

# CÓDIGO DE BUEN GOBIERNO DE LA CIBERSEGURIDAD



2023

Catálogo de publicaciones de la Administración General del Estado

<https://cpage.mpr.gob.es>

Edita:



© Autor y editor,

NIPO (edición impresa): 089-23-014-4

NIPO (edición on-line): 089-23-013-9

DL: M-29298-2023

Fecha de edición: Septiembre 2023

Imprime: MASQUELIBROS S.L.

# CÓDIGO DE BUEN GOBIERNO DE LA CIBERSEGURIDAD

Los expertos participantes en los Grupos de Trabajo lo son a título personal y no a título institucional. Por lo tanto, sus opiniones y recomendaciones no representan ni comprometen a las instituciones a las que pertenecen.

El resultado de los trabajos es producto de un ejercicio de reflexión colectivo, si bien, no tiene por qué representar la opinión individual de todos los participantes, quienes no necesariamente comparten todas las conclusiones o propuestas.

# AGRADECIMIENTOS

## **Coordinador sociedad civil:**

Gianluca D'Antonio (Presidente de ISMS Forum)

## **Coordinador institucional:**

Andrés J. Ruiz Vázquez (Departamento de Seguridad Nacional)

## **Autores y colaboradores:**

Raúl Amigorena Eguiluz

Roberto Baratta Martínez

Mariano J. Benito Gómez

Juan Fco. Cornago Baratech

Ángel Domínguez Fernández-Burgos

Javier García Quintela

Daniel Largacha Lamela

Idoia Mateo Murillo

Francisco del Olmo Fons

Luis Paredes Hernández

Julia Perea Velasco

Olga Ramírez Sánchez

Antonio Ramos García

Jesús Sánchez López

Alejandro Viana Lara

María Elisa Vivancos Cerezo

# ÍNDICE

1. INTRODUCCIÓN	7
2. OBJETIVO	9
3. ALCANCE	10
4. ESTRUCTURA	11
5. PRINCIPIOS Y RECOMENDACIONES	12
Principio 1: Proporcionalidad	12
5.1 Estrategia y organización	12
Principio 2: Alineamiento estratégico y visión de futuro	12
Principio 3: Responsabilidad y organización	13
Principio 4: Ética y cumplimiento	14
5.2 Gestión	14
Principio 5: Modelo de gestión	14
Principio 6: Dotación de recursos	15
Principio 7: Gestión de incidentes y resiliencia	15
Principio 8: Formación y concienciación	16
Principio 9: Innovación y mejora continua	16
5.3 Supervisión	16
Principio 10: Ciberinteligencia	16
Principio 11: Informe periódico	17
Principio 12: Continuidad	18
Principio 13: Gestión del riesgo	18
6. GLOSARIO	19



---

## 1. INTRODUCCIÓN

---

En abril del año 2019, el Consejo de Seguridad Nacional aprobó la **Estrategia Nacional de Ciberseguridad** en cuyo texto se destaca la cooperación público-privada como un elemento clave en la consecución de los objetivos marcados en ciberseguridad. Así mismo la Estrategia prevé el Foro Nacional de Ciberseguridad, espacio encuadrado en el Sistema de Seguridad Nacional e integrado por representantes de la sociedad civil, expertos independientes, sector privado, instituciones académicas, asociaciones y organismos sin ánimo de lucro, entre otros, a fin de potenciar y crear sinergias público-privadas.

La ciberseguridad se ha convertido en el pilar estratégico sobre el que poder asentar la revolución digital que han experimentado todos los sectores de la sociedad, incluyendo Administraciones públicas, empresas y ciudadanía. Solo sobre la base de la ciberseguridad es posible continuar avanzando de forma segura en dicha transformación.

El marco regulatorio en materia de ciberseguridad ha evolucionado en los últimos años, tanto a nivel nacional como europeo, con el objetivo de mejorar la ciberseguridad de nuevos sectores cuyas obligaciones se han visto incrementadas. Gran parte de las novedades y cambios normativos en esta materia han venido propiciados por los cada vez más frecuentes y costosos efectos negativos soportados por las organizaciones, bien a causa de ciberataques, bien debido a la inadecuada gestión interna de los riesgos en ciberseguridad.

A nivel nacional, el nuevo **Esquema Nacional de Ciberseguridad**, recogido en el Real Decreto 311/2022<sup>1</sup>, menciona explícitamente la necesidad de seguir una dinámica de mejora continua y adaptativa de la ciberseguridad, que es parte cada vez más relevante del modelo de **sostenibilidad del país**, debido al impacto que puede generar, no solamente en la propia organización, sino también en sus empleados, proveedores, clientes y grupos de interés que puedan verse afectados por las actividades de la organización. Así mismo, el **Real Decreto 43/2021**<sup>2</sup> exige el nombramiento de un **responsable de la seguridad de la información** en las organizaciones que reporte directamente a la alta dirección y

---

<sup>1</sup> Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

<sup>2</sup> Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

que mantenga la debida independencia respecto de los responsables de las redes y los sistemas de información.

A nivel europeo, la Directiva UE 2022/2555 conocida como **NIS 2**, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, incluye medidas específicas de gobernanza de la ciberseguridad. Entre ellas, establece que los órganos de dirección de las organizaciones **aprueben las medidas para la gestión de riesgos de ciberseguridad y supervisen su puesta en práctica.**

El **Foro Nacional de Ciberseguridad**, en reunión plenaria el 8 de octubre de 2021, procedió a la aprobación de las líneas de trabajo para el periodo 2021–2022 por cada uno de los grupos de trabajo que lo conforman. Concretamente, la **incorporación de la ciberseguridad al buen gobierno corporativo de las organizaciones** fue la línea de trabajo aprobada para desarrollar por parte del **Grupo de Trabajo número 1 de Cultura de Ciberseguridad.**

Desde los **órganos de administración se ejerce el liderazgo de las organizaciones** y se lleva a cabo el seguimiento de su correcto funcionamiento, incluyendo la supervisión de la gestión y control de los **riesgos corporativos**, entre los que cada vez con mayor frecuencia e intensidad se incluyen los de carácter cibernético.

En este sentido y siguiendo la línea aprobada en el Foro Nacional de Ciberseguridad, el Grupo de Trabajo 1 dio comienzo a la labor de desarrollar un trabajo de **recopilación de los principios fundamentales y recomendaciones asociadas a los mismos, que los órganos de gobierno de una organización**, con independencia de su tamaño o sector, pudieran seguir para realizar una adecuada gobernanza de su ciberseguridad.

El presente Código de buen gobierno es el fruto final del trabajo del grupo referido, compuesto por expertos en materia de ciberseguridad, así como del análisis de distintas normativas y estándares existentes, examinadas desde una perspectiva práctica y actual, para la mejora del buen gobierno corporativo en materia de ciberseguridad.



---

## 2. OBJETIVO

---

Los nuevos retos derivados de la materialización de amenazas en el ciberespacio, han generado un notable incremento de los ciberataques, tanto en volumen como en frecuencia y sofisticación. Hacer frente a los nuevos retos de ciberseguridad requiere de políticas de revisión y mejora continuada, así como de la optimización de los controles y medidas de ciberseguridad, aplicadas tanto a la protección del valor y funcionamiento de las organizaciones, como a la protección de los datos de los ciudadanos en poder de aquellas.

El presente Código de buen gobierno no es una definición de un nuevo estándar de controles ni un manual de implantación. Por el contrario, el objetivo del Código es proponer a las organizaciones las prácticas dirigidas a sustentar el **modelo de buen gobierno de la ciberseguridad** que facilite la gestión de la seguridad de las redes y los sistemas de información y contribuya a mejorar el proceso de toma de decisiones en este ámbito por parte de los órganos de gobierno de las organizaciones y, en especial, por el órgano de administración.

Teniendo en cuenta este objetivo general, a continuación, se establecen una serie de objetivos específicos:

- **Objetivo I. Integrar en un único código de buen gobierno los principios maestros para gobernar la ciberseguridad.**

Agrupar, de forma concreta y sucinta, las principales actividades que una organización debe realizar para gobernar de forma adecuada y madura la ciberseguridad corporativa.

Disponer de un enfoque común de los principios maestros, medidas de seguridad y procedimientos de auditoría, así como de elementos que permitan llevar a cabo el seguimiento del cumplimiento de estándares actuales o futuros del ámbito de la ciberseguridad que puedan ser implantados.

- **Objetivo II. Desarrollar un documento de ayuda para el órgano de administración de la organización y su equipo directivo.**

Identificar las principales materias relacionadas con la gestión y los riesgos en materia de ciberseguridad que deben ser tratadas por una organización, así como, las sesiones en las que dichas cuestiones deban abordarse y su periodicidad.

- **Objetivo III. Formar y concienciar a los órganos de gobierno y a los equipos directivos de las organizaciones sobre su rol y responsabilidad en materia de ciberseguridad.**

Servir como referencia para que los administradores de las organizaciones y sus órganos de gobierno puedan conocer sus responsabilidades y funciones en la correcta gestión de la ciberseguridad corporativa.

- **Objetivo IV. Proporcionar una visión integrada de las responsabilidades de supervisión y reporte de la ciberseguridad.**

Definir de forma explícita las responsabilidades de supervisión y reporte en materia de ciberseguridad, así como proporcionar orientación sobre qué eventos o incidentes significativos deben reportarse a la dirección, a los órganos de gobierno o a los organismos supervisores.

---

### 3. ALCANCE

---

El presente Código de buen gobierno de la ciberseguridad **ofrece recomendaciones de alcance general**, organizadas en principios para que pueda ser utilizado por cualquier organización que persiga realizar una adecuada gobernanza de la ciberseguridad, con independencia de su tamaño, sector, actividad o incluso grado de madurez en la materia.

La efectiva incorporación de los principios y recomendaciones recogidos en el presente Código por parte de una organización podría interpretarse de hecho como una **señal de madurez en ciberseguridad** y contribuir tanto a una mejor gestión del riesgo como a la protección de sus objetivos y los de aquellos grupos de interés que puedan verse afectados por las actividades de la organización.

Asimismo, este Código **podría ser utilizado por parte de la organización como guía para el cumplimiento de las obligaciones** de información que pudieran requerirle los distintos organismos de supervisión.

---

## 4. ESTRUCTURA

---

El Código plantea un **enfoque de principios** definidos como el conjunto de valores, experiencias y normas que orientan y regulan el buen gobierno de la ciberseguridad.

Estos principios podrían considerarse **como el soporte de la visión, misión y objetivos estratégicos** de la gestión del riesgo asociado a la ciberseguridad. Su seguimiento tendría el objetivo de mejorar el proceso de toma de decisiones por parte de los órganos responsables de cualquier organización, con atención al principio de proporcionalidad y con independencia de su tamaño o actividad.

**Los principios se desarrollan en recomendaciones** que son fundamentales a la hora de implantarlos.

Se han organizado en 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. Estos principios están relacionados, de manera directa, con la gestión de la ciberseguridad.

- **Gestión**

Conjunto de actividades, controles y decisiones fundamentales que deben las organizaciones para garantizar que disponen de una madurez adecuada en ciberseguridad, incluyendo la prevención, detección, respuesta y recuperación ante incidentes. Estos principios deben ser aplicados por la dirección de la organización desde la unidad de ciberseguridad o seguridad de la información.

- **Supervisión**

Detalla los elementos mínimos que deben validar los órganos de gobierno de la organización, así como los requerimientos básicos que debe cubrir la información requerida para poder realizar esta validación. Concreta cómo debería realizarse la supervisión de forma continua por parte de la dirección de las organizaciones y la unidad de ciberseguridad o seguridad de la información.

---

## 5. PRINCIPIOS Y RECOMENDACIONES

---

### Principio 1: Proporcionalidad

Las recomendaciones contenidas en este Código se aplicarían a las organizaciones bajo el principio de proporcionalidad, teniendo en cuenta su propia complejidad, tamaño, riesgos a los que estén sometidas, recursos con los que cuenten y el resto de circunstancias aplicables.

#### 5.1 Estrategia y organización

### Principio 2: Alineamiento estratégico y visión de futuro

La **ciberseguridad**, como disciplina que ayuda a las organizaciones a alcanzar sus objetivos, **debe estar alineada con la misión y visión de la organización**.

**Recomendación 1:** El órgano de administración reconocerá formalmente, en un documento visible públicamente, los principios y compromisos de la ciberseguridad como elemento fundamental para proteger los activos del negocio, con el fin de lograr sus objetivos y cumplir con su misión.

**Recomendación 2:** Uno de los ámbitos explícitos de la política de control y gestión de riesgos de la organización será la ciberseguridad.

**Recomendación 3:** La organización, teniendo en cuenta las necesidades operativas del negocio y los riesgos que puedan afectar a la consecución de sus objetivos, definirá planes a corto, medio y largo plazo que aseguren la visión de futuro y mejora continua de la ciberseguridad, permitiendo reducir su exposición al riesgo dentro de los niveles de tolerancia definidos.

**Recomendación 4:** Se tomarán decisiones en materia de ciberseguridad en función del riesgo real de la materialización de las amenazas sobre la organización. Se implantará, de igual manera, un sistema de monitorización de la eficiencia y el cumplimiento de los objetivos de seguridad definidos.

### Principio 3: Responsabilidad y organización

La ciberseguridad es una disciplina compleja y transversal que afecta a todas las actividades de una organización. Es por esto que requiere de un adecuado liderazgo y una estructura que, para ser implantada y gestionada adecuadamente, a su vez debe estar integrada por profesionales con formación y experiencia adecuados.

**Recomendación 5:** 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.

**Recomendación 6:** La organización dispondrá de una unidad que asuma la función de definición, impulso y control de la ciberseguridad y que participe en la toma de decisiones y estrategias en este ámbito. Del mismo modo deberá asegurar el reporte adecuado, y a los niveles oportunos, de los riesgos relacionados con la ciberseguridad, así como de los mecanismos de mitigación y control de los mismos que sean necesarios.

Esta unidad contará con suficientes capacidades y recursos, materiales y humanos, para la consecución de sus objetivos, y dependerá funcionalmente del órgano de administración, de alguna de sus comisiones especializadas o de cualquier otro órgano o miembro de la alta dirección de la organización, siempre que se mantenga la debida independencia respecto de los responsables de sistemas de redes y de información.

**Recomendación 7:** El máximo responsable de esta unidad será el director de ciberseguridad, director de seguridad de la información o Chief Information Security Officer (en adelante CISO). Esta figura será una persona con el conocimiento, experiencia y competencias adecuadas para desarrollar la función y contará con la suficiente capacidad de decisión e influencia en la organización.

**Recomendación 8:** Existirá un comité de ciberseguridad, constituido formalmente, en el que estarán representado, además del CISO, un número adecuado de áreas de la organización para adoptar cualquier resolución, con relevancia en materia de seguridad de la información, que pueda afectar sustancialmente a la actividad de la organización.

**Recomendación 9:** Las organizaciones, en función de su complejidad y exposición al riesgo cibernético, deberán tener en cuenta la ciberseguridad al menos en uno de sus comités de crisis.

**Recomendación 10:** El órgano de administración asignará la supervisión ejecutiva de la gestión de la ciberseguridad a alguna de sus comisiones especializadas (por ejemplo, la comisión de riesgos, la comisión de auditoría ...).

#### Principio 4: Ética y cumplimiento

El gobierno de la ciberseguridad debe incluir 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**.

**Recomendación 11:** El órgano de administración comprenderá las implicaciones de las buenas prácticas, entre otras, en la gestión de los riesgos en materia de ciberseguridad, tanto en su organización, como en cada uno de los mercados en los que opera y en su relación con los distintos grupos de interés.

## 5.2 Gestión

#### Principio 5: Modelo de gestión

**La ciberseguridad es una materia transversal** a toda la organización y a sus procesos de negocio. La gestión de la ciberseguridad debe estar guiada por las mejores prácticas y ser las adecuadas para cada organización.

**Recomendación 12:** La organización se apoyará en reconocidos estándares, nacionales, europeos o internacionales, adecuados a sus necesidades, para un mejor seguimiento de la evolución de su madurez.

## Principio 6: Dotación de recursos

Las organizaciones deben tener en cuenta que la función de la **ciberseguridad requiere una constante y adecuada dotación de recursos** asignados a su mantenimiento y mejora.

**Recomendación 13:** 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 las funciones asignadas de forma efectiva y eficiente.

## Principio 7: Gestión de incidentes y resiliencia

Una de las finalidades perseguidas por la ciberseguridad es asegurar la continuidad de la capacidad operativa para los fines de la organización y la de los grupos de interés que puedan verse afectados por sus actividades. Esto se conoce como **resiliencia operativa** y por ello se deben desarrollar capacidades para contener o recuperarse de los ciberincidentes.

**Recomendación 14:** 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.

**Recomendación 15:** Se identificarán los grupos operativos encargados de su gestión (tanto a nivel técnico y táctico, como estratégico) para minimizar el impacto en el negocio y para asegurar el cumplimiento regulatorio y la adecuada comunicación interna o externa.

**Recomendación 16:** Se dispondrá de capacidades que permitan a la organización ser resiliente para 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.

## Principio 8: Formación y concienciación

Todo el personal de la organización necesita poseer suficientes conocimientos en materia de ciberseguridad para enfrentarse y mitigar el riesgo al que esté expuesto<sup>3</sup>.

**Recomendación 17:** La dirección y el órgano de administración fomentarán la formación, concienciación y cultura de ciberseguridad en toda la organización con el objetivo de capacitar a su personal acerca de los hábitos y prácticas recomendables para prevenir y mitigar riesgos en el ámbito de la ciberseguridad.

## Principio 9: Innovación y mejora continua

La ciberseguridad requiere adaptarse y mejorar en consonancia con los nuevos y constantes avances de la tecnología y de las ciberamenazas.

**Recomendación 18:** La gestión de la ciberseguridad estará en constante mejora y evolución para garantizar una defensa adecuada ante las amenazas.

## 5.3 Supervisión

## Principio 10: Ciberinteligencia

La anticipación es un elemento clave en la protección contra cualquier riesgo no sólo de la propia organización, sino también de los grupos de interés que puedan verse afectados por sus actividades, por lo que la organización necesita apoyarse en la ciberinteligencia como base de la preparación en la gestión de la ciberamenazas.

---

<sup>3</sup> Las personas son el principal activo que disponen las organizaciones para la adecuada protección en materia de ciberseguridad. A la vez, los principales riesgos en esta materia suelen provenir de incidentes que, de forma activa o pasiva, son generados por las personas.



**Recomendación 19:** El comité de ciberseguridad informará a la dirección y al órgano de administración de las ciberamenazas que podrían afectar a los objetivos de la organización. Para ello, se tendrán en cuenta, al menos, los principales actores y las principales y más recientes ciberamenazas, considerando su potencial impacto sobre las operaciones de la organización.

## Principio 11: Informe periódico

Constituye una buena práctica de gobierno según las normas internacionales, y en algunos casos una obligación, **el reporte periódico de la situación de la ciberseguridad de la organización a los órganos de gobierno de la misma.**

**Recomendación 20:** El órgano de administración realizará un seguimiento regular de la ciberseguridad, incluyendo este tema en el orden del día de sus reuniones o en las de sus comisiones especializadas correspondientes donde aplique (auditoría, riesgos, sostenibilidad u otras comisiones específicas para el tratamiento del riesgo de ciberseguridad), para lo que requerirá informes periódicos de la gestión de ciberseguridad al responsable ejecutivo (director de seguridad de la información o CISO). Este reporte deberá realizarse periódicamente. Se considera una buena práctica su realización al menos dos veces al año.

**Recomendación 21:** El informe periódico debe contener al menos el estado de la ciberseguridad, la evolución del grado de madurez y del ciberriesgo, la evolución de las amenazas, la asignación de los recursos destinados a la seguridad de las redes y los sistemas de información, los incidentes significativos gestionados si los hubiera, el estado de la seguridad de las operaciones de la cadena de suministro que dependan de terceros, así como cualquier resolución con relevancia en materia de ciberseguridad adoptada por el equipo directivo que pueda afectar sustancialmente a la actividad de la organización. El director de seguridad de la información o CISO también deberá reportar, en su caso, cualquier obstáculo o impedimento que pudiera restringir el adecuado desempeño de su actividad.

**Recomendación 22:** Cuando en el orden del día de 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 referido tema como, por ejemplo: grandes iniciativas de transformación digital, implementación de nuevas tecnologías y grandes inversiones en activos tecnológicos, fusiones y adquisiciones, expansión de instalaciones o grandes actualizaciones.

## Principio 12: Continuidad

**La ciberseguridad es parte de la estrategia de continuidad de la organización** y su ensayo es esencial para una correcta preparación ante los ciberincidentes.

**Recomendación 23:** El órgano de administración requerirá el desarrollo de pruebas periódicas completas que pongan a prueba los mecanismos de resiliencia de la organización como parte de los planes de ciberseguridad.

En este contexto:

- Deben realizarse pruebas del plan de continuidad de negocio, así como simulaciones y ejercicios de preparación de los comités de gestión de crisis.
- En general, las compañías deben ejecutar de forma sistemática simulacros y pruebas efectivas de las distintas medidas de protección, respuesta y recuperación.
- Estos ejercicios han de implicar a toda la organización, con especial atención a los procesos críticos de la compañía, y deben involucrar también a la cadena de suministro.

**Recomendación 24:** El órgano de administración se asegurará de que la dirección apoye la creación, implementación, prueba y mejora continua de los mecanismos de ciberresiliencia.

## Principio 13: Gestión del riesgo

La correcta gestión, evaluación y comunicación del riesgo de ciberseguridad es un **elemento clave en la gestión del riesgo corporativo para toda organización**.

**Recomendación 25:** Se deberán realizar evaluaciones independientes respecto a la unidad de ciberseguridad, al menos una vez al año, que permitan al órgano de administración obtener un punto de vista adicional y complementario del correcto estado del programa de gestión de los riesgos de ciberseguridad de los procesos críticos de la organización, incluyendo a la cadena de suministro.

---

## 6. GLOSARIO

---

A continuación, se incluye un glosario para facilitar la comprensión de los conceptos presentados en este Código:

**Activo de información:** es cualquier información o sistema relacionado con el tratamiento de esta que tenga valor para la organización. Pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, equipamiento auxiliar o instalaciones. Esta información es susceptible de ser atacada, deliberada o accidentalmente, con consecuencias para la organización.

**Ciberamenaza:** amenaza a los sistemas y servicios presentes en el ciberespacio o alcanzables a través de este.

**Ciberataque:** intento deliberado de un ciberdelincuente de obtener acceso a un sistema informático sin autorización sirviéndose de diferentes técnicas y vulnerabilidades para la realización de actividades con fines maliciosos, como el robo de información, extorsión del propietario o simplemente daños al sistema.

**Ciberinteligencia:** es la disciplina que permite que la información procesada sobre la intención, la oportunidad y la capacidad que poseen los actores maliciosos sirva para anticipar la ciberseguridad más adecuada.

**Ciberseguridad:** la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos. Se materializa en la combinación de personas, políticas, procesos y tecnologías empleadas por una organización para proteger sus activos contra las ciberamenazas con el fin de lograr sus objetivos y cumplir con su misión.

**Organización:** en este término se engloba no solamente la propia sociedad, sino también a todas las entidades de su grupo.

**Riesgo cibernético o ciberriesgo:** circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Si esta circunstancia desfavorable acontece a la vez que existe una vulnerabilidad o debilidad de los sistemas puede derivar en un incidente de seguridad.



# GOOD GOVERNANCE CODE ON CYBERSECURITY



2023



# GOOD GOVERNANCE CODE ON CYBERSECURITY

Experts participating in these Working Groups have acted in their personal capacities. Therefore, their opinions and recommendations do not stand for or hold their organisations accountable.

These papers are the result of a collective reflection exercise; however, their conclusions and proposals does not necessarily represent the opinion of all the participants, which do not necessarily share all them.

## ACKNOWLEDGMENTS

### **Civil society coordinator:**

Gianluca D'Antonio (Presidente de ISMS Forum)

### **Institutional coordinator:**

Andrés J. Ruiz Vázquez (Departamento de Seguridad Nacional)

### **Authors and contributors:**

Raúl Amigorena Eguiluz

Roberto Baratta Martínez

Mariano J. Benito Gómez

Juan Fco. Cornago Baratech

Ángel Domínguez Fernández-Burgos

Javier García Quintela

Daniel Largacha Lamela

Idoia Mateo Murillo

Francisco del Olmo Fons

Luis Paredes Hernández

Julia Perea Velasco

Olga Ramírez Sánchez

Antonio Ramos García

Jesús Sánchez López

Alejandro Viana Lara

María Elisa Vivancos Cerezo



# CONTENTS

1. INTRODUCTION	27
2. GOAL	29
3. SCOPE	30
4. STRUCTURE	31
5. PRINCIPLES AND RECOMMENDATIONS	32
Principle 1: Proportionality	32
5.1 Strategy and organisation	32
Principle 2: Strategic alignment and foresight	32
Principle 3: Responsibility and organisation	33
Principle 4: Ethics and compliance	34
5.2 Management	34
Principle 5: Management model	34
Principle 6: Resourcing	35
Principle 7: Managing incidents and resilience	35
Principle 8: Training and awareness	36
Principle 9: Innovation and continuous improvement	36
5.3 Supervision	36
Principle 10: Cyber intelligence	36
Principle 11: Periodic reporting	37
Principle 12: Continuity	38
Principle 13: Risk management	38
6. GLOSSARY	39



---

## 1. INTRODUCTION

---

In April 2019, the **National Security Council** approved the National Cybersecurity Strategy, the text of which highlights public-private cooperation as a key component to achieve the goals established in cybersecurity. The Strategy also foresees the National Cybersecurity Forum, an area within the National Security System composed of representatives of civil society, independent experts, the private sector, academic institutions, associations and non-profit organisations, among others, with the aim to strengthen and create public-private synergies.

Cybersecurity has become the strategic foundation on which the digital revolution experienced by all sectors of society, including public administrations, companies and citizens, is based. It will only be possible to continue to progress safely in this transformation if cybersecurity is the basis.

The regulatory framework for cybersecurity has evolved over the last few years, both at a national and European level, seeking to improve the cybersecurity of new sectors whose obligations have been increased. Many of the regulatory developments and changes in this area have been prompted by the increasingly frequent and costly negative effects borne by organisations, either as a result of cyber-attacks or inadequate internal management of cybersecurity risks.

In Spain, the new **National Cybersecurity Framework**, set down in Royal Decree 311/2022<sup>1</sup>, explicitly mentions the need to follow a process of continuous and adaptive improvement of cybersecurity, which is an increasingly relevant part of the **country's sustainability model**, because of the impact it can have, not only on the organisation itself, but also on its employees, suppliers, customers and stakeholders who may be affected by the organization's activities. Also, **Royal Decree 43/2021**<sup>2</sup> requires the appointment of an **information security officer** in the organisation who reports directly to senior management and maintains appropriate independence from those in charge of networks and information systems.

---

1 Royal Decree 311/2022, of 3 May, regulating the National Cyber-security Scheme.

2 Royal Decree 43/2021, of 26 January, implementing Royal Decree-Act 12/2018, of 7 September, on the security of networks and information systems

At European level, Directive EU 2022/2555, known as **NIS 2**, on measures for a high common level of cybersecurity across the Union, includes specific cybersecurity governance measures. Among these, it establishes that the management bodies of organisations shall **approve cybersecurity risk management measures and supervise their implementation**.

The **National Cybersecurity Forum**, at its plenary session on 8 October 2021, approved the lines of work for the 2021 - 2022 period for each of the working groups comprised in the Forum. Specifically, the **incorporation of cybersecurity into the good corporate governance of organisations** was the line of work approved to be elaborated by **Working Group 1 on Cybersecurity Culture**.

**Management bodies are in charge of the organisation's leadership** and the monitoring of their correct functioning, including supervising the management and control of **corporate risks**, which ever more frequently and more intensely include those of a cybernetic nature.

Accordingly, and along the lines approved at the National Cybersecurity Forum, Working Group 1 began the task of **compiling the fundamental principles and associated recommendations that the management bodies of an organisation**, regardless of its size or sector, can follow in order to ensure suitable governance of its cybersecurity.

This Code of Good Governance is the final result of the work of the aforementioned Group, made up of experts in cybersecurity, as well as the analysis of various existing regulations and standards, examined from a practical and current perspective, to improve corporate governance in the field of cybersecurity.

---

## 2. GOAL

---

The new challenges arising from the materialisation of threats in cyberspace have generated a significant increase in cyber attacks, both in terms of volume and in terms of frequency and/or sophistication. Facing new cybersecurity challenges requires policies of continuous review and improvement, together with the optimisation of cybersecurity controls and measures, applied both to the protection of the value and functioning of organisations and to the protection of the citizens' data they hold.

This Code of good governance is neither a definition of a new standard of controls, nor an implementation manual. On the contrary, the goal of the Code is to propose to organisations practices aimed at supporting a **cybersecurity governance model** that facilitates the management of the security of networks and information systems, as well as contributing to improve the decision-making process in this field by the organisations' governing bodies and, in particular, by the management body.

With this general goal in mind, a number of specific goals are set out below:

- **Goal I. Integrate the guiding principles of cybersecurity governance into a single code of good governance.**

Group together, in a specific and succinct manner, the main activities that an organisation must carry out to govern its corporate cybersecurity in a suitable and mature manner.

Have in place a common approach for the guiding principles, security measures and audit procedures, as well as elements to monitor compliance with current or future cybersecurity standards that may be implemented.

- **Goal II. Create a document to assist the organisation's management body and management team.**

Identify the major issues related to cybersecurity management and/or risks that need to be addressed by an organisation, the sessions in which these issues are to be addressed and their periodicity.

- **Goal III. Train and raise awareness among organisations' governing bodies and management teams on their role and responsibility in the field of cybersecurity.**

Serve as a reference for managers of organisations and their governance bodies to understand their responsibilities and functions in the proper management of corporate cybersecurity.

- **Goal IV. Provide a comprehensive view of cybersecurity monitoring and reporting responsibilities.**

Explicitly define the cybersecurity monitoring and reporting responsibilities and provide guidance on which significant events or incidents should be reported to management, governance bodies and/or supervisory bodies.

---

### 3. SCOPE

---

This Good governance code on cybersecurity **provides general recommendations**, organised in Principles so that it may be used by any organisation seeking to achieve an adequate governance of cybersecurity, regardless of its size, sector, activity or even degree of maturity in the field.

The effective implementation of the Principles and Recommendations included in this Code by an organisation could de facto be interpreted as a **sign of maturity in cybersecurity** and contribute to better risk management and protection of its goals and of the stakeholders that may be affected by the activities of the organisation.

This Code **may also be used by the organisation as a guide for compliance with reporting obligations** that may be required by various supervisory bodies.

---

## 4. STRUCTURE

---

The Code presents a **principles' approach** defined as the set of values, experiences and standards that guide and regulate the governance of cybersecurity.

These principles may be considered as **supporting the vision, mission and strategic goals** of cybersecurity risk management and should be observed for the improvement of the decision-making process by the bodies responsible for any organisation, according to the Principle of proportionality, irrespective of its size or activity.

The principles are drawn up in the form of recommendations that are fundamental for their implementation.

They are organised in three major blocks:

- **Strategy and organisation**

This details the most important principles on which management bodies must build the cybersecurity strategy and organisation. These principles are directly related to the management of cybersecurity.

- **Management**

A set of fundamental activities, controls and decisions that organisations must undertake to ensure that they have suitable cybersecurity maturity, including the prevention, detection, response to and recovery from incidents. These principles should be implemented by the organisation's management from the cybersecurity or information security unit.

- **Supervision**

This details the minimum elements that need to be validated by the organisation's governance bodies, as well as the basic requirements that the information to be received must meet in order to perform this validation. It specifies how continuous supervision should be carried out by the organisations' management and the cybersecurity or information security unit.

---

## 5. PRINCIPLES AND RECOMMENDATIONS

---

### Principle 1: Proportionality

The recommendations included in this Code will be applied to organisations under the principle of proportionality, taking into account their own complexity, size, the risks to which they are subject, the resources they have available and other applicable circumstances.

#### 5.1 Strategy and organisation

### Principle 2: Strategic alignment and foresight

**Cybersecurity**, as a discipline that helps organisations achieve their goals, **needs to be aligned with the organisation's mission and vision.**

**Recommendation 1:** The management body shall formally recognise, in a publicly visible document, the principles and commitments to cybersecurity as a fundamental element to protect the business assets, for the purpose of achieving its goals and fulfilling its mission.

**Recommendation 2:** Cybersecurity shall be one of the declared areas of the organisation's risk management and control policy.

**Recommendation 3:** The organisation, taking into consideration the operational needs of the business and the risks that might affect achieving its goals, shall define short-, medium- and long-term plans that ensure the future vision and continuous improvement of cybersecurity, enabling it to reduce its exposure to risk within the defined tolerance levels.

**Recommendation 4:** Decisions on cybersecurity will be made according to the actual risk of the materialisation of threats to the organisation. A system for monitoring the efficiency and compliance with the defined security goals shall likewise be implemented.



### Principle 3: Responsibility and organisation

Cybersecurity is a complex and cross-cutting discipline that affects all the activities of an organisation, so it requires suitable leadership and a structure that, in order to be properly implemented and managed, must in turn be made up of professionals with appropriate training and experience.

**Recommendation 5:** The organization shall aim to have at least one member of the management body with experience in cybersecurity management to support and validate the objectives prior to their approval by the management team.

**Recommendation 6:** The organisation shall have a unit that assumes the function of defining, driving and controlling cybersecurity, that participates in cybersecurity decision-making and strategy, and that ensures appropriate reporting of cybersecurity-related risks at the proper levels, as well as the necessary mechanisms to mitigate and control those risks.

This unit shall have sufficient material and human capacities and resources to achieve its goals, and shall report functionally to the management body, to one or more of its specialised committees, or to any other body or member of the organisation's senior management, provided that due independence is maintained with respect to those responsible for the network and information systems.

**Recommendation 7:** The head of this unit, the Chief Information Security Officer (hereinafter, CISO), shall be a person with the appropriate knowledge, experience and skills to perform this function, and shall have sufficient decision-making capacity and influence in the organisation.

**Recommendation 8:** There shall be a formally constituted cybersecurity committee in which, in addition to the CISO, an appropriate number of areas of the organisation will be represented in order to adopt any important resolution for information security that may substantially affect the organisation's activities.

**Recommendation 9:** Organisations, depending on their complexity and exposure to cyber risk, should take cybersecurity into consideration in at least one of their crisis committees.

**Recommendation 10:** The management body shall assign the executive supervision of cybersecurity management to one of its specialised committees (e.g. risk committee, audit committee).

#### Principle 4: Ethics and compliance

Cybersecurity governance shall include not only compliance with applicable regulations, but also **best practices in security and the ethical use of the organisation's resources**.

**Recommendation 11:** The management body shall understand the implications of best practices, among others, in the management of cybersecurity risks, both within its organization and in each of the markets in which it operates and in its relationship with the different stakeholders.

## 5.2 Management

#### Principle 5: Management model

**Cybersecurity is a cross-cutting matter** for the entire organisation and its business processes. Cybersecurity management should be guided by best practices and be suited to each organisation.

**Recommendation 12:** The organisation shall rely on recognised national, european or international standards, suited to its needs, in order to better monitor the evolution of its maturity.

## Principle 6: Resourcing

Organisations should bear in mind that **the cybersecurity function requires constant and suitable resources** allocated to its maintenance and improvement.

**Recommendation 13:** The management body shall ensure that the unit in charge of cybersecurity management, as well as other units with responsibility to achieve the established goals, have sufficient material and human capacities to be able to carry out the assigned functions effectively and efficiently.

## Principle 7: Managing incidents and resilience

One of the purposes sought by cybersecurity is to ensure the continuity of operational capability for the purposes of the organisation and the stakeholders that may be affected by its activities. This is known as **operational resilience** and as a result it is necessary to develop capabilities to contain and/or recover from cyber incidents.

**Recommendation 14:** It will be defined when an incident is considered significant, depending on the impact, the type of organization, its sector and the regulations to which it may be subject in the markets in which it operates.

**Recommendation 15:** The operating groups in charge of its management (both at technical, tactical and strategic level) shall be identified in order to minimise the impact on the business, and to ensure regulatory compliance and suitable internal/external communication.

**Recommendation 16:** Capabilities shall be available that allow the organisation to be resilient to ensure continuity of operations and full recovery of services within an appropriate timeframe, which shall be determined in the business continuity plan.

## Principle 8: Training and awareness

All **the staff in the organisation need to have sufficient cybersecurity know-how** to deal with and mitigate the risk to which they are exposed<sup>3</sup>.

**Recommendation 17:** Management and the management body shall promote cybersecurity training, awareness and culture throughout the organisation in order to educate its staff on best practices and habits to prevent and mitigate cybersecurity risks.

## Principle 9: Innovation and continuous improvement

**Cybersecurity needs to adapt and improve in keeping** with new and constant developments in technology and cyber threats.

**Recommendation 18:** Cybersecurity management will be constantly improving and evolving to guarantee a suitable defence against threats.

## 5.3 Supervision

### Principle 10: Cyber intelligence

**Anticipation is a key element in protecting** against any risk not only the organisation itself, but also the stakeholders who may be affected by its activities, so the organisation needs to rely on cyber intelligence as a basis to prepare for the management of cyber threats.

---

<sup>3</sup> People are the main asset available to organisations for suitable cybersecurity protection. At the same time, the main risks in this area often arise from incidents which, whether actively or passively, are generated by people

**Recommendation 19:** The cybersecurity committee shall inform management and the management body of cyber threats that might affect the organisation's goals. For this purpose, at least the main actors and the major and most recent cyber threats shall be taken into account, considering their potential impact on the organisation's operations.

## Principle 11: Periodic reporting

**Regular reporting of the organisation's cybersecurity situation to the organisation's governance bodies** is among governance best practices according to international standards, and in some cases it is an obligation.

**Recommendation 20:** The management body shall regularly monitor cybersecurity by including this topic on the agenda of its meetings and/or those of its specialised committees where applicable (audit, risk, sustainability or other specific committees for the treatment of cybersecurity risk), for which it will require regular reporting of cybersecurity management to the executive responsible (Chief Information Security Officer - CISO). This reporting should take place periodically, and it is a best practice to report at least twice a year.

**Recommendation 21:** The periodic reporting should at least include the status of cybersecurity, the evolution of the degree of maturity and cyber risk, the evolution of threats, the allocation of resources for network and information systems security, significant incidents managed, if any, the status of security of supply chain operations dependent on third parties, as well as any relevant cybersecurity resolutions taken by the management team that may materially affect the organisation's activities. The Chief Information Security Officer - CISO - shall also report, if applicable, any obstacle or hindrance that might restrict the proper performance of their activity.

**Recommendation 22:** When a matter that may affect cybersecurity is on the agenda of the management body meetings, the cybersecurity implications of the matter must be discussed, for instance: major digital transformation initiatives, implementation of new technologies and major investments in technology assets, mergers and acquisitions, expansion of facilities, and major upgrades.

## Principle 12: Continuity

**Cybersecurity is part of an organisation's continuity strategy**, and its testing it is essential to be properly prepared for cyber incidents.

**Recommendation 23:** The management body shall require the performance of comprehensive periodic tests in order to check the resilience mechanisms of the organization as part of the cybersecurity plans

In this context:

- Testing the business continuity plan as well as simulations and preparation exercises for crisis management committees should be conducted.
- In general terms, companies should systematically conduct effective drills and tests of the various protection, response and recovery measures.
- These exercises should involve the entire organisation, particularly focusing on the company's critical processes, also involving the supply chain.

**Recommendation 24:** The management body shall make sure that management supports the establishment, implementation, testing and continuous improvement of cyber resilience mechanisms.

## Principle 13: Risk management

The proper management, assessment and communication of cybersecurity risk is a **key component of corporate risk management for any organisation**.

**Recommendation 25:** Independent assessments, with respect to the cybersecurity unit, shall be conducted at least once a year to enable the management body to obtain an additional and complementary view of the proper status of the cybersecurity risk management programme for the organisation's critical processes, including the supply chain.

---

## 6. GLOSSARY

---

A glossary is included below for a better understanding of the concepts covered in this Code:

**Information asset:** Any information or system related to the processing of information of value to the organisation. It can be business processes, data, applications, computer equipment, personnel, carriers of information, ancillary equipment or facilities. This information is susceptible to being attacked, whether deliberately or accidentally, with consequences for the organisation.

**Cyber threat:** A threat to systems and services present in cyberspace or reachable through cyberspace.

**Cyber attack:** A deliberate attempt by a cybercriminal to gain unauthorised access to a computer system by using various techniques and vulnerabilities in order to carry out activities for malicious purposes, such as theft of information, extortion of the owner or simply damaging the system.

**Cyber intelligence:** The discipline that allows processed information about the intent, opportunity and capability of malicious actors to be used in order to anticipate the most appropriate cybersecurity measures.

**Cybersecurity:** The ability of network and information systems to withstand, at a given level of reliability, any action compromising the availability, authenticity, integrity or confidentiality of the stored, transmitted or processed data, or the corresponding services offered by or accessible through such network and information systems. It comprises the combination of people, policies, processes and technologies employed by an organisation to protect its assets against cyber threats in order to achieve its goals and fulfil its mission.

**Organisation:** This term refers not only to the company itself but also to all the other entities within its group.

**Cyber risk:** An unfavourable circumstance that may occur and when it happens it has negative consequences on the assets, causing their unavailability, incorrect operation or loss of value. If this unfavourable circumstance occurs at the same time as a vulnerability or weakness in the systems, it can result in a security incident.

