MINERY REPORT

EVALÚA · INFORME DE EJEMPLO · EMPRESA FICTICIA

Informe de ciberseguridad

Distribuciones Ejemplo, S. L. (empresa ficticia)

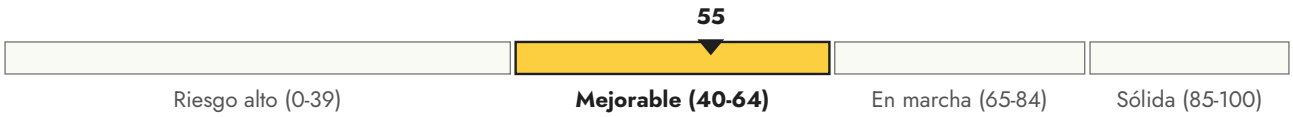
20 de octubre de 2026

Nivel orientativo

Mejorable

Tienes parte de lo básico, pero quedan huecos que un atacante o un cliente exigente encontrarían.

Has contestado las 25; 1 con «No lo sé».



Contenido

Resumen para dirección 2
De un vistazo 4
Hasta dónde llega este test 4
Para dirección 5
Qué hacer, punto por punto 7
Lo que ya haces bien 13
Plan de 90 días 14
Para tu equipo técnico 15
Cómo se calcula y alcance 16

Autoevaluación orientativa basada en tus respuestas: no es una auditoría ni una certificación. La puntuación no es una probabilidad de sufrir un incidente.

01 Resumen para dirección

Lo esencial en una página.

55
de 100
Nivel orientativo: Mejorable

4 ⚠
imprescindibles por resolver
De los 7 puntos imprescindibles

13 ⚡
tareas de esfuerzo bajo
Hasta 2 jornadas cada una. No hace falta hacerlas todas este trimestre.

6
ya bien resueltos
De 25 puntos

Has contestado las 25; 1 con «No lo sé». No es una auditoría ni una certificación. La puntuación no es una probabilidad de sufrir un incidente. Puntuación según tus respuestas: 55 de 100. Con lo que se ve desde fuera: 55 de 100. El contraste disponible no cambia la puntuación.

Resultado por tema

1. Gobierno: quién decide y responde	**64 de 100**
2. Saber qué tienes	**50 de 100**
3. Quién entra y cómo	**86 de 100**
4. Equipos protegidos y al día	**43 de 100**
5. Correo, pagos y presencia en Internet	**50 de 100**
6. Recuperarte si te paran	**56 de 100**
7. Detectar y responder	**57 de 100**
8. Personas y proveedores	**20 de 100**

Los 3 huecos que conviene cerrar primero

1. **Responsable y seguimiento de la dirección** — **Imprescindible**
   Falta una de las dos piezas: un responsable con el encargo por escrito o una revisión de la dirección con fecha. Sin las dos, el seguimiento depende de la buena voluntad y es difícil de demostrar ante un cliente. Nos dijiste: «Hay responsable designado, pero la dirección no lo revisa al menos una vez al año».

2. **Protección contra programas maliciosos** — **Imprescindible**
   Un equipo sin protección o sin vigilancia central puede ser la entrada de un secuestro de datos sin que nadie vea la alerta. Nos dijiste: «En casi todos, o nadie mira las alertas».

3. **Actualizaciones** — **Imprescindible**
   Sin plazo ni control, un fallo que el fabricante ya ha corregido puede seguir abierto semanas sin que lo sepas. Nos dijiste: «Se instalan, pero sin plazo ni control».

También: cambios de cuenta bancaria. Si la comprobación depende de quién reciba el correo, un cambio de cuenta falso puede colarse el día que no se hace. Lo has contestado así: «A veces, o depende de quién lo reciba».

Tus 3 decisiones para este trimestre

1. **Completar lo que falta (el encargo escrito o la revisión de dirección) y llevar a dirección un informe breve con riesgos, incidentes y plan**
   Esfuerzo: Bajo (hasta 2 jornadas) · Quién: Dirección

2. **Definir con dirección los tiempos máximos de parada de los 3-5 procesos clave y un plan mínimo**
   Esfuerzo: Medio (3-10 jornadas) · Quién: Dirección, TI

3 **Convertirla en un paso obligatorio del alta de cuentas en el sistema de pagos**
Esfuerzo: Bajo (hasta 2 jornadas) · Quién: Dirección, TI

02 De un vistazo

Tus 25 respuestas, por temas. Cada casilla dice cómo está ese punto.

Bien · Parcial · Sin cubrir · Sin confirmar

1. Gobierno: quién decide y responde 64 de 100	Responsable y seguimiento de la dirección **Parcial**	Política de seguridad **Parcial**	Análisis de riesgos **Bien**	
2. Saber qué tienes 50 de 100	Inventario **Parcial**	Configuración segura y software con soporte **Parcial**	Datos críticos y personales **Parcial**	
3. Quién entra y cómo 86 de 100	Verificación en dos pasos **Bien**	Cuentas de administrador **Parcial**	Altas y bajas **Bien**	
4. Equipos protegidos y al día 43 de 100	Protección contra programas maliciosos **Parcial**	Actualizaciones **Parcial**	Pruebas de seguridad **Sin cubrir**	
5. Correo, pagos y presencia en Internet 50 de 100	Cambios de cuenta bancaria **Parcial**	Filtrado de correo y navegación **Parcial**	Lo que tenéis expuesto a Internet **Bien**	Protección del dominio frente a la suplantación **Sin cubrir**
6. Recuperarte si te paran 56 de 100	Copia fuera del alcance de un ataque **Bien**	Restauración probada **Parcial**	Continuidad **Sin cubrir**	
7. Detectar y responder 57 de 100	Registros y alertas **Parcial**	Plan de respuesta a incidentes **Bien**	Notificación **Sin confirmar**	
8. Personas y proveedores 20 de 100	Concienciación **Parcial**	Proveedores **Sin cubrir**	Formación de la dirección **Sin cubrir**	

Hasta dónde llega este test

- Nadie ha comprobado tus respuestas: el resultado sale de lo que nos has contado.
- Son 25 preguntas sobre lo esencial. Los controles CIS v8.1, un estándar de referencia, reúnen 153 medidas concretas.
- Lo que no vemos: cómo están configurados de verdad tus sistemas, si la lista de equipos está completa, si las copias se recuperan, qué cuentas existen y qué dicen los registros.
- Un análisis con evidencias comprueba cada punto con pruebas, prioriza con datos de tu empresa y termina en una hoja de ruta y una presentación para dirección.

Fuente de la cifra: Center for Internet Security, «CIS Critical Security Controls Implementation Groups» (cisecurity.org).

03

Para dirección

Qué te pueden pedir, qué tener en cuenta por tu tamaño y a quién avisar si te pasa algo.

Acordad quién se responsabiliza de cada acción, qué evidencia permitirá darla por hecha y cuándo revisarla. Este informe no estima pérdidas económicas ni garantiza resultados.

Qué te pueden pedir

Lo que te puede pedir tu cliente

Algunos clientes piden garantías a sus proveedores, por política propia o porque, en los países donde NIS2 está transpuesta, deben cuidar su cadena de suministro (art. 21.2.d). En España, a 06-11-2026, esa obligación aún no está en una ley nacional. Mientras no tengamos cuestionarios reales anonimizados para señalar las preguntas que más se repiten, empieza por los puntos de tu resultado que no están completos. Fuente: Directiva (UE) 2022/2555.

NIS2: no podemos determinarlo con este perfil

Con este perfil no podemos determinar si NIS2 te afecta; depende de tu actividad concreta y de tu tamaño. Mira la guía NIS2. Fuente: Directiva (UE) 2022/2555, art. 2, 4, 20, 21 y 23.

El RGPD ya pide seguridad y aviso

Si tratas datos personales, el RGPD pide medidas de seguridad apropiadas al riesgo (art. 32). Ante una brecha, el responsable la notifica a la autoridad de control sin dilación indebida y, si es posible, en 72 horas desde que tiene constancia, salvo que sea improbable que suponga un riesgo para las personas (art. 33). A las personas afectadas se les comunica cuando el riesgo es alto (art. 34). Fuente: Reglamento (UE) 2016/679; guía de brechas de la AEPD.

Ninguno de estos bloques confirma que una norma te aplique, y que no aparezca uno no significa que no te afecte. Textos revisados a 06-11-2026.

Según el tamaño de tu empresa

Si sois de 20 a 50 personas

Orientación general según el tamaño que nos has indicado. No sustituye un análisis de tu caso.

- Con varios departamentos y proveedores, conviene que el responsable de seguridad tenga el encargo por escrito y tiempo asignado.
- Las altas y bajas y los accesos de proveedores ya no se controlan bien de memoria: pon por escrito cómo se gestionan.
- Si un cliente grande te envía un cuestionario de seguridad, la política, el plan de respuesta y las evidencias del plan de 90 días te permiten responderlo.
- Valora servicios gestionados para lo que necesita atención continua, como las alertas.

Lo que se ve desde fuera

example.com: ¿te pueden suplantar por email? Sí, es posible. Tu DMARC está en «p=none»: no pide a los buzones que rechacen ni que aparten los correos que se hacen pasar por tu dominio.

Si te pasa, avisa a...

Contactos oficiales, comprobados el 12 de octubre de 2026.

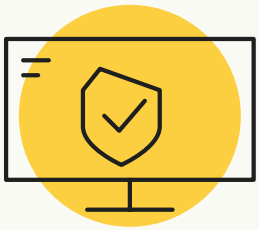
- Ayuda gratuita inmediata: INCIBE, «Tu Ayuda en Ciberseguridad». Teléfono 017, todos los días de 8:00 a 23:00; también WhatsApp 900 116 117 y Telegram @INCIBE017.
- Notificar el incidente al CERT nacional (empresas): INCIBE-CERT, incidencias@incibe-cert.es.
- Sector público, o si le prestas el servicio afectado: el CCN-CERT, por el canal de notificación de incidentes que indica en su web.
- Brecha de datos personales: el responsable la notifica a la autoridad de control competente (la AEPD, cuando corresponda; tiene un formulario en su sede electrónica) sin dilación indebida y, de ser posible, a más tardar en 72 horas desde que tiene constancia, salvo que sea improbable que suponga un riesgo para las personas (RGPD, art. 33). A las personas afectadas, cuando el riesgo es alto (art. 34).
- Delito (fraude, extorsión): denuncia ante la Policía Nacional, la Guardia Civil o la policía autonómica.
- Por contrato: tu aseguradora y tus clientes, en los plazos de la póliza y de los contratos.

- INCIBE · Línea de ayuda en ciberseguridad: https://www.incibe.es/linea-de-ayuda-en-ciberseguridad
- CCN-CERT: https://www.ccn-cert.cni.es/
- AEPD · Brechas de datos personales: https://www.aepd.es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/brechas-de-datos-personales
- Guía «Notificar un incidente en España» (Minery Report): https://mineryreport.com/recursos/notificar-incidente-espana/

04

Qué hacer, punto por punto

19 fichas, una por cada punto mejorable: lo que nos dijiste, por qué importa y qué hacer.



Cada ficha recoge lo que nos dijiste, por qué importa y qué hacer. El esfuerzo y el responsable son orientativos.

TEMA 1

Gobierno: quién decide y responde

64 de 100 · 2 puntos mejorables

Responsable y seguimiento de la dirección

Tema 1 · Gobierno: quién decide y responde

Imprescindible · Parcial · +3 puntos

Nos dijiste: «Hay responsable designado, pero la dirección no lo revisa al menos una vez al año»

Por qué importa: Falta una de las dos piezas: alguien con el encargo por escrito o que la dirección lo revise. Sin las dos, es difícil demostrar que se hace.

Qué hacer

1. Pon en el calendario de dirección una revisión de seguridad al año.
2. Para esa revisión, pide al responsable un informe breve y guarda el acta con lo decidido.

Sabrás que está hecho cuando: Hay un nombramiento firmado y una fecha para la próxima revisión.

Esfuerzo: Bajo (hasta 2 jornadas) · Quién: Dirección · Cuándo: Días 0-30

Política de seguridad

Tema 1 · Gobierno: quién decide y responde

Parcial · +2 puntos

Nos dijiste: «Existe, pero está desactualizada o la plantilla no la conoce»

Por qué importa: Una política antigua o que nadie conoce no cambia lo que hace la plantilla.

Qué hacer

1. Actualízala para que refleje cómo trabajáis hoy.
2. Vuelve a comunicarla y pide que confirmen su lectura.
3. Revísala una vez al año.

Sabrás que está hecho cuando: Hay una política aprobada o revisada en los últimos 12 meses y la plantilla ha confirmado su lectura.

Esfuerzo: Bajo (hasta 2 jornadas) · Quién: TI · Cuándo: Días 0-30
Te puede ayudar: Plantilla de política de seguridad (mineryreport.com)

TEMA 2

Saber qué tienes

50 de 100 · 3 puntos mejorables

Inventario

Tema 2 · Saber qué tienes

Parcial

+2 puntos

Nos dijiste: «Parcial, o sin revisión en el último año»

Por qué importa: Lo que falta en la lista, como un móvil o un servicio en la nube, puede quedarse sin proteger.

Qué hacer

1. Completa la lista, sobre todo móviles y servicios en la nube.
2. Pon un responsable a cada elemento.
3. Revisa la lista cada seis meses.

Sabrás que está hecho cuando: Hay una lista completa, revisada en los últimos seis meses.

Esfuerzo: Bajo (hasta 2 jornadas) · Quién: TI · Cuándo: Días 0-30

Configuración segura y software con soporte

Tema 2 · Saber qué tienes

Parcial

+1 punto

Nos dijiste: «No hay guía, aunque todos los sistemas siguen recibiendo actualizaciones»

Por qué importa: Queda un punto débil: algún sistema sin actualizaciones del fabricante o equipos sin una configuración común.

Qué hacer

1. Escribe una guía corta de cómo se instala un equipo nuevo, por ejemplo a partir de las del CCN.
2. Aplícala a los equipos nuevos desde ya.
3. Revisa después los equipos existentes, empezando por los servidores.

Sabrás que está hecho cuando: No queda ningún sistema sin soporte y los equipos se instalan siguiendo una guía escrita.

Esfuerzo: Medio (3-10 jornadas) · Quién: TI · Cuándo: Después de 90 días

Datos críticos y personales

Tema 2 · Saber qué tienes

Parcial

+1 punto

Nos dijiste: «Más o menos, pero no está documentado»

Por qué importa: Saberlo «más o menos» no basta cuando hay que avisar rápido de una fuga.

Qué hacer

1. Pon por escrito qué información es sensible y dónde está.
2. Crúzalo con vuestro registro de actividades de tratamiento (art. 30 del RGPD).
3. Revísalo una vez al año.

Sabrás que está hecho cuando: Hay un documento con la información sensible, dónde está y quién accede.

Esfuerzo: Bajo (hasta 2 jornadas) · Quién: Compras/Legal · Cuándo: Después de 90 días

TEMA 3

Quién entra y cómo

86 de 100 · 1 punto mejorable

Cuentas de administrador

Tema 3 · Quién entra y cómo

Parcial

+2 puntos

Nos dijiste: «Separadas, pero sin revisión, o solo en parte»

Por qué importa: Las cuentas de administrador que nadie revisa pueden seguir activas aunque ya nadie las necesite.

Qué hacer

1. Revisa quién tiene permisos de administrador y por qué, y elimina las cuentas que sobran.
2. Programa la revisión cada seis meses.

Sabrás que está hecho cuando: Los administradores usan una cuenta aparte y la lista se revisa cada seis meses.

Esfuerzo: Bajo (hasta 2 jornadas) · Quién: TI · Cuándo: Días 31-60

TEMA 4

Equipos protegidos y al día

43 de 100 · 3 puntos mejorables

Protección contra programas maliciosos

Tema 4 · Equipos protegidos y al día

Imprescindible Parcial

+3 puntos

Nos dijiste: «En casi todos, o nadie mira las alertas»

Por qué importa: Un equipo sin protección, o una alerta que nadie mira, deja pasar el ataque.

Qué hacer

1. Cubre los equipos que faltan.
2. Decide quién mira las alertas y en qué horario.
3. Comprueba cada mes que no falta ningún equipo.

Sabrás que está hecho cuando: Todos los equipos aparecen en la consola y alguien atiende las alertas.

Esfuerzo: Bajo (hasta 2 jornadas) · Quién: TI · Cuándo: Días 0-30

Actualizaciones

Tema 4 · Equipos protegidos y al día

Imprescindible Parcial

+3 puntos

Nos dijiste: «Se instalan, pero sin plazo ni control»

Por qué importa: Sin plazos ni control, algún equipo se queda atrás sin que lo sepas, como el portátil de quien viaja o el router.

Qué hacer

1. Pon por escrito los plazos de actualización, también para servidores y equipos de red.
2. Pide cada mes un informe de qué está al día.

Sabrás que está hecho cuando: Hay plazos escritos y un informe mensual que muestra que se cumplen.

Esfuerzo: Bajo (hasta 2 jornadas) · Quién: TI · Cuándo: Días 0-30

⚠ Pruebas de seguridad

Tema 4 · Equipos protegidos y al día

Sin cubrir · **+2 puntos**

Nos dijiste: «Nunca»

Por qué importa: Sin probar tu seguridad, no sabrás si funciona hasta que alguien la pruebe por ti, por ejemplo con un acceso remoto olvidado y una contraseña débil.

Qué hacer

1. Encarga una búsqueda de vulnerabilidades (fallos conocidos) en lo que tienes abierto a Internet.
2. Corrige primero lo más grave.
3. Repítela de forma periódica y planifica una prueba de intrusión al año (un experto intenta entrar).

✓ Sabrás que está hecho cuando: Hay una prueba de los últimos 12 meses y sus fallos están corregidos.

Esfuerzo: Medio (3-10 jornadas) · Quién: TI · Cuándo: Días 61-90

TEMA 5

Correo, pagos y presencia en Internet

50 de 100 · 3 puntos mejorables

⚠ Protección del dominio frente a la suplantación

Tema 5 · Correo, pagos y presencia en Internet

Sin cubrir · **+4 puntos**

Nos dijiste: «No»

Por qué importa: Sin una protección en tu dominio, alguien puede enviar correos que parecen tuyos, por ejemplo una factura falsa a un cliente.

Qué hacer

1. Pide a quien gestiona tu correo SPF, DKIM y DMARC en modo observación (registros que acreditan tus correos).
2. Revisa los informes unas semanas y autoriza cada servicio que envía en tu nombre (facturas, boletines).
3. Después, pasa DMARC a cuarentena y, tras varias semanas de observación, a rechazo.

✓ Sabrás que está hecho cuando: El comprobador muestra DMARC en cuarentena o rechazo y tus correos legítimos siguen llegando.

Esfuerzo: Bajo (hasta 2 jornadas) · Quién: TI · Cuándo: Días 0-30
Te puede ayudar: Comprobador de correo y dominio (mineryreport.com)

◐ Filtrado de correo y navegación

Tema 5 · Correo, pagos y presencia en Internet

Parcial · **+1 punto**

Nos dijiste: «Solo una de ellas»

Por qué importa: Con un solo filtro, parte de los mensajes o webs peligrosas siguen llegando.

Qué hacer

1. Activa el filtro que falta: el del correo o el de la navegación.
2. Comprueba que funciona también fuera de la oficina.
3. Explica cómo avisar de un correo sospechoso.

✓ Sabrás que está hecho cuando: Los dos filtros están activos y la plantilla sabe cómo avisar.

Esfuerzo: Bajo (hasta 2 jornadas) · Quién: TI · Cuándo: Después de 90 días

Cambios de cuenta bancaria

Parcial

Tema 5 · Correo, pagos y presencia en Internet

+2 puntos

Nos dijiste: «A veces, o depende de quién lo reciba»

Por qué importa: Si la comprobación depende de quién reciba el correo, un día se la saltan.

Qué hacer

1. Pon la norma por escrito y que la apruebe la dirección.
2. Exige que una segunda persona apruebe cada cambio.
3. Deja constancia de cada comprobación.

Sabrás que está hecho cuando: Hay una norma firmada y cada cambio de cuenta queda comprobado por teléfono.

Esfuerzo: Bajo (hasta 2 jornadas) · Quién: Dirección, TI · Cuándo: Días 31-60

TEMA 6

Recuperarte si te paran

56 de 100 · 2 puntos mejorables

Restauración probada

Imprescindible Parcial

Tema 6 · Recuperarte si te paran

+3 puntos

Nos dijiste: «Solo de algún archivo suelto, o hace más de un año»

Por qué importa: Recuperar un archivo suelto no demuestra que puedas recuperar un sistema entero.

Qué hacer

1. Prueba a recuperar un sistema completo, no un archivo suelto, y anota cuánto se tarda.
2. Fija un calendario de pruebas, al menos una al año.

Sabrás que está hecho cuando: Hay un acta de una recuperación completa de los últimos 12 meses, con el tiempo que llevó.

Esfuerzo: Bajo (hasta 2 jornadas) · Quién: TI · Cuándo: Días 0-30

Continuidad

Sin cubrir

Tema 6 · Recuperarte si te paran

+4 puntos

Nos dijiste: «No»

Por qué importa: Sin un plan, cada hora de parada se improvisa: por ejemplo, cómo facturar o atender pedidos si cae el programa de gestión.

Qué hacer

1. Elige con dirección los 3 a 5 procesos sin los que no podéis facturar ni cobrar.
2. Decide cuánto tiempo puede parar cada uno y cómo seguir trabajando mientras tanto.
3. Escríbelo y ensáyalo una vez al año.

Sabrás que está hecho cuando: Hay un plan escrito y aprobado, y un ensayo en los últimos 12 meses.

Esfuerzo: Medio (3-10 jornadas) · Quién: Dirección, TI · Cuándo: Días 31-60
Te puede ayudar: Calculadora del coste de un incidente (mineryreport.com)

TEMA 7

Detectar y responder

57 de 100 · 2 puntos mejorables

Registros y alertas

Tema 7 · Detectar y responder

Parcial

+2 puntos

Nos dijiste: «Se guardan, pero nadie los revisa o no están centralizados»

Por qué importa: Registros dispersos o que nadie revisa no sirven para ver a tiempo un acceso indebido.

Qué hacer

1. Centraliza los registros que ya guardáis.
2. Decide quién revisa las alertas y cada cuánto.
3. Valora un servicio de vigilancia si nadie puede hacerlo.

Sabrás que está hecho cuando: Los registros están centralizados y alguien atiende las alertas.

Esfuerzo: Medio (3-10 jornadas) · Quién: TI · Cuándo: Días 61-90

Notificación

Tema 7 · Detectar y responder

Sin confirmar

+4 puntos

Nos dijiste: «No lo sé»

Por qué importa: Avisar tarde o a quien no toca suma problemas legales y con clientes a los daños del incidente.

Qué hacer

1. Averígualo: pregunta a dirección a quién habría que avisar y en qué plazo.
2. Haz una tabla de a quién avisar, en qué plazo y cómo: AEPD, INCIBE-CERT, clientes y aseguradora.
3. Añade los plazos de tus contratos y de tu seguro.

Sabrás que está hecho cuando: El plan incluye a quién avisar, en qué plazo y quién lo hace.

Esfuerzo: Bajo (hasta 2 jornadas) · Quién: Compras/Legal, TI · Cuándo: Días 0-30
Te puede ayudar: Guía «Notificar un incidente en España» (mineryreport.com)

TEMA 8

Personas y proveedores

20 de 100 · 3 puntos mejorables

Concienciación

Tema 8 · Personas y proveedores

Parcial

+2 puntos

Nos dijiste: «Algo puntual, o solo formación sin simulacros»

Por qué importa: Sin simulacros, no sabes si la formación funciona ante un correo falso bien hecho.

Qué hacer

1. Convierte lo puntual en un programa anual.
2. Añade simulacros de correo falso.
3. Comparte los resultados con dirección.

Sabrás que está hecho cuando: Hay formación anual con asistencia registrada y simulacros.

Esfuerzo: Medio (3-10 jornadas) · Quién: RR. HH. · Cuándo: Días 61-90

⚠ Proveedores

Tema 8 · Personas y proveedores

Sin cubrir **+4 puntos**

Nos dijiste: «No»

Por qué importa: Cada proveedor que entra en tus sistemas, como la gestoría o el mantenimiento informático, es una puerta más. Si sufre un incidente, puede afectarte sin avisarte.

Qué hacer

1. Lista los proveedores con acceso a tus sistemas o datos.
2. Pídeles por escrito lo básico: verificación en dos pasos, copias y aviso de incidentes.
3. Inclúyelo en los contratos nuevos y en las renovaciones.

✓ Sabrás que está hecho cuando: Los proveedores críticos tienen requisitos de seguridad en su contrato.

Esfuerzo: Medio (3-10 jornadas) · Quién: Compras/Legal, TI · Cuándo: Días 31-60
Te puede ayudar: Evaluación de proveedores · Plantilla de cuestionario de proveedores · Cláusulas de seguridad para proveedores (mineryreport.com)

⚠ Formación de la dirección

Tema 8 · Personas y proveedores

Sin cubrir **+2 puntos**

Nos dijiste: «No»

Por qué importa: Sin formación, la dirección decide a ciegas en un incidente: qué parar, a quién avisar o si pagar.

Qué hacer

1. Organiza una sesión de unas dos horas para dirección.
2. Incluye un ejercicio: qué decidiríais ante un ataque.
3. Repítela cada año.

✓ Sabrás que está hecho cuando: La dirección ha hecho una sesión con un ejercicio práctico y tiene fecha para la siguiente.

Esfuerzo: Bajo (hasta 2 jornadas) · Quién: Dirección · Cuándo: Días 61-90

DKIM: sin datos; no podemos ver desde fuera si tu correo sale firmado.

Lo que ya haces bien

Estos puntos ya están en la mejor respuesta. Mantenerlos también cuenta.

✓ Análisis de riesgos

Tienes un análisis de riesgos reciente y con plan: tus decisiones de inversión se apoyan en lo que de verdad te puede parar.

✓ Verificación en dos pasos

Tienes verificación en dos pasos en el correo y en los accesos desde Internet: una contraseña robada ya no basta para entrar.

✓ Altas y bajas

Retiráis los accesos el mismo día de la baja: no quedan puertas abiertas de quien ya no está.

✓ Lo que tenéis expuesto a Internet

Sabéis qué tenéis abierto a Internet y quién lo mantiene: cada entrada tiene a alguien que la mantiene.

✓ Copia fuera del alcance de un ataque

Tienes copias automáticas con una copia aislada o inmutable: tienes una copia pensada para que un secuestro de datos no pueda borrarla ni cifrarla.

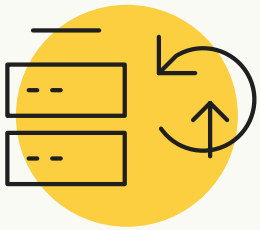
✓ Plan de respuesta a incidentes

Tenéis un plan de respuesta escrito y ensayado: en las primeras horas, cada uno sabe qué hacer.

05

Plan de 90 días

Las tareas de las fichas, en el orden en que conviene hacerlas. En 90 días no se cierra todo: empieza por lo imprescindible; el resto puede esperar al tramo de después.



Días 0-30

Responsable y seguimiento de la dirección
Bajo · Dirección
Imprescindible

Protección contra programas maliciosos
Bajo · TI
Imprescindible

Actualizaciones
Bajo · TI
Imprescindible

Restauración probada
Bajo · TI
Imprescindible

Protección del dominio frente a la suplantación
Bajo · TI

Notificación
Bajo · Compras/Legal, TI

Política de seguridad
Bajo · TI

Inventario
Bajo · TI

Días 31-60

Continuidad
Medio · Dirección, TI

Proveedores
Medio · Compras/Legal, TI

Cuentas de administrador
Bajo · TI

Cambios de cuenta bancaria
Bajo · Dirección, TI

Días 61-90

Formación de la dirección
Bajo · Dirección

Pruebas de seguridad
Medio · TI

Registros y alertas
Medio · TI

Concienciación
Medio · RR. HH.

Después de 90 días

Datos críticos y personales
Bajo · Compras/Legal

Filtrado de correo y navegación
Bajo · TI

Configuración segura y software con soporte
Medio · TI

06 Para tu equipo técnico

El detalle técnico: normas relacionadas, lo que se ve desde fuera y cómo se calcula.

Impacto: lo que subiría tu puntuación si esa pregunta pasara a la mejor respuesta; se cuenta una vez por pregunta. Es una estimación, no un compromiso.

Relación con normas y marcos

Solo de los puntos mejorables. Es una relación temática y, en general, parcial: no es una evaluación de cumplimiento.

Punto	CIS v8.1	ISO 27001	ENS	NIS2
Responsable y seguimiento de la dirección	—	5.1, 5.3, A.5.2	org.1	20.1
Política de seguridad	—	5.2, A.5.1	org.1, org.2	21.2.a
Inventario	1.1, 2.1	A.5.9	op.exp.1	21.2.i
Configuración segura y software con soporte	4.1, 2.2	A.8.9	op.exp.2, op.exp.3	21.2.e
Datos críticos y personales	3.1, 3.2	A.5.12, A.5.34	mp.info.1, mp.info.2	21.2.i
Cuentas de administrador	5.1, 5.4	A.8.2, A.5.18	op.acc.4	21.2.i
Protección contra programas maliciosos	10.1, 10.6	A.8.7	op.exp.6	21.2.e, 21.2.g
Actualizaciones	7.1, 7.3, 7.4	A.8.8	op.exp.4	21.2.e
Pruebas de seguridad	7.5, 7.6, 18.1, 18.2, 18.3	A.8.8	—	21.2.e, 21.2.f
Protección del dominio frente a la suplantación	9.5	A.5.14, A.8.21	mp.s.1	21.2.g
Filtrado de correo y navegación	9.2, 9.6, 9.7	A.8.23, A.8.7	mp.s.1, mp.s.3, op.exp.6	21.2.g
Cambios de cuenta bancaria	14.2	A.5.37, A.6.3	mp.per.3	21.2.g
Restauración probada	11.5	A.8.13, A.5.30	mp.info.6	21.2.c
Continuidad	—	A.5.29, A.5.30	op.cont.1, op.cont.2	21.2.c
Registros y alertas	8.2, 8.9, 8.11	A.8.15, A.8.16	op.exp.8, op.mon.1, op.mon.3	21.2.b
Notificación	17.2, 17.3	A.5.5, A.5.24, A.6.8	op.exp.7	23
Concienciación	14.1, 14.2, 14.6	A.6.3	mp.per.3, mp.per.4	21.2.g
Proveedores	15.1, 15.2, 15.4	A.5.19, A.5.20, A.5.21, A.5.22, A.5.23	op.ext.1, op.ext.2, op.ext.3	21.2.d
Formación de la dirección	14.1	7.2, A.6.3	mp.per.4	20.2

Lo que se ve desde fuera de example.com

Comprobación	Estado	Qué significa y qué hacer
SPF	Mejorable	Tu SPF solo pide marcar como sospechoso el correo de servidores no autorizados, y tu DMARC no pide rechazarlo ni apartarlo. Termina en «~all» y tu DMARC no está en cuarentena ni rechazo. Endurece DMARC o usa «-all».
DKIM	Sin datos	No hemos encontrado ninguna clave con los selectores habituales. Si conoces el tuyo, escríbelo en la opción avanzada. Probados 14 selectores habituales sin resultado. Busca el selector en la cabecera DKIM-Signature (s=) de un correo enviado.
DMARC	Riesgo	Así publicado, no pide a los buzones que los rechacen ni que los aparten. Política «p=none». Pasos: con «p=none» y «rua», revisa los informes 2-4 semanas; después «p=quarantine» y, por último, «p=reject». Añade «rua=mailto:...» para recibir informes agregados.
MTA-STS	Mejorable	No lo tienes publicado. No es obligatorio. Para publicarlo: TXT en _mta-sts.example.com con «v=STSv1; id=...» y la política en https://mta-sts.example.com/.well-known/mta-sts.txt.
DNSSEC	Mejorable	Tu dominio no está firmado con DNSSEC. Sin DS en el padre y sin bit AD. Actívalo en tu proveedor de DNS y publica el DS en el registrador.
CAA	Mejorable	No tienes CAA: cualquier autoridad de certificación puede emitir certificados para tu dominio.
Cabeceras de seguridad	Mejorable	No tienes política de seguridad de contenidos (CSP). Añade Content-Security-Policy con al menos «script-src» sin «*», sin fuentes solo de esquema y sin 'unsafe-inline' salvo con nonces o hashes. Añade «frame-ancestors 'none'» (o 'self') a la CSP, o «X-Frame-Options: DENY». Añade «X-Content-Type-Options: nosniff». Sin Referrer-Policy: el navegador usa su valor por defecto.
security.txt	Sin datos	No hemos podido descargar tu security.txt.

Revisión pública de baja intensidad del 20 de octubre de 2026: no escanea puertos ni prueba vulnerabilidades. «Sin datos» no cuenta como bien.

Fuentes oficiales

- CIS Controls v8.1 (CIS Controls Navigator): https://www.cisecurity.org/controls/cis-controls-navigator
- ISO/IEC 27001:2022 (ISO): https://www.iso.org/standard/82875.html
- ENS: Real Decreto 311/2022, texto consolidado (BOE): https://www.boe.es/buscar/act.php?id=BOE-A-2022-7191
- NIS2: Directiva (UE) 2022/2555 (EUR-Lex): https://eur-lex.europa.eu/eli/dir/2022/2555/oj

Cómo se calcula

Cada respuesta vale 100, 50 o 0 («No lo sé» cuenta 0) y pesa de 1 a 3 según su importancia. La puntuación es la media ponderada de las preguntas aplicables a tu caso. Niveles: Riesgo alto (0-39), Mejorable (40-64), En marcha (65-84) y Sólida (85-100). Siete controles son imprescindibles: si alguno falta, el nivel tiene un tope aunque la puntuación sea alta. Versión del banco: banco-v1.2, revisado a 12 de octubre de 2026.

Marcos: CIS Controls v8.1; ISO/IEC 27001:2022; RD 311/2022 (texto consolidado del BOE); Directiva (UE) 2022/2555.

Alcance y limitaciones: Evalúa es una autoevaluación orientativa basada en tus respuestas y en información pública de tu dominio. No es una auditoría, no certifica el cumplimiento de ninguna norma y no sustituye un análisis profesional. Las referencias a normas indican con qué controles se relaciona cada respuesta, no que cumplas o incumplas. Estado normativo a 12 de octubre de 2026.