MINERY REPORT

SAMPLE REPORT · FICTITIOUS COMPANY

Cybersecurity report

Distribuciones Ejemplo, S. L. (fictitious company)

20 October 2026

Indicative level

Room for improvement

You have some of the basics, but there are gaps that an attacker or a demanding client would find.

You have answered all 25; 1 with "I don't know".

Contents

Summary for management 2
At a glance 4
How far this test goes 4
For management 5
What to do, point by point 7
What you already do well 13
90-day plan 14
For your technical team 15
How it is calculated and scope 16

Indicative self-assessment based on your answers: it is not an audit or a certification. The score is not a probability of suffering an incident.

01 Summary for management

The essentials on one page.

55
out of 100
Indicative level: Room for improvement

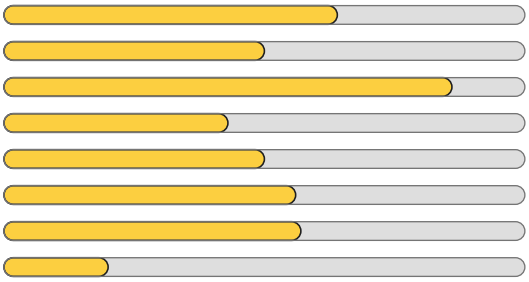
4 ⚠
essential points to fix
Out of 7 essential points

13
low-effort tasks
Up to 2 working days each. You do not need to do them all this quarter.

6
already well covered
Out of 25 points

You have answered all 25; 1 with "I don't know". It is not an audit or a certification. The score is not a probability of suffering an incident. Score from your answers: 55 out of 100. With what can be seen from outside: 55 out of 100. The available comparison does not change the score.

Result by topic



1. Governance: who decides and is accountable	**64 out of 100**
2. Knowing what you have	**50 out of 100**
3. Who gets in and how	**86 out of 100**
4. Devices protected and up to date	**43 out of 100**
5. Email, payments and your internet presence	**50 out of 100**
6. Recovering if you are brought to a halt	**56 out of 100**
7. Detecting and responding	**57 out of 100**
8. People and suppliers	**20 out of 100**

The 3 gaps worth closing first

1. **Security lead and management oversight** — Essential
   One of the two pieces is missing: a lead with the responsibility assigned in writing, or a dated management review. Without both, follow-up depends on goodwill and is hard to show to a client. You told us: "There is a designated lead, but management does not review it at least once a year".

2. **Protection against malware** — Essential
   A device without protection or central monitoring can be the way in for ransomware without anyone seeing the alert. You told us: "On almost all of them, or nobody looks at the alerts".

3. **Updates** — Essential
   Without a deadline or follow-up, a flaw the vendor has already fixed can stay open for weeks without you knowing. You told us: "They get installed, but with no deadline or control".

Also: bank account changes. If the check depends on who receives the email, a fake change of bank details can slip through on the day it is not done. This is how you answered: "Sometimes, or it depends on who receives it".

Your 3 decisions for this quarter

1. **Complete what is missing (the written role or the management review) and take management a short report on risks, incidents and the plan**
   Effort: Low (up to 2 working days) · Who: Management

2. **Agree with management on the maximum downtime for the 3-5 key processes and a minimum plan**
   Effort: Medium (3-10 working days) · Who: Management, IT

3 **Make it a mandatory step when adding bank details to the payment system**

Effort: Low (up to 2 working days) · Who: Management, IT

02 At a glance

Your 25 answers, by topic. Each box shows where that point stands.

Good · Partial · Not covered · Unconfirmed

1. Governance: who decides and is accountable 64 out of 100	Security lead and management oversight **Partial**	Security policy **Partial**	Risk assessment **Good**	
2. Knowing what you have 50 out of 100	Asset inventory **Partial**	Secure configuration and supported software **Partial**	Critical and personal data **Partial**	
3. Who gets in and how 86 out of 100	Two-step verification **Good**	Administrator accounts **Partial**	Joiners and leavers **Good**	
4. Devices protected and up to date 43 out of 100	Protection against malware **Partial**	Updates **Partial**	Security testing **Not covered**	
5. Email, payments and your internet presence 50 out of 100	Bank account changes **Partial**	Email and web filtering **Partial**	What you expose to the internet **Good**	Protecting your domain against spoofing **Not covered**
6. Recovering if you are brought to a halt 56 out of 100	A backup out of an attacker's reach **Good**	Tested restore **Partial**	Business continuity **Not covered**	
7. Detecting and responding 57 out of 100	Logs and alerts **Partial**	Incident response plan **Good**	Notification **Unconfirmed**	
8. People and suppliers 20 out of 100	Security awareness **Partial**	Suppliers **Not covered**	Management training **Not covered**	

How far this test goes

- Nobody has checked your answers: the result comes from what you told us.
- There are 25 questions on the essentials. The CIS Controls v8.1, a reference standard, bring together 153 specific measures.
- What we cannot see: how your systems are really configured, whether your list of devices is complete, whether backups can be restored, which accounts exist and what the logs say.
- An evidence-based analysis checks each point with proof, prioritises with your company's data and ends with a roadmap and a presentation for management.

Source of the figure: Center for Internet Security, "CIS Critical Security Controls Implementation Groups" (cisecurity.org).

03

For management

What you may be asked for, what to bear in mind for your size and who to notify if something happens.

Agree who is responsible for each action, what evidence will allow it to be marked as done and when to review it. This report does not estimate financial losses or guarantee results.

What you may be asked for

What your client may ask of you

Some clients ask their suppliers for assurances, under their own policy or because, in the countries where NIS2 has been transposed, they must look after their supply chain (Article 21(2)(d)). In Spain, as of 6 November 2026, that obligation was not yet in a national law. Until we have real anonymised questionnaires to point out the questions that come up most often, start with the points of your result that are not complete. Source: Directive (EU) 2022/2555.

NIS2: we cannot determine it with this profile

With this profile we cannot determine whether NIS2 affects you; it depends on your specific activity and your size. Check it with "Does NIS2 apply?". Source: Directive (EU) 2022/2555, Articles 2, 4, 20, 21 and 23.

The GDPR already requires security and notification

If you process personal data, the GDPR requires security measures appropriate to the risk (Article 32). In the event of a breach, the controller notifies the supervisory authority without undue delay and, where feasible, not later than 72 hours after becoming aware of it, unless it is unlikely to result in a risk to people (Article 33). The people affected are informed when the risk is high (Article 34). Source: Regulation (EU) 2016/679; personal data breach guidance of Spain's AEPD (in Spanish).

None of these sections confirms that a law applies to you, and the absence of a section does not mean that it does not affect you. Texts reviewed as of 6 November 2026.

For the size of your company

If you have 20 to 50 people

General guidance based on the size you told us. It does not replace an assessment of your own situation.

- With several departments and suppliers, the security lead should have the responsibility in writing and allocated time.
- Joiners, leavers and supplier access can no longer be controlled well from memory: put in writing how they are handled.
- If a large client sends you a security questionnaire, the policy, the response plan and the evidence from the 90-day plan let you answer it.
- Consider managed services for what needs continuous attention, such as alerts.

What can be seen from outside

example.com: can you be spoofed by email? Yes, it is possible. Your DMARC policy is «p=none»: it does not ask mailboxes to reject or quarantine emails that pretend to come from your domain.

If it happens to you, notify...

Official contacts, checked on 12 October 2026.

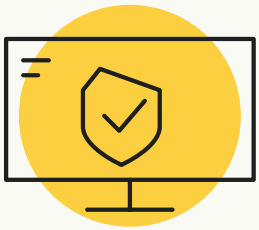
- Free immediate help in Spain: INCIBE's helpline "Tu Ayuda en Ciberseguridad". Phone 017, every day from 8:00 to 23:00; also WhatsApp 900 116 117 and Telegram @INCIBE017.
- Report the incident to the national CSIRT (companies in Spain): INCIBE-CERT, incidencias@incibe-cert.es.
- Public sector in Spain, or if you provide it with the affected service: CCN-CERT, through the incident notification channel shown on its website.
- Personal data breach: the controller notifies the competent supervisory authority (in Spain, the AEPD where applicable; it has a form on its electronic office) without undue delay and, where feasible, not later than 72 hours after becoming aware of it, unless it is unlikely to result in a risk to people (GDPR, Article 33). The people affected are informed when the risk is high (Article 34).
- Crime (fraud, extortion): report it to the police (in Spain, the Policía Nacional, the Guardia Civil or the regional police).
- Under contract: your insurer and your clients, within the deadlines of the policy and the contracts.

- INCIBE · Cybersecurity helpline (in Spanish): https://www.incibe.es/linea-de-ayuda-en-ciberseguridad
- CCN-CERT: https://www.ccn-cert.cni.es/
- AEPD · Personal data breaches (in Spanish): https://www.aepd.es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/brechas-de-datos-personales
- Guide "Notifying an incident in Spain" (Minery Report, in Spanish): https://mineryreport.com/recursos/notificar-incidente-espana/

04

What to do, point by point

19 sheets, one for each point to improve: what you told us, why it matters and what to do.



Each sheet says what you told us, why it matters and what to do. Effort and owner are indicative.

TOPIC 1

Governance: who decides and is accountable

64 out of 100 · 2 points to improve

Security lead and management oversight

Topic 1 · Governance: who decides and is accountable

Essential · Partial

+3 points

You told us: "There is a designated lead, but management does not review it at least once a year"

Why it matters: One of two pieces is missing: someone with the remit in writing, or a review by management. Without both, it is hard to show it is being done.

What to do

1. Put a yearly security review in the management calendar.
2. For that review, ask for a short report and keep the minutes with what was decided.

You will know it is done when: There is a signed appointment and a date for the next review.

Effort: Low (up to 2 working days) · Who: Management · When: Days 0-30

Security policy

Topic 1 · Governance: who decides and is accountable

Partial

+2 points

You told us: "It exists, but it is out of date or staff do not know it"

Why it matters: An old policy, or one nobody knows about, does not change what your staff do.

What to do

1. Update it so it reflects how you work today.
2. Share it again and ask staff to confirm they have read it.
3. Review it once a year.

You will know it is done when: There is a policy approved or reviewed in the last 12 months and staff have confirmed they have read it.

Effort: Low (up to 2 working days) · Who: IT · When: Days 0-30

TOPIC 2

Knowing what you have

50 out of 100 · 3 points to improve

Asset inventory

Topic 2 · Knowing what you have

Partial

+2 points

You told us: "Partial, or not reviewed in the last year"

Why it matters: Anything missing from the list, such as a phone or a cloud service, can be left unprotected.

What to do

1. Complete the list, especially phones and cloud services.
2. Give each item an owner.
3. Review the list every six months.

You will know it is done when: There is a complete list, reviewed in the last six months.

Effort: Low (up to 2 working days) · Who: IT · When: Days 0-30

Secure configuration and supported software

Topic 2 · Knowing what you have

Partial

+1 point

You told us: "There is no guide, but all systems still receive updates"

Why it matters: One weak spot remains: a system without updates from the maker, or computers without a common set-up.

What to do

1. Write a short guide on how a new computer is set up, for example based on the CCN's.
2. Apply it to new computers from now on.
3. Then review existing computers, starting with the servers.

You will know it is done when: No system is left without support and computers are installed following a written guide.

Effort: Medium (3-10 working days) · Who: IT · When: After 90 days

Critical and personal data

Topic 2 · Knowing what you have

Partial

+1 point

You told us: "More or less, but it is not documented"

Why it matters: Knowing it "more or less" is not enough when you have to report a leak quickly.

What to do

1. Put in writing which information is sensitive and where it is kept.
2. Cross-check it with your record of processing activities (GDPR Art. 30).
3. Review it once a year.

You will know it is done when: There is a document listing sensitive information, where it is kept and who can access it.

Effort: Low (up to 2 working days) · Who: Procurement/Legal · When: After 90 days

TOPIC 3

Who gets in and how

86 out of 100 · 1 point to improve

Administrator accounts

Topic 3 · Who gets in and how

Partial

+2 points

You told us: "Separate, but not reviewed, or only in part"

Why it matters: Admin accounts that nobody reviews can stay active even when nobody needs them any more.

What to do

1. Check who has admin rights and why, and delete the accounts that are not needed.
2. Schedule the review every six months.

You will know it is done when: Admins use a separate account and the list is reviewed every six months.

Effort: Low (up to 2 working days) · Who: IT · When: Days 31-60

TOPIC 4

Devices protected and up to date

43 out of 100 · 3 points to improve

Protection against malware

Topic 4 · Devices protected and up to date

Essential Partial

+3 points

You told us: "On almost all of them, or nobody looks at the alerts"

Why it matters: One unprotected computer, or an alert nobody looks at, lets the attack through.

What to do

1. Cover the computers that are missing.
2. Decide who looks at the alerts and during which hours.
3. Check every month that no computer is missing.

You will know it is done when: Every computer shows up in the console and someone deals with the alerts.

Effort: Low (up to 2 working days) · Who: IT · When: Days 0-30

Updates

Topic 4 · Devices protected and up to date

Essential Partial

+3 points

You told us: "They get installed, but with no deadline or control"

Why it matters: Without deadlines or checks, some computer falls behind without you knowing, such as the laptop of someone who travels or the router.

What to do

1. Put the update deadlines in writing, also for servers and network equipment.
2. Ask for a monthly report of what is up to date.

You will know it is done when: There are written deadlines and a monthly report showing they are met.

Effort: Low (up to 2 working days) · Who: IT · When: Days 0-30

Security testing

Topic 4 · Devices protected and up to date

Not covered

+2 points

You told us: "Never"

Why it matters: If you never test your security, you will not know whether it works until someone tests it for you, for example through a forgotten remote access with a weak password.

What to do

1. Commission a vulnerability scan (known flaws) of everything you have open to the Internet.
2. Fix the serious issues first.
3. Repeat it at regular intervals and plan a yearly penetration test (an expert tries to get in).

You will know it is done when: There is a test from the last 12 months and its flaws have been fixed.

Effort: Medium (3-10 working days) · Who: IT · When: Days 61-90

TOPIC 5

Email, payments and your internet presence

50 out of 100 · 3 points to improve

Protecting your domain against spoofing

Topic 5 · Email, payments and your internet presence

Not covered

+4 points

You told us: "No"

Why it matters: Without protection on your domain, someone can send emails that look like yours, for example a fake invoice to a client.

What to do

1. Ask whoever runs your email for SPF, DKIM and DMARC in monitoring mode (records that vouch for your emails).
2. Review the reports for a few weeks and authorise every service sending in your name (invoices, newsletters).
3. Then move DMARC to quarantine and, after several weeks of monitoring, to reject.

You will know it is done when: The email and domain check shows DMARC at quarantine or reject, and your genuine emails still arrive.

Effort: Low (up to 2 working days) · Who: IT · When: Days 0-30
This can help: Email and domain check (mineryreport.com)

Email and web filtering

Topic 5 · Email, payments and your internet presence

Partial

+1 point

You told us: "Only one of them"

Why it matters: With only one filter, some dangerous emails or websites still get through.

What to do

1. Turn on the missing filter: email or browsing.
2. Check that it also works outside the office.
3. Explain how to report a suspicious email.

You will know it is done when: Both filters are on and staff know how to report.

Effort: Low (up to 2 working days) · Who: IT · When: After 90 days

Bank account changes

Topic 5 · Email, payments and your internet presence

Partial

+2 points

You told us: "Sometimes, or it depends on who receives it"

Why it matters: If the check depends on who receives the email, one day it will be skipped.

What to do

1. Put the rule in writing and have management approve it.
2. Require a second person to approve each change.
3. Keep a record of each check.

You will know it is done when: There is a signed rule and every change of bank account is checked by phone.

Effort: Low (up to 2 working days) · Who: Management, IT · When: Days 31-60

TOPIC 6

Recovering if you are brought to a halt

56 out of 100 · 2 points to improve

Tested restore

Topic 6 · Recovering if you are brought to a halt

Essential Partial

+3 points

You told us: "Only of the odd file, or more than a year ago"

Why it matters: Recovering a single file does not prove you can recover a whole system.

What to do

1. Try recovering a whole system, not a single file, and note how long it takes.
2. Set a schedule of tests, at least one a year.

You will know it is done when: There is a record of a full recovery in the last 12 months, with the time it took.

Effort: Low (up to 2 working days) · Who: IT · When: Days 0-30

Business continuity

Topic 6 · Recovering if you are brought to a halt

Not covered

+4 points

You told us: "No"

Why it matters: Without a plan, every hour of downtime is improvised: for example, how to invoice or take orders if your management software goes down.

What to do

1. Choose with management the 3 to 5 processes without which you cannot invoice or get paid.
2. Decide how long each one can stop and how to keep working in the meantime.
3. Write it down and rehearse it once a year.

You will know it is done when: There is a written, approved plan and a rehearsal in the last 12 months.

Effort: Medium (3-10 working days) · Who: Management, IT · When: Days 31-60
This can help: Incident cost calculator (mineryreport.com)

TOPIC 7

Detecting and responding

57 out of 100 · 2 points to improve

Logs and alerts

Topic 7 · Detecting and responding

Partial

+2 points

You told us: "They are kept, but nobody reviews them or they are not centralised"

Why it matters: Scattered logs, or logs nobody reviews, will not show unauthorised access in time.

What to do

1. Bring the logs you already keep into one place.
2. Decide who reviews the alerts and at what intervals.
3. Consider a monitoring service if nobody can do it.

You will know it is done when: The logs are in one central place and someone deals with the alerts.

Effort: Medium (3-10 working days) · Who: IT · When: Days 61-90

Notification

Topic 7 · Detecting and responding

Unconfirmed

+4 points

You told us: "I don't know"

Why it matters: Reporting late, or to the wrong people, adds legal and client problems to the damage of the incident.

What to do

1. Find out: ask management whether they know who would have to be notified, and by when.
2. Make a table of who to notify, by when and how: AEPD, INCIBE-CERT, clients and insurer.
3. Add the deadlines in your contracts and your insurance policy.

You will know it is done when: The plan includes who to notify, by when and who does it.

Effort: Low (up to 2 working days) · Who: Procurement/Legal, IT · When: Days 0-30

TOPIC 8

People and suppliers

20 out of 100 · 3 points to improve

Security awareness

Topic 8 · People and suppliers

Partial

+2 points

You told us: "Something occasional, or training only, without simulations"

Why it matters: Without simulations, you do not know whether training works against a well-made fake email.

What to do

1. Turn one-off training into a yearly programme.
2. Add fake email simulations.
3. Share the results with management.

You will know it is done when: There is yearly training with recorded attendance, plus simulations.

Effort: Medium (3-10 working days) · Who: HR · When: Days 61-90

Suppliers

Topic 8 · People and suppliers

Not covered

+4 points

You told us: "No"

Why it matters: Every supplier that gets into your systems, such as your accountants or your IT maintenance firm, is one more door. If they suffer an incident, it can affect you without them telling you.

What to do

1. List the suppliers with access to your systems or data.
2. Ask them in writing for the basics: two-step verification, backups, incident notice.
3. Include it in new contracts and in renewals.

You will know it is done when: Critical suppliers have security requirements in their contracts.

Effort: Medium (3-10 working days) · Who: Procurement/Legal, IT · When: Days 31-60
This can help: Supplier security assessment (mineryreport.com)

Management training

Topic 8 · People and suppliers

Not covered

+2 points

You told us: "No"

Why it matters: Without training, management decides blind during an incident: what to stop, who to tell or whether to pay.

What to do

1. Run a session of about two hours for management.
2. Include an exercise: what would you decide during an attack?
3. Repeat it every year.

You will know it is done when: Management has held a session with a practical exercise and has a date for the next one.

Effort: Low (up to 2 working days) · Who: Management · When: Days 61-90

DKIM: no data; we cannot see from outside whether your email is signed.

What you already do well

These points are already at the best answer. Keeping them up counts too.

Risk assessment
You have a recent risk assessment with a plan: your investment decisions rest on what could really bring you to a halt.

Two-step verification
You have two-step verification on email and on access from the internet: a stolen password is no longer enough to get in.

Joiners and leavers
You remove access on the day someone leaves: no doors are left open for people who have gone.

What you expose to the internet
You know what you have exposed to the internet and who maintains it: every way in has someone who maintains it.

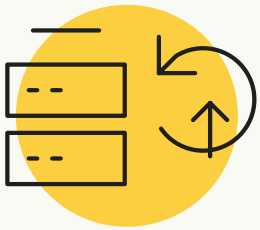
A backup out of an attacker's reach
You have automatic backups with an isolated or immutable copy: you have a copy designed so that ransomware cannot delete or encrypt it.

Incident response plan
You have a written, rehearsed response plan: in the first hours, everyone knows what to do.

05

90-day plan

The tasks from the sheets, in the order in which it makes sense to do them. Not everything gets closed in 90 days: start with what is essential; the rest can wait for the later stretch.



Days 0-30

Security lead and management oversight
Low · Management
Essential

Protection against malware
Low · IT
Essential

Updates
Low · IT
Essential

Tested restore
Low · IT
Essential

Protecting your domain against spoofing
Low · IT

Notification
Low · Procurement/Legal, IT

Security policy
Low · IT

Asset inventory
Low · IT

Days 31-60

Business continuity
Medium · Management, IT

Suppliers
Medium · Procurement/Legal, IT

Administrator accounts
Low · IT

Bank account changes
Low · Management, IT

Days 61-90

Management training
Low · Management

Security testing
Medium · IT

Logs and alerts
Medium · IT

Security awareness
Medium · HR

After 90 days

Critical and personal data
Low · Procurement/Legal

Email and web filtering
Low · IT

Secure configuration and supported software
Medium · IT

06 For your technical team

The technical detail: related standards, what can be seen from outside and how it is calculated.

Impact: how much your score would rise if that question moved to the best answer; it is counted once per question. It is an estimate, not a commitment.

Relationship with standards and frameworks

Only for the points to improve. It is a thematic and, in general, partial relationship: it is not a compliance assessment.

Point	CIS v8.1	ISO 27001	ENS	NIS2
Security lead and management oversight	—	5.1, 5.3, A.5.2	org.1	20.1
Security policy	—	5.2, A.5.1	org.1, org.2	21.2.a
Asset inventory	1.1, 2.1	A.5.9	op.exp.1	21.2.i
Secure configuration and supported software	4.1, 2.2	A.8.9	op.exp.2, op.exp.3	21.2.e
Critical and personal data	3.1, 3.2	A.5.12, A.5.34	mp.info.1, mp.info.2	21.2.i
Administrator accounts	5.1, 5.4	A.8.2, A.5.18	op.acc.4	21.2.i
Protection against malware	10.1, 10.6	A.8.7	op.exp.6	21.2.e, 21.2.g
Updates	7.1, 7.3, 7.4	A.8.8	op.exp.4	21.2.e
Security testing	7.5, 7.6, 18.1, 18.2, 18.3	A.8.8	—	21.2.e, 21.2.f
Protecting your domain against spoofing	9.5	A.5.14, A.8.21	mp.s.1	21.2.g
Email and web filtering	9.2, 9.6, 9.7	A.8.23, A.8.7	mp.s.1, mp.s.3, op.exp.6	21.2.g
Bank account changes	14.2	A.5.37, A.6.3	mp.per.3	21.2.g
Tested restore	11.5	A.8.13, A.5.30	mp.info.6	21.2.c
Business continuity	—	A.5.29, A.5.30	op.cont.1, op.cont.2	21.2.c
Logs and alerts	8.2, 8.9, 8.11	A.8.15, A.8.16	op.exp.8, op.mon.1, op.mon.3	21.2.b
Notification	17.2, 17.3	A.5.5, A.5.24, A.6.8	op.exp.7	23
Security awareness	14.1, 14.2, 14.6	A.6.3	mp.per.3, mp.per.4	21.2.g
Suppliers	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
Management training	14.1	7.2, A.6.3	mp.per.4	20.2

What can be seen from outside example.com

Check	Status	What it means and what to do
SPF	Could improve	Your SPF record only asks for email from unauthorised servers to be marked as suspicious, and your DMARC record does not ask for it to be rejected or quarantined. It ends in «~all» and your DMARC record is not at quarantine or reject. Tighten DMARC or use «-all».
DKIM	No data	We did not find any key with the common selectors. If you know yours, enter it in the advanced option. 14 common selectors tried with no result. Look for the selector in the DKIM-Signature header (s=) of an email you sent.
DMARC	Risk	As published, it does not ask mailboxes to reject or quarantine them. Policy «p=none». Steps: with «p=none» and «rua», review the reports for 2-4 weeks; then «p=quarantine» and, finally, «p=reject». Add «rua=mailto:...» to receive aggregate reports.
MTA-STS	Could improve	You do not have it published. It is not mandatory. To publish it: a TXT record at _mta-sts.example.com with «v=STSv1; id=...» and the policy at https://mta-sts.example.com/.well-known/mta-sts.txt.
DNSSEC	Could improve	Your domain is not signed with DNSSEC. No DS at the parent and no AD bit. Enable it with your DNS provider and publish the DS at the registrar.
CAA	Could improve	You have no CAA record: any certificate authority may issue certificates for your domain.
Security headers	Could improve	You have no Content Security Policy (CSP). Add a Content-Security-Policy with at least «script-src» without «*», without scheme-only sources and without 'unsafe-inline' unless used with nonces or hashes. Add «frame-ancestors 'none'» (or 'self') to the CSP, or «X-Frame-Options: DENY». Add «X-Content-Type-Options: nosniff». No Referrer-Policy: the browser uses its default value.
security.txt	No data	We could not download your security.txt.

Low-intensity public review of 20 October 2026: it does not scan ports or test for vulnerabilities. "No data" does not count as good.

Official sources

- 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
- Spain's National Security Framework (ENS): Royal Decree 311/2022, consolidated text (BOE, in Spanish): https://www.boe.es/buscar/act.php?id=BOE-A-2022-7191
- NIS2: Directive (EU) 2022/2555 (EUR-Lex): https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

How it is calculated

Each answer is worth 100, 50 or 0 ("I don't know" counts as 0) and weighs from 1 to 3 depending on its importance. The score is the weighted average of the questions that apply to you. Levels: High risk (0-39), Room for improvement (40-64), On track (65-84) and Solid (85-100). Seven controls are essential: if any of them is missing, the level is capped even if the score is high. Question bank version: banco-v1.2, reviewed as of 12 October 2026.

Frameworks: CIS Controls v8.1; ISO/IEC 27001:2022; Spain's Royal Decree 311/2022 (ENS, consolidated text in the BOE); Directive (EU) 2022/2555.

Scope and limitations: This assessment is an indicative self-assessment based on your answers and on public information about your domain. It is not an audit, it does not certify compliance with any law or standard and it does not replace a professional analysis. References to laws and standards show which controls each answer relates to, not whether you comply or not. Regulatory status as of 12 October 2026.