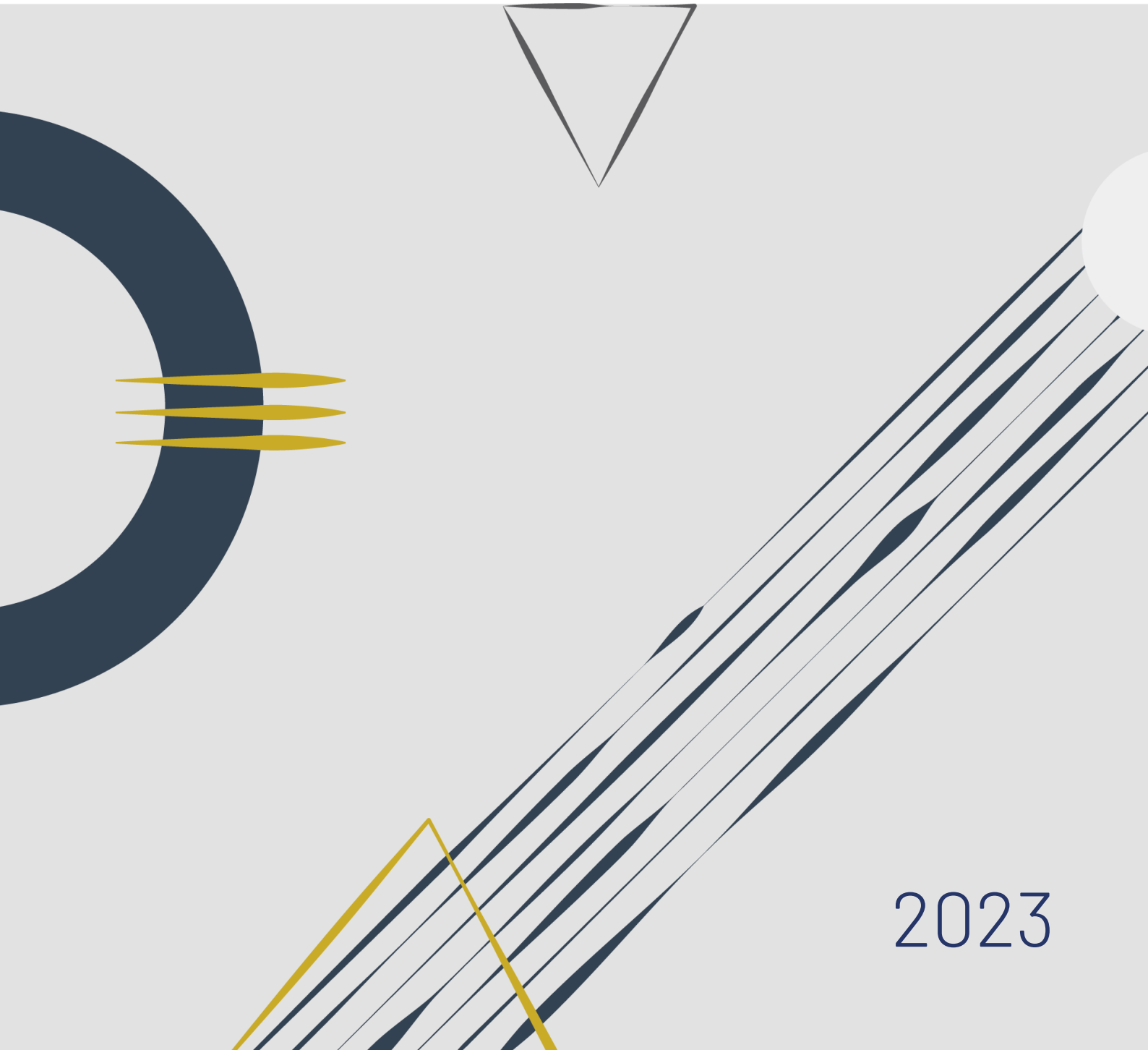
FORO NACIONAL DE CIBERSEGURIDAD

CÓDIGO DE BUEN GOBIERNO DE LA CIBERSEGURIDAD



2023

Catálogo de publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA, RELACIONES CON LAS CORTES Y MEMORIA DEMOCRÁTICA

NIPO (edición online): 089-23-013-9
Fecha de edición: junio 2023

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

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[1], 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**[2] exige el nombramiento de un **responsable de la seguridad de la información** en las organizaciones que reporte directamente a la alta dirección y

[1] Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

[2] 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[3].

> **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.

[3] 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.

FORO
NACIONAL DE
CIBERSEGURIDAD

2023