GUÍA DE SUPERVISIÓN DE CIBERSEGURIDAD PARA DIRECTIVOS NO TÉCNICOS

Recomendaciones para empresas

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Índice

Índice

1. Introducción

El presente manual proporciona una estructura comprehensiva y accesible para que los ejecutivos sin especialización tecnológica comprendan la relevancia de incorporar la seguridad digital dentro de la planificación estratégica empresarial.

1.1 Glosario de términos

Para facilitar la comprensión de algunos términos técnicos, se incluye un **glosario de términos clave** de INCIBE.

1.2 Introducción

En la actualidad, **la ciberseguridad es fundamental para la supervivencia y crecimiento de cualquier organización**. La transformación digital ha cambiado por completo la manera de trabajar de las empresas, haciendo más rápidos los procesos, las comunicaciones y el manejo de la información. Pero también ha creado nuevas amenazas que ponen en peligro la privacidad, integridad y disponibilidad de los datos.

Para hacer frente a estos retos, no es suficiente confiar únicamente en los equipos técnicos. Es necesario que la alta dirección, aunque no tenga conocimientos tecnológicos, participe de forma activa en la supervisión y gestión de la seguridad digital. Esto permite impulsar una cultura organizacional enfocada en la prevención y la protección.

Una gestión efectiva de la ciberseguridad necesita incluir buenas prácticas desde el diseño de los sistemas. Esto significa incorporar controles, validaciones y mecanismos de protección desde las primeras fases del desarrollo de los proyectos. La participación de los equipos no técnicos también incluye garantizar que se promueva la formación en buenas prácticas de desarrollo seguro. Además, se debe mantener una documentación clara basada en estándares y dar una respuesta rápida ante vulnerabilidades detectadas.

Durante todo el ciclo de desarrollo de proyectos, debe protegerse cualquier información sensible que se use, incluso en fases de prueba, evitando el uso de datos reales cuando no sea estrictamente necesario. [REF - 1].

Esta guía ofrece un marco claro y fácil de entender para que los directivos no especializados en tecnología comprendan la importancia de integrar la ciberseguridad en la estrategia de negocio. Solo así podrán liderar con criterio iniciativas que protejan los activos digitales de la organización y fortalezcan la confianza de clientes, socios y empleados en un entorno donde la exposición al riesgo es constante.

El panorama empresarial contemporáneo ha posicionado la protección digital como un elemento fundamental para garantizar la supervivencia y expansión organizacional. El proceso de digitalización empresarial ha transformado radicalmente las metodologías operativas, optimizando flujos de trabajo, canales comunicativos y sistemas de gestión informacional.

Simultáneamente, este proceso ha introducido vectores de amenaza que comprometen la seguridad, autenticidad y accesibilidad de la información corporativa. La mitigación efectiva de estos riesgos trasciende la dependencia exclusiva en recursos tecnológicos especializados.

Los niveles ejecutivos superiores, independientemente de su experiencia técnica, deben establecer un compromiso directo en la supervisión y administración de la seguridad informática. Este enfoque permite fomentar un ecosistema organizacional orientado hacia la prevención y el resguardo.

La administración exitosa de la protección cibernética exige la integración de metodologías optimizadas desde la conceptualización arquitectónica de los sistemas. Debe incorporar mecanismos de control, procesos de verificación y estructuras de salvaguarda durante las etapas preliminares del ciclo de desarrollo de proyectos.

El seguimiento detallado de los indicadores del nivel de riesgo, combinado con la verificación de cumplimiento de medidas técnicas y organizativas, representa una contribución sustancial hacia la minimización de exposiciones vulnerables. Resulta igualmente esencial garantizar que, en cualquier fase de un proyecto, se utilicen componentes, herramientas y recursos previamente validados, minimizando así riesgos de seguridad. Es imprescindible ejecutar evaluaciones y pruebas especializadas antes de la puesta en operación de los sistemas o servicios. Asimismo, debe establecerse una separación clara y definitiva entre los distintos entornos del proyecto, como los de desarrollo, pruebas, validación y producción, acompañada de controles de acceso estrictos, alineados con las responsabilidades y perfiles de cada participante, para reducir la exposición a amenazas y garantizar la integridad del proyecto.

Las decisiones relacionadas con la seguridad de la información son, en realidad, decisiones de negocio. Detrás de cada medida de seguridad hay una valoración previa del riesgo, del impacto que puede tener un incidente y del esfuerzo que la empresa está dispuesta a asumir para evitarlo. Gestionar adecuadamente los riesgos permite a la empresa proteger su información, garantizar la continuidad del negocio y optimizar recursos, aplicando criterios de coste-beneficio que resulten realistas y sostenibles. En INCIBE contamos con la **'Guía de Gestión de Riesgos. Una guía de aproximación para el empresario**', la cual ofrece a pymes y autónomos una visión práctica y accesible para integrar la gestión de riesgos en su día a día, alineándola con los objetivos de la empresa y con una correcta gestión de la seguridad de la información.

El compromiso de los equipos no especializados técnicamente incluye la promoción de capacitación en metodologías seguras. Además, requiere el mantenimiento de documentación estructurada fundamentada en estándares reconocidos y la implementación de respuestas eficientes ante vulnerabilidades identificadas. Paralelamente, a lo largo de todo el proceso de desarrollo debe salvaguardarse cualquier información confidencial utilizada, incluyendo las etapas de prueba. Es crucial evitar el empleo de información auténtica cuando no resulte estrictamente indispensable.

2. Principios básicos de ciberseguridad

La ciberseguridad afecta a toda la organización y, por tanto, debe formar parte de la agenda de cualquier equipo directivo.

No se trata de que los directivos responsables de gestión tengan que conocer al detalle cómo funciona un cortafuegos o qué tipo de virus puede atacar a un sistema. Lo que sí necesita es comprender los aspectos generales que le permitan saber si su organización está bien protegida, si se están haciendo las cosas correctamente y si hay señales de alerta que requieren atención.

Esta sección ofrece una mirada sencilla y práctica, pensada para quienes deben tomar decisiones, asignar recursos o supervisar equipos, pero no tienen formación técnica. A través de ejemplos, preguntas clave y explicaciones claras, se pretende que cualquier directivo pueda hacerse una idea general del estado de la ciberseguridad de su organización, identificar riesgos y, sobre todo, actuar con sentido común y criterio.

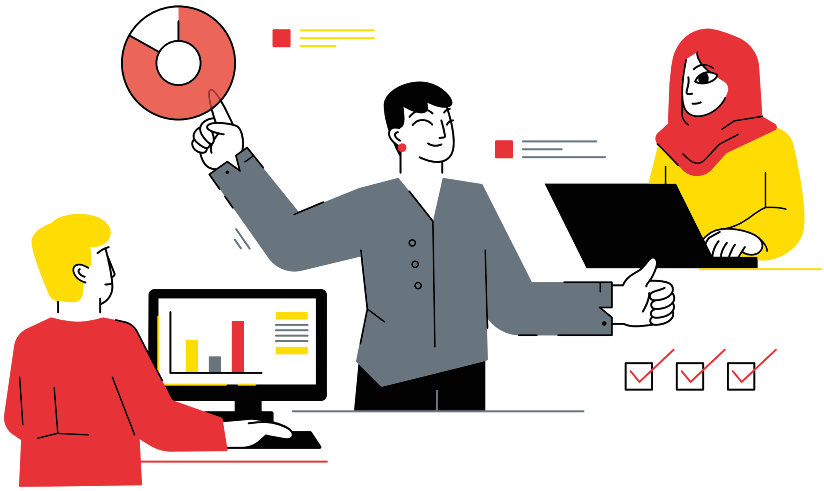
Confidencialidad

Integridad

Disponibilidad

2.1 Confidencialidad, integridad y disponibilidad

La protección de la información dentro de la empresa se articula en torno a tres principios que conforman la base de cualquier estrategia de ciberseguridad: confidencialidad, integridad y disponibilidad. Estos pilares no funcionan por separado, sino que trabajan juntos para dar una protección completa contra amenazas que pueden dañar el funcionamiento, la reputación o la competitividad de la empresa.



- La **confidencialidad** asegura que sólo las personas autorizadas pueden ver los datos, usando controles como contraseñas, permisos especiales o técnicas de cifrado que protegen la información importante de accesos no permitidos. Mantener este aspecto ayuda a conservar la confianza de clientes, socios y empleados, y evita filtraciones que podrían dañar tanto la privacidad como la estrategia de la empresa.

- La **integridad** se encarga de que los datos se mantengan completos y sin cambios no autorizados. Cualquier modificación debe poder seguirse, lo que se consigue con registros de actividad, copias de seguridad, firmas digitales o sistemas de control de versiones que permiten comprobar que la información es auténtica en todo momento.

- Por último, la **disponibilidad** se refiere a poder acceder a los datos y sistemas por personal autorizado cuando se necesiten. Tener infraestructuras estables, planes de emergencia para fallos, actualizaciones regulares y mantenimiento preventivo son acciones que evitan interrupciones en el trabajo diario. Esto permite que la empresa siga funcionando con normalidad ante cualquier problema. [REF - 2]

Estos tres principios están estrechamente interrelacionados. Si uno de ellos se ve comprometido, los otros también corren peligro. La información puede estar disponible, pero si ha sido alterada, su valor desaparece. Del mismo modo, un sistema íntegro pero inaccesible resulta inútil para la toma de decisiones. Por ello, **cualquier estrategia eficaz de ciberseguridad debe tratar de manera integrada la protección del acceso, la confiabilidad de los datos y la continuidad del servicio**. Solo de esta forma es posible reducir riesgos y asegurar una gestión segura y fiable de la información en un mundo cada vez más digital. Un ejemplo de caso de éxito de una empresa que toma medidas de seguridad digital, se muestra en el siguiente video.

2.2 Concepto de riesgo digital

La transformación digital ha traído consigo nuevas formas de operar, comunicar y crecer, pero también ha incrementado considerablemente la exposición a ciberamenazas. El riesgo digital surge precisamente de esta dependencia creciente de sistemas informáticos, servicios en la nube y plataformas conectadas, y representa una de las mayores preocupaciones para cualquier organización en la actualidad.

No se trata solo de ataques informáticos. El riesgo digital también abarca errores humanos, incumplimientos de normas, fallos de sistemas automáticos, problemas de privacidad y vulnerabilidades que vienen de proveedores externos. Todas estas situaciones pueden cambiar el funcionamiento normal de una empresa y dañar su seguridad, reputación y capacidad de reacción.

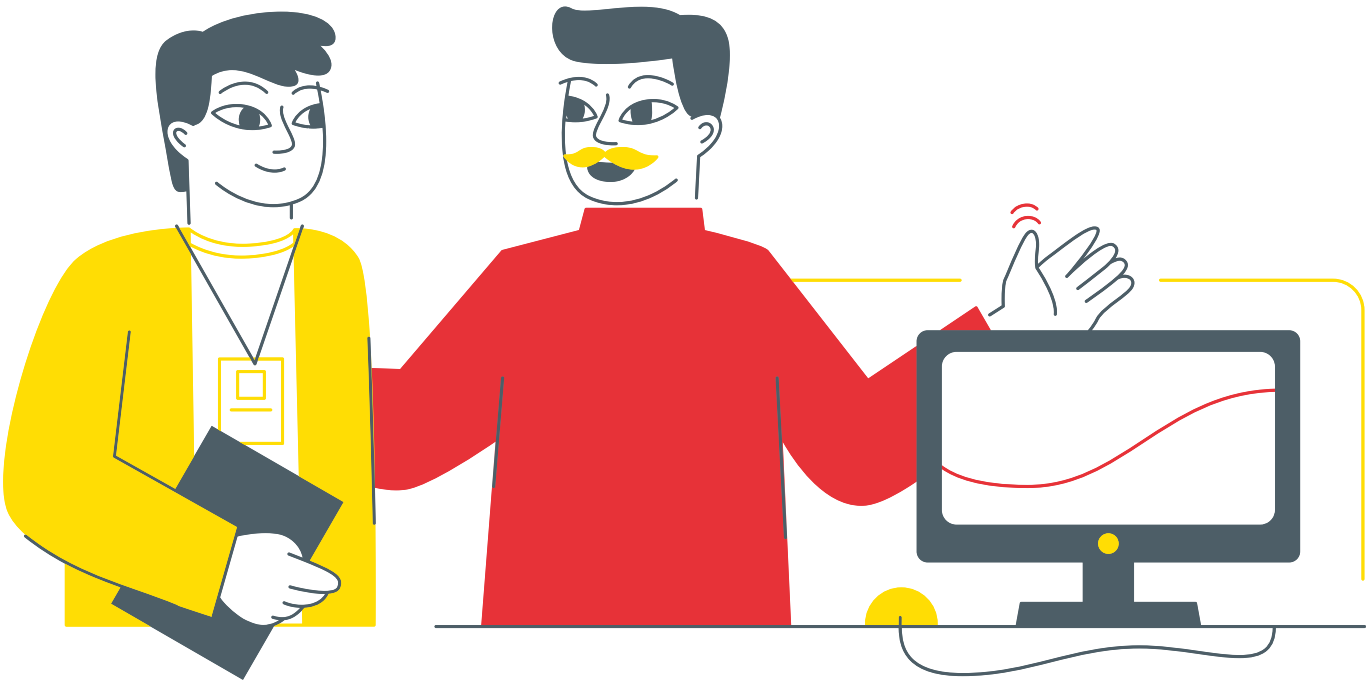
Entre los riesgos más frecuentes se encuentran:

- Robo de información confidencial
- Ransomware y secuestro de sistemas
- Pérdida de control sobre datos personales
- Falta de competencias digitales
- Incapacidad de recuperación rápida
- Compromiso de operación diaria

Gestionar estos riesgos implica conocer qué activos son prioritarios, evaluar con regularidad las amenazas que los rodean y establecer medidas claras para protegerlos. No basta con reaccionar ante un problema, es necesario anticiparse, definir responsabilidades y disponer de procedimientos de respuesta que estén activos antes de que ocurra una crisis.

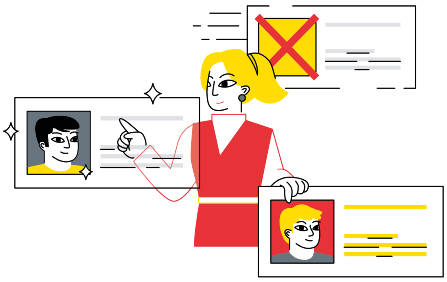
Las herramientas de gestión de riesgos digitales, combinadas con sistemas de monitoreo continuo y planes de contingencia, permiten mantener la seguridad bajo control y responder con rapidez. El seguimiento constante del entorno digital, la evaluación de terceros y la adaptación a nuevas amenazas ayudan a minimizar impactos y a fortalecer la resiliencia organizacional.

La gestión del riesgo no debe verse como una cuestión técnica aislada, sino como un enfoque transversal que requiere colaboración entre todas las áreas de la empresa. Solo así es posible proteger los activos digitales, asegurar la continuidad del negocio y construir un entorno de confianza frente a los desafíos actuales.[REF - 3]



2.3 Diferencia entre amenaza, vulnerabilidad e incidente

Saber diferenciar entre amenaza, vulnerabilidad e incidente permite actuar con mayor eficacia ante posibles riesgos digitales. Aunque a menudo se confunden, cada término señala una fase distinta dentro de un fallo o ataque.



- Una **amenaza** es un peligro que podría afectar a los sistemas. Puede presentarse como un ataque dirigido, una avería técnica o un error cometido por una persona. Identificar correctamente estos elementos facilita diseñar respuestas ajustadas a cada situación y reducir el impacto sobre la seguridad informática. [REF - 4]

- La **vulnerabilidad** es aquello que facilita que una amenaza tenga éxito. Se trata de fallos de seguridad, malas configuraciones, programas sin actualizar o contraseñas débiles. Cualquier descuido puede abrir la puerta a una posible intrusión o daño. [REF - 5]

- El **incidente** aparece cuando una amenaza aprovecha una vulnerabilidad y se produce un impacto real. Es el momento en que se accede a datos sin permiso, se interrumpe un servicio o se filtra información. En ese punto, ya no se trata de una posibilidad, sino de un hecho que requiere una reacción rápida.

	¿Qué es?	Ejemplo
Amenaza	Algo que puede causar un daño a la empresa	Un virus informático o un apagón
Vulnerabilidad	Una debilidad que hace que una amenaza tenga más posibilidades de éxito	Un ordenador sin antivirus o una contraseña débil
Incidente	Cuando la amenaza se hace realidad aprovechando una vulnerabilidad	Se roban datos, se cae el sistema o se filtra información confidencial

Estos tres elementos se relacionan entre sí y forman una cadena de riesgo. Una amenaza no causa daño por sí sola si no hay vulnerabilidades, y un incidente no ocurre si no se permite esa combinación. Por eso, **detectar las debilidades y anticiparse a los peligros es clave para evitar que el impacto llegue a producirse**.

3. El rol de la alta dirección

La implicación de la dirección es clave para que la empresa cuente con una protección adecuada frente a los riesgos digitales.

3.1 Supervisión y gobernanza

Las decisiones sobre ciberseguridad deben partir de los niveles más altos. Es la dirección quien debe marcar el rumbo, definiendo políticas y procedimientos claros para proteger la información y los sistemas.

Estas políticas deben adaptarse a la realidad de la empresa y cumplir con la normativa vigente. Además, todos los trabajadores deben conocerlas y aplicarlas en su día a día.

Es recomendable que la dirección revise con frecuencia el estado de la seguridad. Los informes ayudan a saber qué amenazas se han detectado, qué se ha hecho y si las medidas funcionan bien o hay que cambiarlas.

Cuando la dirección se implica, transmite a toda la organización que la ciberseguridad es una prioridad. Esto refuerza el compromiso de los equipos y mejora el cumplimiento de las normas.

También es necesario asignar responsabilidades y crear canales de comunicación efectivos. Debe haber una persona o un equipo encargado de coordinar la seguridad y contar con los recursos adecuados para ello. [REF - 6]

3.2 Integración de la ciberseguridad en la estrategia de negocio

La ciberseguridad no debe tratarse como un asunto aislado del área técnica. Integrarla en la estrategia general de la organización permite abordar los riesgos digitales desde el inicio de cualquier decisión o proyecto.

No es sólo una cuestión de sistemas o presupuestos informáticos. **Evaluar la seguridad en cada área**, desde el diseño de productos hasta la relación con el cliente, ayuda a detectar puntos débiles antes de que se conviertan en un problema. **Este enfoque mejora la capacidad de anticiparse a amenazas, evitando errores al adoptar nuevas tecnologías o al ampliar la presencia digital.** Así, las decisiones se toman con mayor conocimiento del entorno y sus riesgos.

También refuerza la imagen de la empresa. Un fallo de seguridad puede dañar gravemente la reputación, y eso afecta a la confianza de clientes, socios y empleados. Incluir la ciberseguridad en el plan estratégico reduce esa exposición. Además, prepararse ante posibles interrupciones o ataques permite que la empresa siga funcionando sin parar. Esto reduce el impacto y evita pérdidas importantes, incluso en situaciones difíciles.

Incluir la ciberseguridad como parte de la estrategia también ayuda a cumplir con la normativa. Las empresas que lo hacen evitan sanciones y refuerzan su imagen frente a otras del sector.

Cuando la ciberseguridad forma parte del plan estratégico, la empresa avanza con mayor seguridad.

Para comenzar a incorporar buenas prácticas, existe un **decálogo de ciberseguridad** donde se resumen las medidas para integrar la seguridad en una empresa.

4. Preguntas clave para evaluar el estado de la ciberseguridad

La ciberseguridad es un aspecto clave para la continuidad y reputación de cualquier organización. No basta con instalar soluciones técnicas. La protección debe incluir procedimientos claros, formación para el equipo, revisiones periódicas y colaboración segura con proveedores o socios externos.

Para ayudar a las empresas a evaluar su estado de ciberseguridad y a avanzar hacia mayores niveles de protección, INCIBE pone a su disposición una **herramienta de autodiagnóstico** ligero especialmente diseñada para este fin. Con esta herramienta, a través de una serie de preguntas, se guía al usuario para que determine su estado en seguridad de la información, qué riesgos amenazan el funcionamiento de la empresa y qué aspectos debe mejorar. Todo ello, para empezar a medir y a mejorar.

Calcula el riesgo de tu negocio

Y es que, toda la empresa debe saber cómo actuar si ocurre un incidente. La información crítica debe estar protegida y cada persona debe conocer su papel ante una posible amenaza.

Este apartado incluye preguntas útiles para evaluar el nivel de preparación. Analizar si existe un plan de respuesta, cómo se gestionan los accesos o si el personal está formado ayuda a detectar fallos y mejorar la seguridad.

El enfoque no es técnico, sino operativo: se trata de saber si la empresa puede seguir funcionando tras un incidente, si se conocen las responsabilidades, si hay sistemas de alerta y si se cumplen las normativas vigentes.

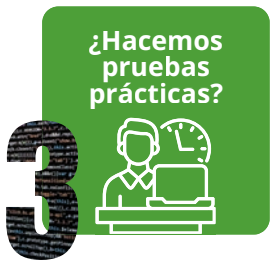
La ciberseguridad debe gestionarse como un proceso continuo y global, no como una solución puntual.

SABER CÓMO ACTUAR ANTE UN INCIDENTE

Tener un **plan de respuesta** es tan importante como tener extintores en la oficina. Si ocurre un problema, cada persona debe saber qué hacer, a quién avisar y cómo actuar para reducir el daño. Sin este plan (y comprobando que funcione) cualquier ataque puede tener consecuencias mucho más graves.

PROTEGER LO MÁS VALIOSO

Cada empresa tiene activos clave: datos de clientes, diseños, bases de datos... Hay que identificarlos y comprobar si están bien protegidos: contraseñas robustas, accesos restringidos, cifrado, etc. Saber qué datos tenemos y dónde con un inventario actualizado de la información y su ubicación.



REVISAR PARA MEJORAR

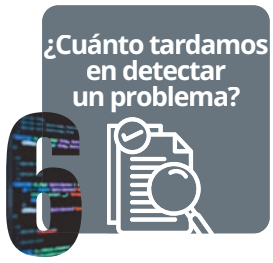
La seguridad hay que revisarla cada cierto tiempo, igual que se hace con el mantenimiento técnico. Esto permite detectar errores y corregirlos antes de que se conviertan en un problema. Simular ataques o situaciones de riesgo es útil para ver cómo responde el equipo y detectar puntos débiles.

CONTROLAR LOS ACCESOS

No todo el mundo necesita ver todo. Cada persona debe tener acceso sólo a lo necesario para su trabajo. Es necesario actualizar los permisos para que nadie tenga más acceso del que necesita para su trabajo diario, eliminar permisos a aquellos empleados que se les otorgara de manera temporal acceso a la información o que dejen de formar parte de la plantilla.

FORMAR EQUIPO

La mejor tecnología no sirve si el personal no sabe usarla bien. La formación ayuda a evitar errores, reconocer amenazas y actuar con rapidez.
Enviar pruebas controladas, como correos simulados de phishing, ayuda a saber si el equipo está atento y preparado.



SUPERVISAR LA ACTIVIDAD

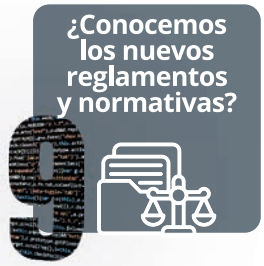
El tiempo de reacción es clave. Detectar y resolver incidentes rápidamente reduce el impacto. Disponer de herramientas que supervisen y alerten de manera temprana el comportamiento sospechoso o inusual en los sistemas de la compañía ayuda a prevenir un incidente y a mejorar las medidas a implementar.

COLABORAR DE FORMA SEGURA

Si un proveedor tiene acceso a tus sistemas, tu nivel de seguridad depende directamente del que disponga en su organización. Trabajar con proveedores seguros y confiables reduce riesgos compartidos. Los contratos deben establecer responsabilidades y cómo actuar en caso de incidente, así como tener una definición clara de la seguridad de la compañía proveedora, y una implicación del mantenimiento y aplicación de la **medidas necesarias** para salvaguardar la información.

RECUPERARSE TRAS UN INCIDENTE

Saber cuánto tiempo puedes estar sin funcionar ayuda a preparar un plan realista de recuperación. Es fundamental realizar copias de seguridad de manera periódica para no perder información de producción, y comprobar que los datos se pueden recuperar.



CUMPLIR CON LA NORMATIVA

Las leyes cambian, y cada sector tiene sus propias obligaciones. Estar al día evita sanciones y protege la reputación. Conviene revisar periódicamente si hay nuevos requisitos legales que afectan a la gestión de la seguridad de la compañía, poniendo especial atención al sector que aplica y a los plazos máximos de implantación.

MEDIR EL PROGRESO

Sin indicadores, no se puede saber si las cosas mejoran. Número de incidentes, tiempo de respuesta o nivel de formación del personal son buenas métricas. Los responsables deben entender los riesgos y avances en seguridad en términos de impacto en el negocio y conocer el nivel de seguridad y las necesidades a aplicar en la organización, pero sin entrar en tecnicismos.

5. Indicadores para la dirección

La ciberseguridad debe abordarse desde una perspectiva global, en la que la alta dirección asuma un papel activo y bien informado. Para ello, resulta imprescindible contar con indicadores que permitan conocer el estado real de la seguridad en la organización, sin necesidad de recurrir a lenguaje técnico o conocimientos especializados. Estos indicadores deben proporcionar una visión clara, accesible y directamente relacionada con los objetivos estratégicos del negocio.

El propósito de este apartado es presentar un conjunto de referencias que sirvan como apoyo a la toma de decisiones. No se trata solo de tecnología. **La dirección necesita datos claros que muestren el nivel de riesgo al que está expuesta la empresa, cómo responde ante incidentes y cuánto sabe el personal para actuar**.

Indicadores para la dirección

Riesgo y exposición

- Nivel de riesgo general
- Vulnerabililidades críticas sin resolver
- Tiempo medio de resolución

Incidentes y ataques

- Número de incidentes de seguridad
- Tiempo de detección
- Tiempo de respuesta y solución
- Coste de los incidentes

Preparación y capacidades

- Empleados formados en seguridad
- Simulacros de *phishing*
- Estado de las copias de seguridad
- Cobertura de sistemas críticos:

Cumplimiento

- Cumplimiento normativo
- Revisión de accesos

Financieros

- Inversión en seguridad versus presupuesto
- Retorno de la Inversión en Seguridad (ROI)
- Coste de inactividad evitada

Tendencias

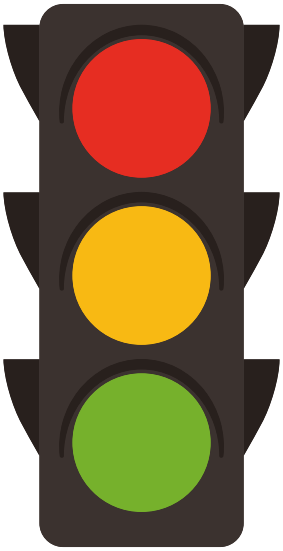
- Evolución de amenazas
- Madurez de seguridad

5.1 Indicadores de riesgo y exposición

La dirección necesita contar con indicadores que reflejen claramente el nivel de riesgo frente a amenazas digitales. No es necesario conocer detalles técnicos, sino disponer de datos que muestren de forma sencilla el estado de la seguridad.
Estos indicadores ayudan a identificar prioridades y tomar decisiones para mejorar la protección, asignando recursos donde más se necesitan. Así, quienes dirigen pueden supervisar y actuar con claridad y confianza.

Nivel de riesgo general

- **¿Qué muestra?** una valoración global del nivel de riesgo actual al que se enfrenta la organización: Bajo, Medio o Alto.
- **¿Por qué es relevante?** permite conocer de forma inmediata si la situación es estable o requiere atención urgente.
- **¿Cómo se representa?** normalmente mediante un código de colores (verde, amarillo, rojo) para facilitar la interpretación visual.



Riesgo alto: se deben tomar acciones inmediatas para mitigar amenazas.

Riesgo medio: se recomienda reforzar medidas y monitorizar la situación.

Riesgo bajo: la situación es estable y no se requieren medidas urgentes.

Vulnerabililidades críticas sin resolver

- **¿Qué muestra?** número de fallos de seguridad de alto impacto que todavía no han sido corregidos.

- **¿Por qué es relevante?** cada vulnerabilidad supone una posible puerta de acceso para un atacante, lo que convierte su presencia en un riesgo inmediato para la organización.
- **¿Cómo se representa?** comparativa entre el número de vulnerabilidades críticas detectadas y las que permanecen pendientes:

> Actualmente existen X vulnerabilidades críticas. El mes anterior: Y

Tiempo medio de resolución

- **¿Qué muestra?** promedio de días que se tarda en resolver incidencias de seguridad significativas.
- **¿Por qué es relevante?** un tiempo de respuesta prolongado aumenta el período en que la organización queda expuesta a posibles ataques.
- **¿Cómo se representa?** informe con valor numérico directo:

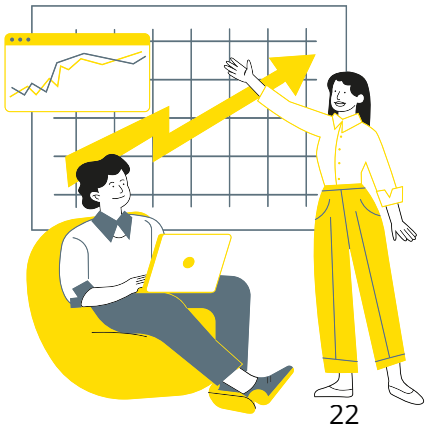
> El tiempo medio de resolución en el último trimestre ha sido de X días.

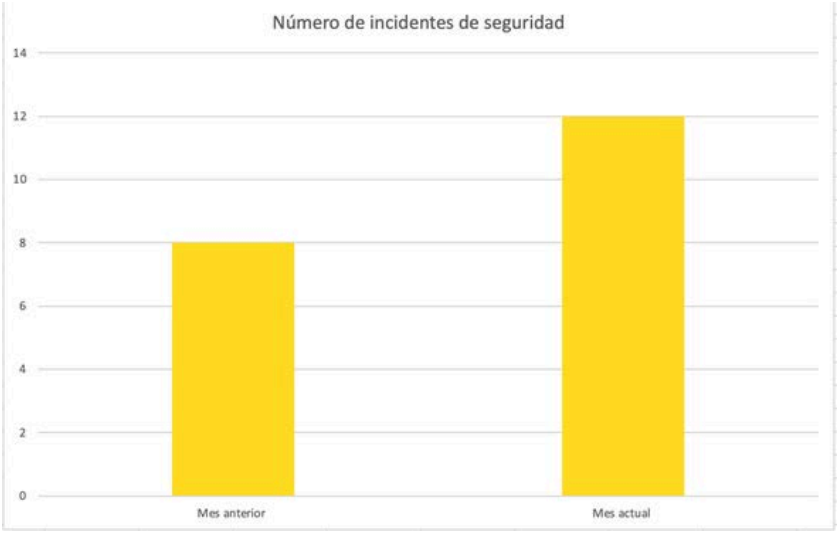
5.2 Indicadores de incidentes y ataques

Para gestionar eficazmente la ciberseguridad, es fundamental medir y analizar los problemas de seguridad que sufre una empresa, muestran cómo responde ante los ataques. Saber cuántos incidentes hay, cuánto tiempo se tarda en detectarlos y solucionarlos, y cuánto cuestan, ayuda a mejorar la protección y a decidir dónde invertir.

Número de incidentes de seguridad

- **¿Qué mide?** cuántos incidentes se han producido.
- **¿Por qué importa?** muestra si los ataques están creciendo.
- **¿Cómo se presenta?** gráfico:





Tiempo de detección

- **¿Qué mide?** Horas desde el ataque hasta su detección.
- **¿Por qué importa?** Cuanto antes se detecta, menor daño.
- **¿Cómo se presenta?** Media: X horas

Tiempo de respuesta y solución

- **¿Qué mide?** Tiempo hasta que el incidente se resuelve del todo.
- **¿Por qué importa?** Una respuesta rápida reduce pérdidas.
- **¿Cómo se presenta?** Media: X horas

Coste de los incidentes

- **¿Qué mide?** Impacto económico directo.
- **¿Por qué importa?** Traduce la seguridad a cifras de negocio.
- **¿Cómo se presenta?** Este trimestre: X euros.

5.3 Indicadores de preparación y capacidades

La capacidad de una organización para prevenir y responder a amenazas depende en gran medida de la preparación de su personal y de la robustez de sus sistemas. Medir indicadores relacionados con la formación, la eficacia de simulacros, el estado de las copias de seguridad y la protección de sistemas críticos permite evaluar el nivel de preparación ante incidentes y detectar áreas donde se debe reforzar la seguridad.

Estos datos facilitan la planificación de acciones que incrementen la resistencia frente a posibles ataques.[REF - 7]

Empleados formados en seguridad

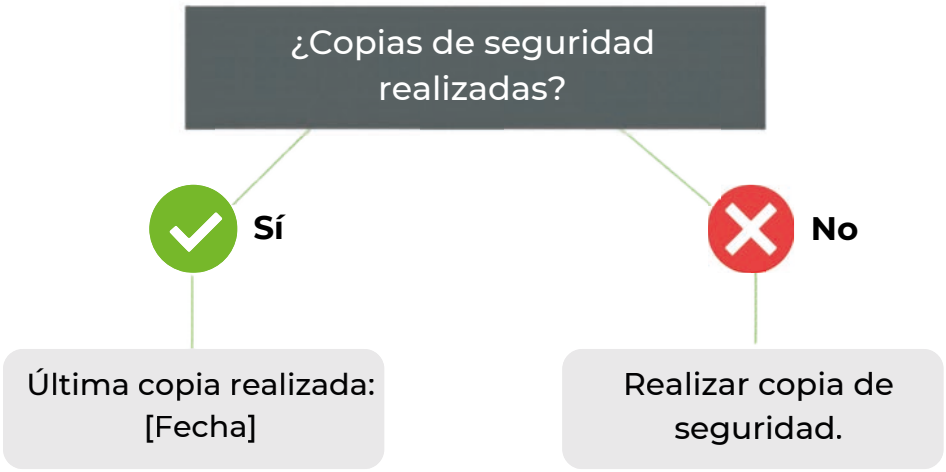
- **¿Qué mide?** Porcentaje de personal con formación actualizada.
- **¿Por qué importa?** La formación evita errores humanos.
- **¿Cómo se presenta?** El personal formado.

Simulacros de *phishing*

- **¿Qué mide?** Porcentaje de empleados que cayeron o no.
- **¿Por qué importa?** Indica si saben reconocer intentos de engaño.
- **¿Cómo se presenta?** Número que pasó el test correctamente.

Estado de las copias de seguridad

- **¿Qué mide?** Funcionamiento real de las copias.
- **¿Por qué importa?** Son clave en caso de desastre.
- **¿Cómo se presenta?** ¿Copias correctas?: Sí/No. Última prueba: [fecha].



Cobertura de sistemas críticos:

- **¿Qué mide?** Porcentaje de sistemas importantes bien protegidos.
- **¿Por qué importa?** Los sistemas sin protección son vulnerables.
- **¿Cómo se presenta?** Número de sistemas cubiertos con medidas adecuadas.

5.4 Indicadores de cumplimiento

Garantizar que la organización cumple con las normativas legales y regulatorias es una parte fundamental de la gestión de la ciberseguridad. Los indicadores de cumplimiento permiten verificar que se respetan las obligaciones establecidas, minimizando riesgos legales y mejorando la confianza de clientes y socios.

Además, el seguimiento regular de los accesos asegura que solo el personal autorizado tenga permiso para manejar información sensible, reduciendo posibles brechas de seguridad.[REF - 8]

Cumplimiento normativo

- **¿Qué mide?** Grado de cumplimiento legal y regulatorio.
- **¿Por qué importa?** Evita sanciones y mejora reputación.
- **¿Cómo se presenta?** Cumplimiento: X%. Próxima auditoría: [fecha].

Revisión de accesos

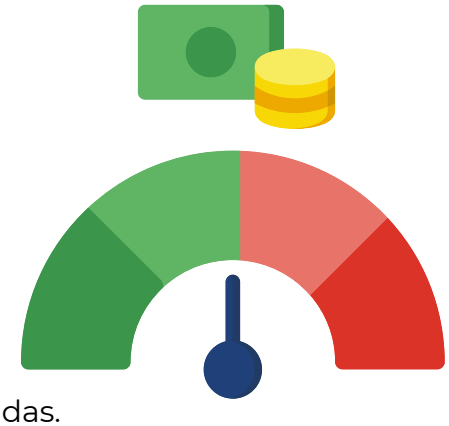
- **¿Qué mide?** Si se han actualizado permisos de acceso.
- **¿Por qué importa?** Accesos antiguos pueden generar fugas.
- **¿Cómo se presenta?** Última revisión: [fecha]. Próxima: [fecha].[REF - 9]

5.5 Indicadores financieros

La gestión financiera en ciberseguridad es clave para entender el valor de las medidas adoptadas. No basta con aplicar controles técnicos; también es necesario evaluar cómo se utilizan los recursos y el impacto económico de estas acciones.

Los indicadores financieros muestran cuánto se invierte, cuánto se ahorra al prevenir incidentes y cómo se reducen las interrupciones en la actividad diaria. Este enfoque ayuda a tomar decisiones acertadas, optimizar inversiones y demostrar que la seguridad aporta beneficios claros para la organización.[REF - 10]

Inversión en seguridad versus presupuesto



- **¿Qué mide?** Lo gastado frente a lo planificado.
- **¿Por qué importa?** Permite ajustar inversiones.
- **¿Cómo se presenta?** Gastado: X€ de Y€.

Retorno de la Inversión en Seguridad (ROI)

- **¿Qué mide?** Ahorro generado gracias a las medidas aplicadas.
- **¿Por qué importa?** Muestra que la seguridad también da beneficios.
- **¿Cómo se presenta?** Cada 1€ invertido ahorra X€ en daños evitados.

Coste de inactividad evitada

- **¿Qué mide?** Dinero ahorrado al evitar paradas del negocio.
- **¿Por qué importa?** Refleja valor real de la protección.
- **¿Cómo se presenta?** Evitadas X horas de inactividad: Y€ ahorrados.

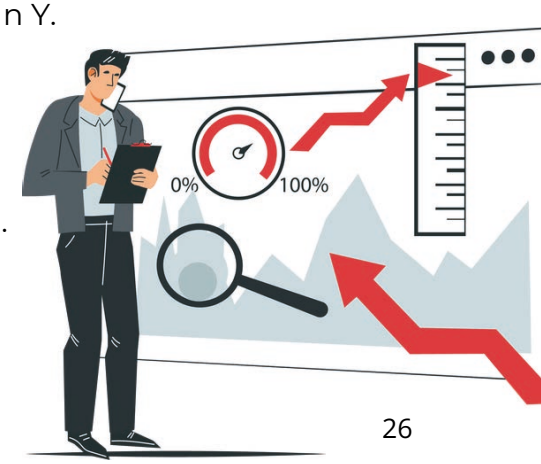
5.6 Indicadores de tendencias

Los indicadores de tendencias ofrecen una **visión dinámica sobre cómo evolucionan las amenazas y el nivel de madurez en la gestión de la ciberseguridad** dentro de la organización. Analizar estos cambios permite anticiparse a nuevos riesgos y evaluar el progreso en las medidas de protección adoptadas. Esta información es clave para ajustar estrategias y mantener un enfoque proactivo frente a un entorno de amenazas en constante transformación.

Evolución de amenazas

- **¿Qué mide?** Cambios en los tipos de ataque.
- **¿Por qué importa?** Permite prepararse frente a lo nuevo.
- **¿Cómo se presenta?** Los ataques de tipo X subieron un Y.

Madurez de seguridad



- **¿Qué mide?** Progreso en la gestión de ciberseguridad.
- **¿Por qué importa?** Indica si se está avanzando.
- **¿Cómo se presenta?** Escala 1–5: Hoy: X/5. Antes: Y/5.

5.7 Cómo presentar la información

La presentación de información ejecutiva se enfoca en entregar los datos que realmente importan, de manera que los líderes puedan actuar sin perder tiempo en detalles innecesarios. Un *dashboard* o **cuadro de resultados ejecutivo** utiliza códigos visuales como semáforos de riesgo para identificar rápidamente áreas que requieren atención. Los gráficos deben ser simples y claros, con números grandes que destaquen los puntos más importantes y comparaciones con el mes anterior para mostrar si la situación mejora o empeora.

El **informe mensual** complementa el *dashboard*, condensando en una sola página los riesgos más relevantes y las mejoras logradas, lo que ayuda a mantener un seguimiento constante y ordenado. Además, debe incluir un plan de acción claro, orientando a los responsables sobre los próximos pasos. [REF - 11]

Las **alertas inmediatas**, por otro lado, sirven para comunicar problemas urgentes. Estas alertas deben ser directas y contener tres elementos: qué está pasando, qué impacto tiene, y qué se está haciendo para resolverlo, además de un tiempo estimado para la solución.

Finalmente, para que la información sea realmente útil, se deben formular **preguntas clave** que ayuden a interpretar los datos en contexto y guiar la toma de decisiones: ¿Estamos avanzando? ¿Cómo afecta esto a nuestro negocio? ¿Qué medidas inmediatas se requieren? ¿Cuál será el coste de la situación?

Este enfoque garantiza que la **información ejecutiva sea comprensible, accionable y relevante.**

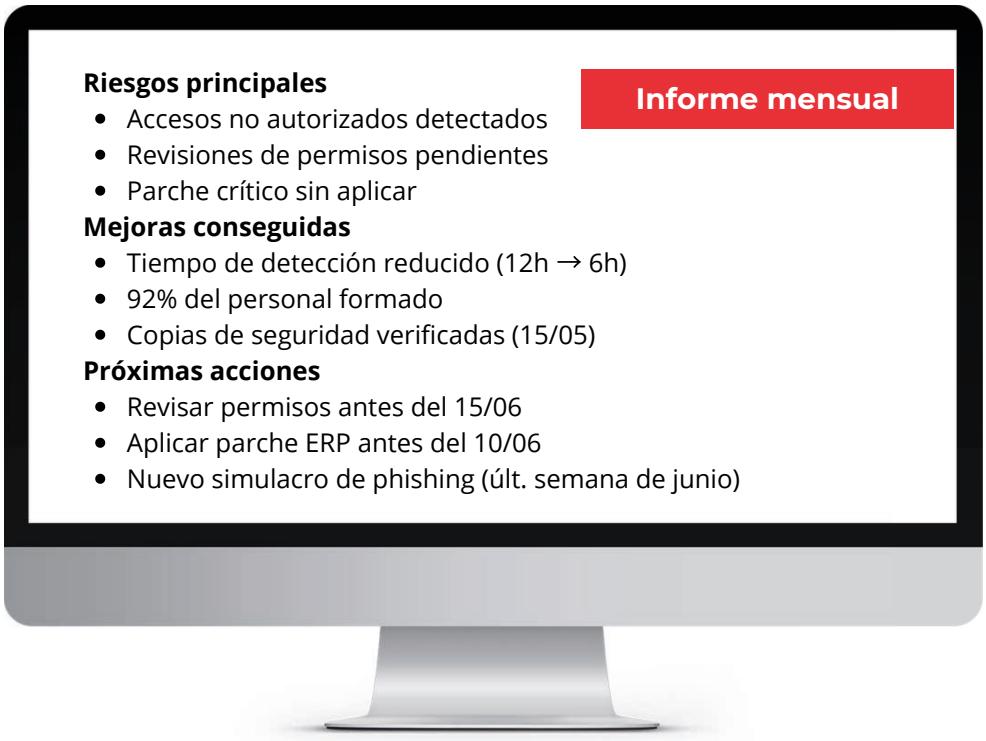
Dashboard ejecutivo

- **Semáforos de riesgo:** muestran qué áreas están en situación crítica, moderada o estable.
- **Gráficos simples:** permiten entender tendencias sin complicaciones.
- **Números grandes:** destacan datos clave como número de incidentes o nivel de cumplimiento.
- **Comparación con el mes anterior:** ayuda a saber si se mejora o empeora.

Informe mensual

Documento que resume lo más relevante del mes en ciberseguridad. Este informe facilita el seguimiento continuo y ayuda a priorizar acciones de forma ordenada. Incluye:

- Los **3 riesgos más importantes** detectados o activos.
- Las **3 mejoras conseguidas** en protección, detección o respuesta.
- **Próximos pasos** recomendados para reducir riesgos o consolidar avances.

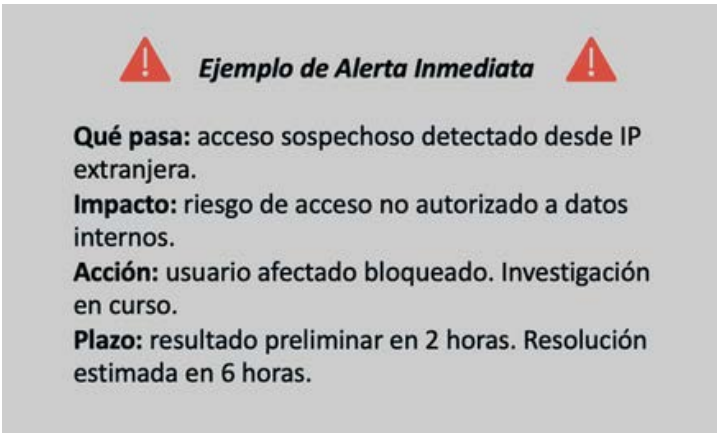


Alertas inmediatas

Mensajes breves que informan sobre incidentes urgentes de ciberseguridad. Permiten actuar con rapidez y claridad.

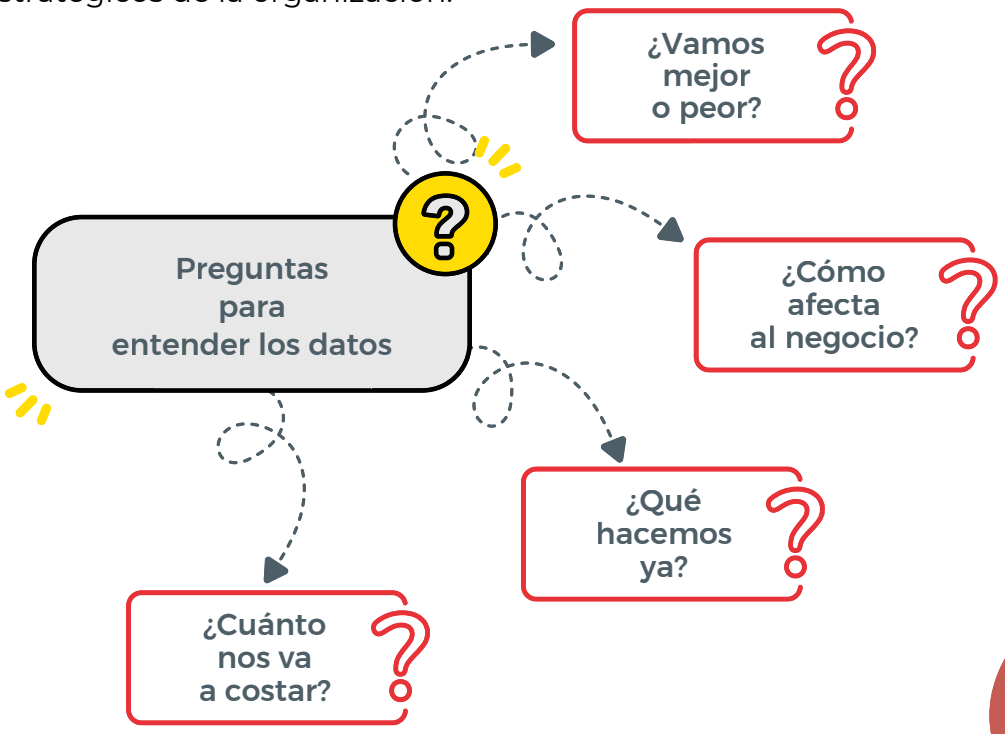
Contenido clave de la alerta:

- **Qué pasa**: descripción rápida del incidente.
- **Impacto**: riesgos si no se actúa.
- **Acción**: qué se está haciendo.
- **Plazo**: cuándo se resolverá.



Preguntas para entender los datos

Son preguntas clave que ayudan a interpretar los indicadores de ciberseguridad y a tomar decisiones informadas desde una perspectiva de negocio. **Ayudan a transformar datos técnicos en acciones concretas**, alineadas con los objetivos estratégicos de la organización.



6. Recomendaciones para mejorar la supervisión

6.1 Comunicación y participación activa de la dirección

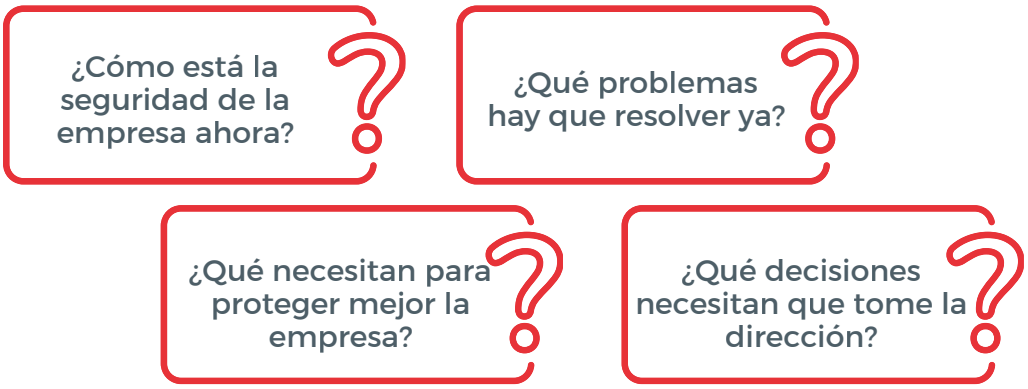
Los directivos no deben limitarse a esperar informes técnicos sobre ciberseguridad. Es fundamental que mantengan un **diálogo constante** con los equipos especializados, solicitando explicaciones claras y accesibles que les permitan comprender los riesgos de manera adecuada. La implicación activa de la alta dirección en la toma de decisiones estratégicas no solo facilita una mejor comprensión del panorama de amenazas, sino que contribuye de forma decisiva a la adopción de medidas eficaces para proteger la organización.

Para lograrlo, es importante que haya una comunicación clara, con un lenguaje sencillo y con la información adecuada para todos.

Fomentar el diálogo con el área técnica, solicitar informes en lenguaje accesible y participar en revisiones de seguridad permite a la dirección mantenerse informada y tomar decisiones con criterio.

Reunirse con el equipo técnico permite compartir información y tomar mejores decisiones. No es solo cuestión de recibir datos, sino de hablar, resolver dudas juntos y asegurarse de que todos trabajen con los mismos objetivos.

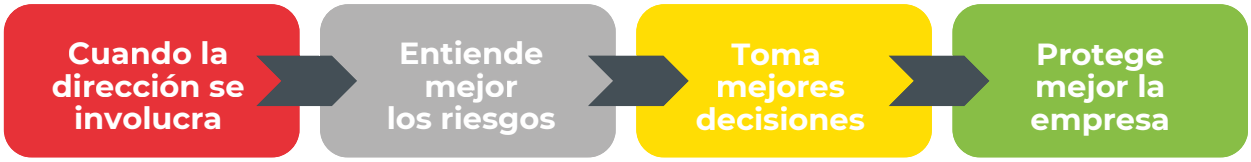
Lo recomendable es reunirse una vez por semana o, como mínimo, cada dos semanas. La frecuencia dependerá del tamaño del equipo, la carga de trabajo y la situación actual (por ejemplo, si hay una incidencia en curso, puede ser necesario reunirse más a menudo).



6.1.1 ¿Por qué es importante?

La seguridad informática no es solo responsabilidad del equipo técnico. Afecta directamente al funcionamiento del negocio, la confianza de los clientes y la imagen de la organización. Por eso, los directivos no pueden limitarse a recibir informes: tienen que estar presentes y participar.[REF - 12]

- **Hablar regularmente con el equipo técnico**: mantener una comunicación continua ayuda a entender mejor los riesgos, anticiparse a problemas y tomar decisiones con más criterio.
- **Pedir explicaciones en palabras sencillas**: no hace falta entender los detalles técnicos, pero sí comprender las consecuencias. Pedir que se explique todo de forma clara permite tomar decisiones sin perderse en tecnicismos.
- **Participar activamente en decisiones importantes**: la seguridad tiene implicaciones estratégicas y económicas. Estar presente en las decisiones clave garantiza que se actúe con visión de conjunto y no solo desde lo técnico.[REF - 13]



6.1.2 Informes fáciles de entender

Una de las barreras más frecuentes entre el equipo técnico y la dirección es la forma en la que se comunican los temas relacionados con la ciberseguridad. Informes largos, cargados de tecnicismos o listas interminables de vulnerabilidades no ayudan a tomar decisiones. Lo que se necesita son **informes comprensibles, directos y enfocados en el impacto real sobre el negocio**.

Para ello, proponemos una **estructura sencilla, útil y eficaz**, que permita a los directivos entender en pocos minutos qué está pasando, qué se ha hecho y qué deben decidir. No se trata sólo de informar, sino de facilitar la acción.

Resumir la ciberseguridad con sentido

El objetivo de esta sección es ofrecer una fotografía general de la situación actual en materia de seguridad. Se recomienda usar indicadores visuales simples, como un sistema de colores que indique el nivel de riesgo o estabilidad:

- **Bien**: no se han detectado amenazas significativas ni brechas. Las medidas de protección están funcionando correctamente.
- **Atención**: hay elementos que requieren seguimiento o mejoras, pero no suponen un riesgo inmediato.
- **Problema**: se ha detectado una amenaza relevante, una vulnerabilidad crítica o una brecha que puede tener consecuencias directas sobre la actividad.

Este resumen debe leerse relativamente rápido y dejar claro si todo que partes están bajo control o si hay que tomar medidas correctivas. Se recomienda que la información se plasme de manera visual, sencilla, sintetizada y rápida de consultar (uso de colores, conclusiones, medidas, etc.), cuanto más visual, más fácil de asimilar.

Decir lo importante, sin complicarlo

En lugar de listar vulnerabilidades técnicas, es más eficaz destacar los riesgos más relevantes desde el punto de vista empresarial. Para cada uno de ellos, hay que responder a tres preguntas:

- **¿Qué puede pasar?** → Describir el escenario de forma comprensible. Ejemplo: "Un fallo en el control de accesos podría permitir que alguien ajeno acceda a información de clientes."
- **¿Qué impacto tendría?** → Poner cifras o consecuencias claras: "Esto supondría una posible multa de 50.000 €, además de pérdida de confianza y reputación."
- **¿Cómo de probable es?** → Estimar si es un riesgo puntual, recurrente o crítico.

No se trata de generar alarma, sino de ayudar a priorizar. Cuanto más conectada esté la explicación con el negocio (costes, reputación, continuidad de servicios), mayor será la capacidad de la dirección para tomar decisiones.

Cómo explicar los riesgos (sin tecnicismos)

Es igual de relevante comunicar lo que se ha conseguido. Este apartado refuerza la idea de avance, esfuerzo y utilidad del trabajo técnico.

Cada mejora debe explicarse así:

- **¿Qué hemos hecho?** → Por ejemplo: "Hemos actualizado el sistema de correo para filtrar mejor los correos maliciosos."
- **¿Qué resultado ha tenido?** → "Ahora se bloquean más del 95 % de intentos de phishing."
- **¿Qué gana la empresa con ello?** → "Menos riesgo de suplantación de identidad o de robo de información sensible."

Este enfoque positivo también ayuda a justificar inversiones y a visibilizar el trabajo del equipo de seguridad.[REF - 14]

Informes que ayudan a decidir

Aquí se expone de forma clara qué decisiones deben tomarse y por qué. No se trata de presentar opciones técnicas, sino de definir escenarios que requieren una decisión empresarial. Este apartado debe incluir:

- **Acciones pendientes que requieren aprobación** → "Hay que decidir si externalizamos el sistema de backups o si se amplía el servidor actual."
- **Recursos necesarios** → "Se necesita un presupuesto de 12.000 € para implantar esta solución antes de que acabe el trimestre."
- **Justificación breve** → "Retrasar esta decisión nos deja expuestos a un tipo de ataque que ya ha afectado a tres empresas del sector, y que conllevaría estas repercusiones."

6.1.3 Preguntas que debe hacerse la dirección

Para que la ciberseguridad no sea un asunto aislado ni ajeno a las decisiones estratégicas, la dirección debe implicarse activamente. No se espera que conozca los detalles técnicos, pero sí que haga las preguntas adecuadas en el momento oportuno.

A continuación, se presentan preguntas clave que la dirección puede usar en distintos contextos. Su objetivo es entender mejor los riesgos, valorar el impacto en el negocio y facilitar la toma de decisiones informadas.

En **reuniones habituales**: estas preguntas sirven para mantenerse informado y al tanto de lo realmente relevante:

- ¿Cuáles son nuestros 3 problemas de seguridad más graves? para centrarse en lo prioritario y no perderse en detalles menores.
- ¿Cuánto nos costaría si pasa algo malo? traducir el riesgo a términos económicos o reputacionales ayuda a valorar su impacto.
- ¿Qué opciones tenemos para solucionarlo y cuánto cuestan? conocer posibles soluciones permite decidir con criterio, evaluando coste y beneficio.
- ¿Qué está impidiendo que mejoremos la seguridad? a veces no es cuestión técnica, sino de falta de recursos, decisiones o coordinación.
- ¿Qué necesitas que decida yo? una forma directa de facilitar el trabajo técnico y evitar bloqueos por falta de respuesta.

Cuando se inicia un proyecto nuevo: cada nuevo sistema, servicio o cambio tecnológico puede traer consigo nuevos riesgos. Estas preguntas ayudan a anticiparlos:

- ¿Este proyecto nuevo crea algún riesgo de seguridad? para no introducir vulnerabilidades sin darnos cuenta.
- ¿Qué medidas de seguridad hay que añadir? la seguridad debe integrarse desde el inicio, no al final del proyecto.
- ¿Cuánto dinero y tiempo extra necesitamos? invertir a tiempo evita problemas más caros después.
- ¿Qué riesgos corremos si no hacemos nada? permite valorar si aplazar una medida tiene consecuencias serias.

En caso de crisis o incidente de seguridad: ante un incidente, las decisiones deben ser rápidas y bien fundamentadas. [REF - 15] Estas preguntas ayudan a gestionar la situación con claridad:

- ¿Qué sabemos seguro de lo que está pasando? separar hechos de suposiciones es vital en las primeras horas.
- ¿Qué opciones tenemos y qué consecuencias? conocer escenarios y posibles impactos permite decidir con rapidez.
- ¿A quién tenemos que avisar? puede incluir clientes, socios, autoridades, o el equipo de comunicación.
- ¿Qué les decimos a los clientes? la gestión de la comunicación es tan importante como la resolución técnica.

6.1.4 Participación activa de la dirección

La ciberseguridad no puede delegarse por completo en el equipo técnico. La dirección no debe actuar solo cuando hay un problema. Participar de forma constante ayuda a prevenir riesgos, tomar mejores decisiones y fomentar un entorno donde la seguridad sea parte del trabajo diario.

Revisión cada 3 meses: cada trimestre, la dirección debe dedicar un tiempo específico a revisar el estado general de la seguridad:

- Ver el mapa de riesgos de la empresa: un resumen visual que muestra los principales riesgos detectados, clasificados por nivel de impacto y probabilidad.
- Entender qué problemas afectan más al negocio: traducir los aspectos técnicos a consecuencias reales: pérdida de datos, multas, impacto en la reputación o en los ingresos.
- Decidir qué riesgos podemos asumir: no todos los riesgos se pueden eliminar. Algunos deben asumirse, pero de forma consciente y controlada.
- Priorizar en qué gastar el dinero de seguridad: la inversión debe centrarse en lo más crítico y no repartirse de forma genérica o por costumbre.

Aprobar normas de seguridad: las normas no son solo documentos internos. Definen cómo se trabaja en el día a día y deben tener el respaldo de la dirección:

- Entender qué reglas se van a poner: no basta con firmarlas: hay que saber qué implican, a quién afectan y por qué se proponen.
- Asegurarse de que son aplicables en la realidad: las normas deben poder cumplirse. Si no se adaptan al trabajo diario, caerán en desuso o se ignorarán.
- Ver cómo afectan al trabajo diario: ¿Cambian procesos? ¿Obligan a nuevas herramientas? La dirección debe valorar el impacto operativo.

Dar ejemplo cumpliendo las normas: si la dirección no cumple lo que exige a los demás, el mensaje se debilita. El ejemplo arrastra más que cualquier manual.

- Simulacros una vez al año: igual que en emergencias físicas, también es necesario entrenar qué hacer ante una crisis digital:
- Practicar qué hacer en una crisis: simular un ataque o filtración permite detectar fallos en la reacción.
- Aprender a tomar decisiones rápidas: en situaciones reales hay que decidir sin tener toda la información. Practicar ayuda a reducir errores.
- Saber a quién avisar y cómo: comunicación interna, autoridades, clientes... Todo debe estar claro de antemano.
- Mejorar los procedimientos: tras cada simulacro se detectan puntos débiles y se ajustan los protocolos para mejorar la respuesta futura.

6.1.5 Formas de enfocar la ciberseguridad

En las organizaciones, la ciberseguridad se puede abordar de dos maneras muy diferentes: **de forma activa y colaborativa, o de forma pasiva y reactiva**. El primer enfoque permite anticiparse a los riesgos y tomar decisiones bien informadas. El segundo, en cambio, deja a la empresa expuesta, confiando únicamente en informes técnicos que llegan cuando ya hay un problema.

A continuación, se muestra una comparación clara entre ambos estilos de gestión:

Antes		Después
Esperar informes técnicos	→	Reuniones regulares
No entender los riesgos	→	Explicaciones en lenguaje de negocio
Decisiones sin información	→	Preguntas clave respondidas
Equipo técnico aislado	→	Comunicación fluida
Reaccionar a crisis	→	Prevenir problemas

7. Comunicación y participación activa de la dirección en ciberseguridad

Los directivos no pueden quedarse esperando informes sobre seguridad informática. Necesitan hablar regularmente con su equipo técnico, pedirles que expliquen los problemas en palabras sencillas, y participar en las decisiones importantes. Cuando la dirección se implica, todo funciona mejor.

Entender los riesgos y hablar con claridad ayuda a decidir bien y a proteger la empresa. Lo importante es que todos se entiendan y trabajen en la misma dirección.

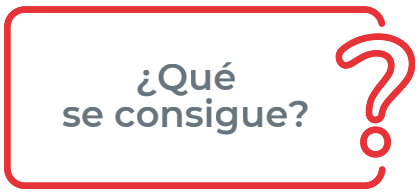
7.1 Fomentar el diálogo con el equipo técnico

La dirección debe mantener una relación fluida con el equipo técnico. Para ello, conviene usar un lenguaje sin tecnicismos y crear espacios donde ambas partes puedan intercambiar ideas, problemas y propuestas.

Hablar claro ayuda a entendernos mejor. Cuando se evitan los tecnicismos y se usan ejemplos sencillos, es más fácil que todos estén en la misma página y se tomen decisiones acertadas.

Además de reuniones formales, pueden establecerse canales informales o dinámicas de trabajo colaborativo (como talleres, mesas redondas o sesiones de intercambio) que favorezcan el entendimiento mutuo y el trabajo conjunto en la toma de decisiones.

Cuando la dirección y el equipo técnico trabajan codo con codo, los resultados hablan por sí mismos. A continuación, se presentan los principales beneficios que se obtienen al mantener un diálogo constante, claro y orientado a la acción:



- Mejor toma de decisiones
- Mayor rapidez al actuar ante riesgos
- Un equipo técnico más motivado
- Menos malentendidos y más confianza

7.2 Solicitar informes en lenguaje accesible

Los informes de seguridad no deben ser complicados ni llenos de términos técnicos que solo entienden los expertos. Los informes deben ser claros y fáciles de leer.
No todo el mundo tiene formación técnica, pero todos deben entender qué está pasando. Si la información se presenta bien, la dirección puede actuar rápido y con criterio.

Un buen informe muestra lo esencial, incluye un resumen con los puntos clave y marca las prioridades. Si además se usan colores o símbolos sencillos para mostrar el nivel de riesgo, mucho mejor.

Ver cómo ha cambiado la situación desde el último informe permite saber si se avanza o si hay que corregir algo. Sin esa comparación, no se puede medir el progreso ni ajustar bien las decisiones. Así, se pueden detectar tendencias y actuar antes de que surjan problemas mayores.

A continuación, una tabla con el semáforo de riesgos que ayuda a visualizar de un vistazo el estado de la seguridad en la empresa:

Color	Estado	Significado
	Situación estable	Todo funciona correctamente
	Riesgos detectados	Riesgos sin impacto grave
	Incidente grave	Problemas con consecuencias reales

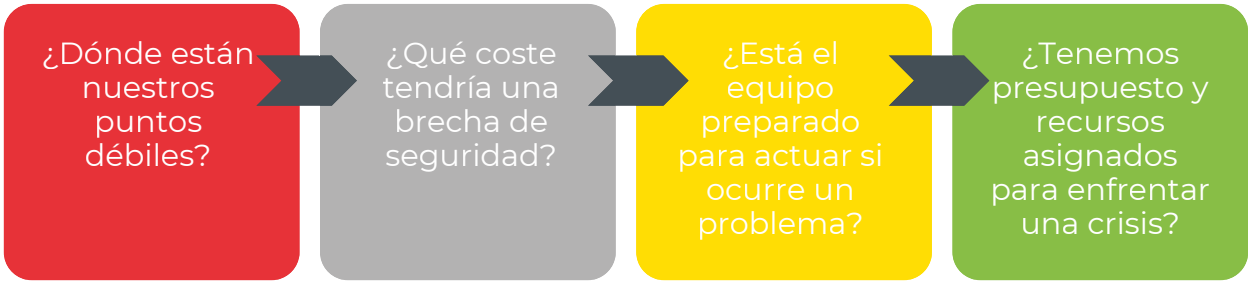
7.3 Participar en revisiones de seguridad

La participación de la dirección en temas de seguridad no implica que deba conocer detalles técnicos, como revisar código o configurar sistemas.

No hace falta saber de ciberseguridad, pero sí tener criterio para decidir qué riesgos se pueden asumir y cuáles no. También hay que saber en qué conviene invertir el dinero para que la empresa esté más protegida.

Las **políticas de seguridad** no deben quedarse solo en manos del equipo técnico. La dirección tiene que validarlas y asegurarse de que encajan con la forma de trabajar de la empresa.[REF - 16]

Aunque no se participe en los detalles, conviene estar informado sobre los simulacros y ejercicios. Así se sabe si todo funciona como debe cuando ocurre un problema real. Para ayudar a la dirección a tomar decisiones claras, es útil plantearse estas preguntas clave:



7.4 Crear una cultura de seguridad desde arriba

Las personas imitan lo que ven. Si quienes dirigen la organización no siguen las normas de seguridad, el resto del equipo tampoco lo hará. Por eso, es clave que la dirección dé ejemplo y muestre que proteger la información es algo serio.

Qué puede hacer la dirección:

- **Hablar de seguridad en reuniones importantes**: no hay que esperar a que ocurra un problema. Igual que se revisan las cuentas o los objetivos del año, también debe comentarse cómo está la empresa en temas de protección digital: si hay riesgos, si hay que mejorar algo o si todo va bien.

- **Reconocer el trabajo preventivo**: cuando alguien del equipo toma medidas para evitar problemas, conviene destacarlo. Agradecer estos esfuerzos refuerza la idea de que la prevención tiene valor, aunque no se vea.

- **Marcar objetivos claros cada año**: la seguridad debe tener un sitio en los planes de la empresa. Por ejemplo: hacer dos simulacros, formar al equipo, actualizar los equipos, revisar accesos... Así no se deja para "cuando haya tiempo".

- **Cumplir las normas como todos**: si hay reglas para proteger datos, hay que cumplirlas desde arriba. Si se pide usar contraseñas seguras o no conectar dispositivos personales, la dirección debe hacerlo igual. El ejemplo arrastra más que las órdenes.

- **Seguir aprendiendo**: no es necesario saber de informática, pero sí entender cómo afectan los riesgos digitales al negocio. Con unas cuantas sesiones al año o leyendo breves resúmenes, la dirección puede tomar decisiones más acertadas. [REF - 17]

7.5 Beneficios para todos

Una implicación activa ayuda a tomar decisiones más acertadas y a invertir el presupuesto justo en lo que realmente importa, sin gastar de más.

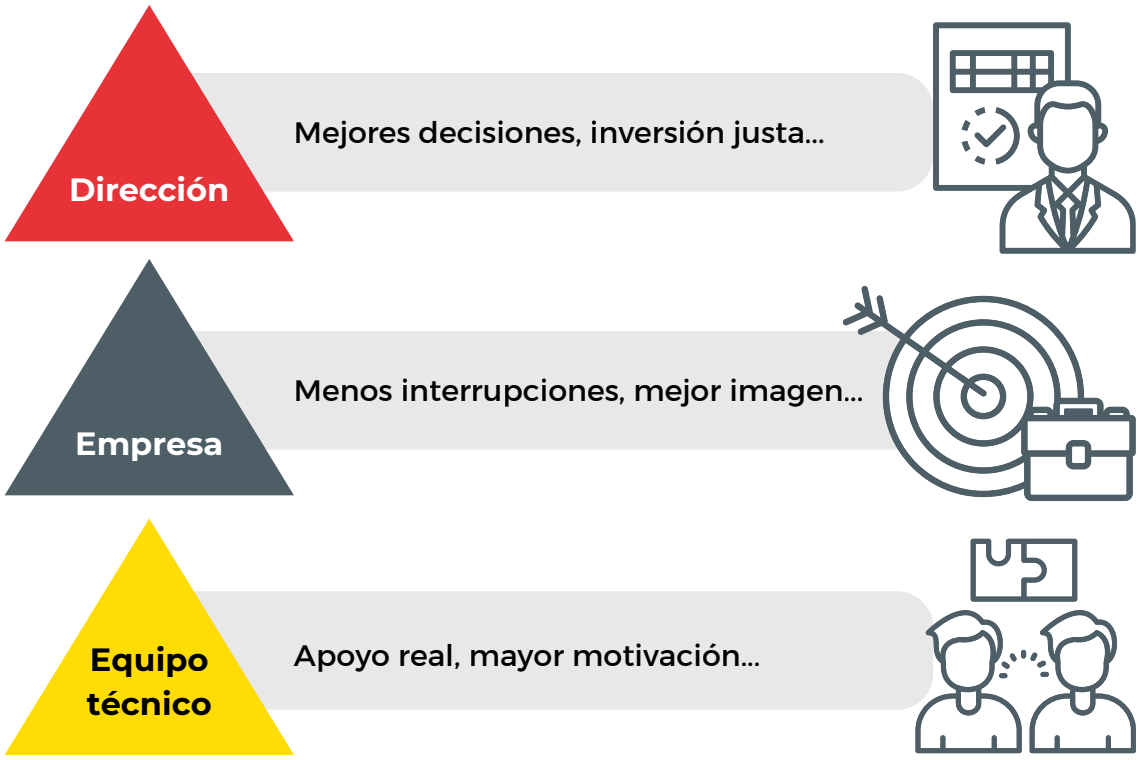
Con una seguridad bien gestionada hay menos interrupciones y se trabaja con más tranquilidad. Además, la confianza de clientes y colaboradores crece, y eso mejora la imagen del negocio.

Contar con el respaldo de la dirección permite trabajar mejor. Hay menos obstáculos, más recursos y más claridad en lo que se espera de cada uno. Esto eleva la motivación y el compromiso, al saber que sus esfuerzos cuentan y que no están trabajando aislados. [REF - 18]

Cuando la dirección participa activamente en la seguridad, se generan **beneficios** que alcanzan a toda la organización.

- **Para la dirección**: estar informada y participar activamente permite decidir mejor dónde invertir. Así se evitan gastos que no aportan valor y se protege lo que realmente lo necesita.
- **Para la empresa**: una gestión eficaz reduce los fallos, evita interrupciones y mantiene el negocio en marcha. También refuerza la confianza de quienes trabajan contigo y mejora la imagen que das hacia fuera.
- **Para el equipo técnico**: cuando cuentan con el apoyo real de la dirección, el equipo se siente valorado y respaldado. Esto aumenta su motivación y facilita que trabajen con más eficiencia, sin la sensación de estar solos frente a los retos de seguridad.

La siguiente imagen muestra que cuando la dirección se involucra, no solo mejora su propia gestión, sino que también fortalece la empresa y crea un entorno positivo para el equipo técnico:



7.6 Promover hábitos seguros diarios

La ciberseguridad,. como ya hemos visto, no se limita a instalar programas, sistemas o medidas técnicas. Se trata de una forma de trabajar y de pensar dentro de toda la organización. Por muy avanzadas que sean las herramientas tecnológicas, si las personas no adoptan comportamientos adecuados, los riesgos seguirán existiendo.

Por eso es tan relevante crear una cultura de seguridad que incluya a todas las personas de la empresa, sin importar su función. Promover hábitos seguros significa integrar en la rutina diaria pequeñas acciones que marcan una gran diferencia: proteger las contraseñas, comprobar si un correo es sospechoso antes de abrirlo, no conectar dispositivos externos sin autorización o preguntar cuando se duda ante algo fuera de lo normal.[REF - 19]

Adoptar buenos hábitos no es una carga extra, sino parte del trabajo bien hecho. La dirección puede reforzar esta idea con gestos sencillos: recordar buenas prácticas en las reuniones, reconocer públicamente el comportamiento responsable y dejar claro que la ciberseguridad es asunto de todos.

Con el tiempo, esta actitud compartida reduce errores, mejora la respuesta ante incidentes y hace que toda la organización esté mejor protegida. En definitiva, convierte la ciberseguridad en algo natural, no impuesto.

7.7 Formación diferenciada por perfil

No todas las personas dentro de la organización necesitan saber lo mismo sobre seguridad digital. Según el tipo de trabajo que realizan, hay aspectos más útiles o más relevantes que otros. Por eso, conviene adaptar la formación al perfil de cada grupo: plantilla general, dirección y personal técnico.

Conviene centrarse en los errores más habituales: reconocer correos falsos, compartir información con seguridad o evitar repetir contraseñas. Si todos saben qué no hacer, muchos riesgos diarios desaparecen.[REF - 20]

- Para la **dirección**, entender el impacto. No es necesario profundizar en lo técnico, sino comprender cómo un fallo afecta la reputación o el funcionamiento del negocio. Así pueden decidir qué riesgos aceptar y cuáles evitar.

- Para el **equipo técnico**, comunicación y colaboración. Deben contar con herramientas para explicar los riesgos sin tecnicismos y saber priorizar según el impacto. También es clave que trabajen en equipo con otros departamentos, evitando aislarse.

Así, cada persona puede actuar con más confianza y contribuir a un entorno más protegido, sin necesidad de convertirse en especialista.

Así, cada persona puede actuar con más confianza y contribuir a un entorno más protegido, sin necesidad de convertirse en especialista.

Perfil	¿Qué necesita aprender?	¿Para qué sirve?
Toda la plantilla	Reconocer correos falsos No compartir contraseñas Reglas básicas de seguridad	Evitar errores comunes que pueden causar incidentes
Dirección	Impacto de una brecha en la empresa Qué decisiones tomar Cómo actuar ante crisis	Tomar decisiones con criterio y proteger la reputación
Personal técnico	Explicar riesgos de forma clara Priorizar por impacto Coordinarse con otros equipos	Comunicar mejor y alinear la seguridad con los objetivos

8. Conclusiones

9. Referencias

[REF - 1]	INCIBE – Empresas – Guía: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_gestion_de_crisis.pdf
[REF - 2]	INCIBE – Empresas – Guía: https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf
[REF - 3]	INCIBE – Empresas – Guía: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_metad.pdf
[REF - 4]	INCIBE – Empresas – Blog: https://www.incibe.es/empresas/blog/amenaza-vs-vulnerabilidad-diferenciarlos
[REF - 5]	INCIBE – Empresas – Blog: https://www.incibe.es/empresas/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian
[REF - 6]	INCIBE – Empresas – Guía: https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan-director-seguridad.pdf
[REF - 7]	INCIBE – INCIBE-CERT – Guía: https://www.incibe.es/sites/default/files/contenidos/guias/IMC/imc_01_metodologia-evaluacion.pdf
[REF - 8]	INCIBE – Empresas – Guía: https://www.incibe.es/sites/default/files/contenidos/dosieres/Actualizado_Cumplimiento%20Legal_2024.pdf

[REF - 9]	INCIBE – Empresas – Política: https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/control-de-acceso.pdf
[REF - 10]	INCIBE – Empresas – Blog: https://www.incibe.es/empresas/blog/como-reducir-el-impacto-financiero-de-los-incidentes-de-ciberseguridad
[REF - 11]	INCIBE – Empresas – Infografía: https://www.incibe.es/empresas/que-te-interesa/proteccion-informacion
[REF - 12]	INCIBE – Empresas – Guía: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_gestion_de_crisis.pdf
[REF - 13]	INCIBE – Empresas – Guía: https://www.incibe.es/sites/default/files/contenidos/guias/doc/ciberamenazas_contra_entornos_empresariales.pdf
[REF - 14]	INCIBE – Empresas – Blog: https://www.incibe.es/empresas/blog/cumples-con-el-rgpd-aprende-hacerlo-con-esta-guia
[REF - 15]	INCIBE – Empresas – Blog: https://www.incibe.es/empresas/blog/proteger-informacion-personal-los-clientes-empresa
[REF - 16]	INCIBE – Empresas – Política: https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/cumplimiento-legal.pdf
[REF - 17]	INCIBE – Empresas – Dosier: https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_desarrollar-cultura-en-seguridad.pdf

[REF - 18]	INCIBE – Empresas – Infografía: https://www.incibe.es/empresas/que-te-interesa/desarrollar-cultura-en-seguridad
[REF - 19]	INCIBE – Empresas – Blog: https://www.incibe.es/empresas/blog/los-habitos-pyme-ciberresiliente
[REF - 20]	INCIBE – Empresas – Blog: https://www.incibe.es/empresas/blog/dudas-legitimidad-correo-aprende-identificarlos

GUÍA DE SUPERVISIÓN DE CIBERSEGURIDAD PARA DIRECTIVOS NO TÉCNICOS

Recomendaciones para empresas

Contacto

INCIBE
Instituto Nacional de Ciberseguridad
Avenida José Aguado 41, 24005 León

https://www.incibe.es
empresas@incibe.es
@incibe

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA · MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA · SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD