicables.

Los 12 principios restantes desarrollan 25 recomendaciones para realizar una adecuada gobernanza de la ciberseguridad, y están agrupados en los siguientes tres grandes bloques:

Estrategia y organización

Detalla los principios más importantes sobre los que los órganos de gobierno deben construir la estrategia y organización de la ciberseguridad.

Gestión

Detalla las medidas y decisiones a realizar para garantizar que exista una madurez de ciberseguridad adecuada, que han de ser aplicados por la dirección de la organización desde la unidad de ciberseguridad.

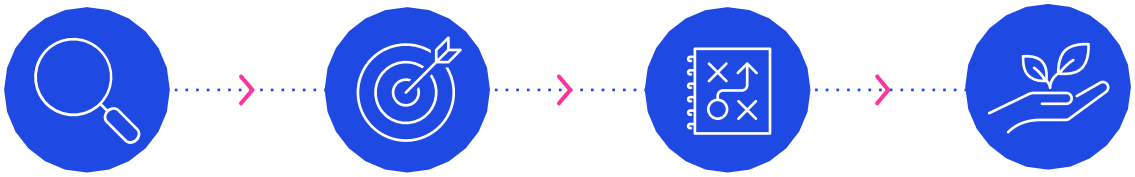
Supervisión

Detalla los elementos y requerimientos para la validación por parte de los órganos de gobierno, y concreta cómo la dirección de la organización y la unidad de ciberseguridad deben realizar una supervisión continua.

> **Aunque el Código no es un documento de la CNMV ni constituye una recomendación de la CNMV a las sociedades cotizadas, dado el interés que puede tener para ellas y el creciente nivel de riesgo de ciberataques, la CNMV difunde este nuevo código y contribuye a su conocimiento entre las cotizadas y entidades supervisadas**
>
> CNMV, en nota de prensa del 13 de julio de 2023

Nuestra solución

KPMG ofrecemos una solución que permitirá a las organizaciones lograr adecuarse al Código, considerando el uso del principio de proporcionalidad. El enfoque de la solución consta de tres fases que ayudarán a tener un entendimiento completo de la situación actual de la compañía frente al cumplimiento de las recomendaciones del Código. Y, a su vez, definir la situación deseada y los planes de acción para alcanzarlo. Además, desde KPMG proponemos una 4ª fase para apoyar a la organización en la implantación de cada uno de los proyectos planificados para lograr el cumplimiento del código de manera exitosa.



Análisis de situación actual (As-Is)

Conocer el estado actual en materia de gobierno de la ciberseguridad.

Definición de situación deseada (To-Be)

Definir el nivel de madurez deseado de la organización en materia de gobierno de la seguridad.

Gap-Assessment y definición de roadmap

Analizar la diferencia entre el estado actual y deseado, definir proyectos y trazar una hoja de ruta.

Soporte en la ejecución

Acompañar en cada una de las iniciativas planificadas con apoyo de equipos especializados.

Beneficios que le aportará nuestra solución

1. Alinear

Y cotejar los estándares y regulaciones aplicables.

2. Identificar

Brechas actuales en el cumplimiento y la gestión de riesgos.

3. Evaluar

La magnitud de las vulnerabilidades.

4. Valorar

El nivel de madurez de la ciberseguridad en la organización.

5. Priorizar

Áreas clave para un plan de acción de gestión exitoso.

6. Garantizar

La ejecución de los planes de acción de manera exitosa.

¿Por qué KPMG?

Global

Más de 265.000 profesionales multidisciplinares en 143 países, siendo 9.300 expertos en ciberseguridad y 45.000 basados en riesgos.

Diferencial

Combinamos una amplia experiencia, con profundos conocimientos del negocio y sector, con profesionales a los que les apasiona ayudar a proteger y fomentar la confianza entre las partes interesadas.

Comprometida

Las relaciones con nuestros clientes se basan en la confianza mutua y el compromiso a largo plazo para proporcionar estrategias eficaces y eficientes.

Contactos

Javier Aznar
Socio de Ciberseguridad
KPMG en España
T: +34 699 350 029
E: jaznar@kpmg.es

Sergio Gómez
Socio de Ciberseguridad
KPMG en España
T: +34 616 912 664
E: sergiogomezrodriguez@kpmg.es

kpmg.es