Raúl Rubio, Josefina García Pedroviejo y Marisa Delgado

Publicado el Código de Buen Gobierno de la Ciberseguridad

El Foro Nacional de Ciberseguridad ha hecho público, mediante su difusión en la página web de la Comisión Nacional de los Mercados de Valores ("**CNMV**"), el Código de Buen Gobierno de la Ciberseguridad (el "**Código**").

1. Alcance y obligatoriedad

El Código es un documento de gran interés, pese a no ser un documento elaborado íntegramente por la CNMV (aunque sí ha participado en su redacción) y dirigido a sociedades cotizadas y entidades reguladas. El Código ofrece recomendaciones de alcance general que, pese a no tener carácter obligatorio, pueden orientar a cualquier organización que pretenda realizar una adecuada gobernanza de la ciberseguridad, con independencia de su tamaño, sector o actividad, sirviéndose de ellas incluso como guía para cumplir con las obligaciones de información que puedan requerirle los organismos de supervisión.

En este sentido, aunque no define un nuevo estándar de controles que deban implementarse para alcanzar un determinado nivel de cumplimiento, el Código puede (i) facilitar la gestión de la seguridad de las redes y los sistemas de información; y (ii) contribuir a mejorar el proceso de toma de decisiones en este ámbito por parte de las organizaciones y, en especial, por su órgano de administración.

2. Estructura y contenido

Los principios que señala el Código (los "**Principios**") se desarrollan en recomendaciones concretas para para ayudar a las entidades, con un enfoque práctico, a implantarlos, debiendo aplicarse de manera proporcionada, en función de la complejidad de la entidad y sus circunstancias.

Para una mejor comprensión de los mismos, los Principios y sus recomendaciones se han organizado en tres grandes bloques, que indicamos a continuación:

A. Estrategia y organización:

(i) Alineamiento estratégico y visión de futuro: la ciberseguridad deberá estar alineada con la misión y visión de la organización. Para ello:

- Se reconocerán formalmente en un documento público los principios y compromisos de la ciberseguridad.
- La ciberseguridad será uno de los ámbitos explícitos de la política de control y gestión de riesgos de la organización.
- La organización definirá planes a corto, medio y largo plazo que aseguren la visión de futuro y mejora continua de la ciberseguridad.
- Se tomarán decisiones en materia de ciberseguridad en función del riesgo real de la materialización de las amenazas sobre la organización, implantando un sistema de monitorización de la eficiencia y el cumplimiento de los objetivos definidos.

(ii) Responsabilidad y organización: dada la complejidad y transversalidad de la ciberseguridad, se requiere de un adecuado liderazgo y una estructura integrada por profesionales con formación y experiencia adecuados. Así:

- La organización aspirará a que, dentro del órgano de administración, haya, al menos, un miembro con experiencia en gestión de ciberseguridad que apoye y valide los objetivos con anterioridad a su aprobación por el equipo directivo.
- Se creará una unidad que asuma la función de definición, impulso y control de la ciberseguridad, cuyo máximo responsable será el director de ciberseguridad, director de seguridad de la información o Chief Information Security Officer (el "**CISO**").
- Existirá un comité de ciberseguridad formado por, además del CISO, las áreas competentes para adoptar cualquier decisión en materia de seguridad de la información que pueda afectar sustancialmente a la actividad de la organización.
- Las organizaciones deberán tener en cuenta la ciberseguridad al menos en uno de sus comités de crisis.
- El órgano de administración asignará la supervisión ejecutiva de la gestión de la ciberseguridad a alguna de sus comisiones especializadas.

(iii) Ética y cumplimiento: el gobierno de la ciberseguridad deberá buscar no sólo el cumplimiento de la normativa aplicable, sino también las buenas prácticas de seguridad y el uso ético de los recursos de la organización En este sentido, el órgano de administración tendrá en cuenta las implicaciones de dichas buenas prácticas en la gestión de los riesgos en materia de ciberseguridad en la organización, en los mercados en los que opera y en su relación con los grupos de interés.

B. Gestión:

(i) Modelo de gestión: dado que la ciberseguridad es una materia transversal, la organización se apoyará en reconocidos estándares adecuados a sus necesidades, para un mejor seguimiento de la evolución de su madurez.

(ii) Dotación de recursos: el órgano de administración se asegurará de que la unidad responsable de la gestión de la ciberseguridad, así como otras unidades con responsabilidad en la consecución de los objetivos establecidos, disponen de suficientes capacidades materiales y humanas para poder llevar a cabo sus funciones.

(iii) Gestión de incidentes y resiliencia operativa: la organización deberá desarrollar capacidades para contener o recuperarse de los ciberincidentes, para lo que:

- Se definirá cuándo un incidente tiene la consideración de significativo en función del impacto, del tipo de organización, su sector y las regulaciones a las que pudiera estar sometida en los mercados en los que opere.
- Se identificarán los grupos operativos encargados de la gestión de incidentes para minimizar el impacto en el negocio y para asegurar el cumplimiento regulatorio y la adecuada comunicación interna o externa.
- Se dispondrá de capacidades que permitan asegurar la continuidad de las operaciones y la recuperación completa de los servicios en un plazo adecuado de tiempo, que se determinará en el plan de continuidad de negocio.

(iv) Formación y concienciación: se fomentarán la formación, concienciación y cultura de ciberseguridad en toda la organización, para capacitar al personal acerca de los hábitos y prácticas recomendables para prevenir y mitigar riesgos.

(v) Innovación y mejora continua: la gestión de la ciberseguridad estará en constante mejora y evolución para garantizar una defensa adecuada ante las ciberamenazas.

C. Supervisión:

(i) Ciberinteligencia: la organización deberá apoyarse en la ciberinteligencia como base de la preparación en la gestión de la ciberamenazas. En particular, el comité de ciberseguridad informará a la dirección y al órgano de administración de las ciberamenazas que puedan existir.

(ii) Informe periódico: el reporte periódico de la situación de la ciberseguridad de una organización a los órganos de gobierno de la misma es una buena práctica, por lo que se recomienda que el órgano de administración incluyendo este tema en el orden del día de sus reuniones o en las de sus comisiones especializadas correspondientes donde aplique, al menos dos veces al año.

El Código establece en contenido recomendado de ese informe periódico y, adicionalmente, se señala que cuando en las reuniones del órgano de administración figure algún tema que pueda afectar a la ciberseguridad, se tendrán que tratar las repercusiones que tenga la ciberseguridad en el mismo.

(iii) Continuidad: dado que la ciberseguridad es parte de la estrategia de continuidad de la organización, se recomienda realizar pruebas periódicas completas que pongan a prueba los mecanismos de resiliencia de la organización como parte de los planes de ciberseguridad.

(iv) Gestión de riesgos: la correcta gestión, evaluación y comunicación del riesgo de ciberseguridad es un elemento clave en la gestión del riesgo, por lo que se deberán realizar evaluaciones independientes respecto a la unidad de ciberseguridad, al menos una vez al año, que permitan valorar la correcta gestión de los riesgos de ciberseguridad de los procesos críticos de la organización, incluida la cadena de suministro.

3. Conclusión

Pese a no ser un documento vinculante, el Código supone una orientación muy útil para las organizaciones, ya que integra en un único documento los principios maestros para gobernar la ciberseguridad, proporcionando a su órgano de administración y su equipo directivo una visión integrada de las responsabilidades de supervisión y reporte de la ciberseguridad y ayudando a concienciarles acerca de su rol y responsabilidad en esta materia.

CONTACTOS

Raúl Rubio
Socio
rrubio@perezllorca.com
T. +34 91 353 45 59

Josefina García Pedroviejo
Socia
jgarciapedroviejo@perezllorca.com
T. +34 91 389 01 09