Cybersecurity and regulation

Have you ever received an email saying "your package is waiting, click here to pay the customs fee"? Or a message from "your bank" asking you to confirm your password? Now imagine that the person who clicks is not you but the receptionist of a hotel, and the computer behind the click holds the passports of every guest of the season.

Every company you have studied this year depends on its data: bookings, orders, meter readings, patient records. In the city-builder game, all those info views are worthless if anybody can walk into the town hall and change the records, or switch off the power station. Cybersecurity is the police, the walls and the locks of the city. And just like a real city, there are laws that say which locks are compulsory. This lesson covers both, and you will check the locks of a real website yourself, from the outside, without touching anything.

What you will learn

- Explain what security protects: **confidentiality**, **integrity** and **availability**
- Sort security measures into **device**, **system** and **global** level
- Run a **passive** security check of a public website: security headers, cookies before consent and the privacy policy
- Check whether your own email address appears in a known **data breach**
- Explain what the **RGPD**, the **LOPDGDD** and **NIS2** regulate, and decide whether each one applies to a company
- Avoid the trap: securing every laptop is not enough if there is no tested backup

What we protect: confidentiality, integrity, availability

> **Information security** protects information in any form, including paper and people. **Cybersecurity** is the part that protects networks, systems and digital data against attacks and incidents.

Both protect the same three things, often called the **CIA triad** (in Catalan and Spanish, *CID*):

Pillar	What it guarantees	It breaks when…	In the city
Confidentiality	Only authorised people can access the data	A customer database leaks	Strangers reading the town hall's files
Integrity	The data are correct and nobody changed them without permission	Somebody alters prices or marks	Somebody forging the land registry
Availability	Data and systems work when they are needed	An attack or a failure takes the service down	The power station switched off

Remember the Unit 1 lesson on IT and OT: in OT (the plant, the pumps, the machines) **availability** and physical safety usually come first, because a stopped water plant is worse than a leaked spreadsheet. In office IT, confidentiality often gets most attention. It is a general rule, not a law.

Three levels of security

Level	Scope	Typical measures	In the city
Device	Each device: computer, phone, server, sensor	Updates, antimalware, disk encryption, screen lock, strong passwords and **two-factor authentication** (a second proof, such as a code on your phone)	A lock on every door
System	The whole organisation: network, applications, people, processes	Firewall and network segmentation, least privilege, **tested** backups, monitoring, an incident response plan, staff training	The police, the walls, the fire brigade's plan
Global	Sectors, countries and the supply chain	Laws and directives, standards, public incident-response teams, international cooperation, security requirements for suppliers	The laws of the country and the cooperation between cities

Examples of the global level: **ENISA**, the EU Agency for Cybersecurity, and in Spain **INCIBE**, the National Cybersecurity Institute, whose free and confidential helpline **017** serves citizens, companies and professionals.

> **Careful: the device level is not enough**
> A perfectly protected laptop does not save a company with no backups. A firewall does not stop an employee from typing their password into a fake page. The **human factor** (**phishing**: fake messages that trick you into clicking or giving your credentials) crosses all three levels. Security is a system, not a product.

In class: a passive security check of a real website

You will look at your project company's public website the way any visitor's browser does, and nothing more.

> **Passive only**
> You only **look** at what the website already shows to any visitor: its response headers, the cookies it sets in your own browser, its cookie banner and its privacy policy. **Never** scan ports, try passwords, test forms with strange input or use any "hacking" tool against a real company. Doing that without written permission can be a crime under the Spanish Criminal Code. The two online tools below only make an ordinary visit to the home page, like your browser does.

Work **individually**. **No AI tools.**

Step	Do this	You should see
1 · HTTPS	Open the company's website. Click the icon left of the address and look at the certificate: who issued it and until when is it valid?	A padlock or "connection secure", an issuer and an expiry date
2 · Headers	Go to securityheaders.com, paste the address and scan. Write down the grade and which headers are **missing**.	A grade from A+ to F and a list in red and green
3 · Observatory	Do the same in Mozilla HTTP Observatory. Write down the score and the two most important failed tests.	A score and a list of tests

Step	Do this	You should see
4 · Cookies before consent	Open a **private window**, open DevTools (`F12`) → *Application* (*Storage* in Firefox) → *Cookies*, and load the site. **Do not click the banner.** List the cookies already set. Then click *Reject* and reload: did any analytics or advertising cookies (names like `_ga`, `_fbp`) stay?	A list of cookies with their domains
5 · Banner	Is there a cookie banner? Is *Reject* as easy as *Accept* (same level, same size)?	Yes or no, with a screenshot
6 · Privacy policy	In the privacy policy, find: who is responsible, the contact of the data protection officer (if any), the purposes, the retention periods, the rights and how to exercise them, and the right to complain to the AEPD.	A checklist with found / not found
7	Hand in the audit sheet on Classroom: URL, date and time, screenshots, and a table of findings with one recommended measure for each.	

What the most common headers do:

Header	What it does, in one line
`Strict-Transport-Security` (HSTS)	Tells the browser to always use HTTPS for this site
`Content-Security-Policy` (CSP)	Lists where scripts and other content may be loaded from, which limits injected scripts
`X-Frame-Options`	Stops other sites from showing this one inside a frame to trick clicks
`X-Content-Type-Options`	Stops the browser from guessing file types (`nosniff`)
`Referrer-Policy`	Controls how much of the address is sent to other sites when you click a link
`Permissions-Policy`	Switches off browser features the site does not need (camera, microphone, location)

A bad grade is a finding, not proof that the site has been hacked. Write findings politely and with evidence: "on 26/04/2027 at 10:15 the site did not send `Content-Security-Policy`".

Your own email: Have I Been Pwned

Have I Been Pwned is a free service run since 2013 by the security researcher Troy Hunt. It collects the lists of accounts from known data breaches and lets you check whether **your own** email address appears in them. It asks only for the email, **never** for a password.

Check your own address (only yours). If it appears: change the password of that service and of any other where you reused it, use a different password per site (a password manager helps) and switch on two-factor authentication. **Do not** hand in your result: it is personal data. In the Classroom activity just answer "what would a company do if an employee's email appeared in a breach?".

The laws: RGPD, LOPDGDD and NIS2

	RGPD (GDPR in English)	LOPDGDD	NIS2
Official name	Regulation (EU) 2016/679	*Ley Orgánica 3/2018*, of 5 December	Directive (EU) 2022/2555

	RGPD (GDPR in English)	LOPDGDD	NIS2
Type	EU regulation: applies directly in every member state, since 25 May 2018	Spanish organic law, in force since 7 December 2018	EU directive: each state must **transpose** it into its own law; deadline 17 October 2024
Protects	People, regarding the processing of their **personal data**	The same: adapts and completes the RGPD in Spain and adds **digital rights** (for example, digital disconnection at work)	The **networks and information systems** of key sectors
Who it binds	Anybody who processes personal data of people in the EU, whatever their size	Processing subject to Spanish law	**Essential** and **important** entities in the sectors of its annexes, usually from medium size up
Key ideas	Principles, legal basis, rights, privacy by design, breach notification within 72 hours	The authority is the **AEPD** (*Agencia Española de Protección de Datos*)	Risk management, incident reporting (24 h early warning, 72 h notification, final report within one month), management accountability, supply-chain security
Maximum fines	Up to €20 million or 4% of worldwide annual turnover, whichever is higher	Classifies RGPD infringements as very serious, serious or minor	Up to €10 million or 2% of turnover for essential entities; €7 million or 1.4% for important ones

RGPD: what a developer needs to know

- **Personal data**: any information about an identified or identifiable person: name, email, ID number, IP address, location. **Special categories** (health, biometric and genetic data, political opinions, religion, ethnic origin, sexual orientation…) have extra protection.
- **Principles**: lawfulness, fairness and transparency; purpose limitation; **data minimisation** (collect only what you need); accuracy; storage limitation (the deletion stage of the lifecycle); integrity and confidentiality; accountability.
- **Rights**: access, rectification, erasure, restriction, portability and objection.
- **Roles**: the **controller** decides what the data are for; the **processor** handles them on the controller's behalf (a cloud provider, a software company).
- **Privacy by design and by default**: privacy is planned when the application is designed, not patched at the end.
- **Breaches**: a breach of personal data must be notified to the AEPD without undue delay and, where feasible, within **72 hours**, unless it is unlikely to be a risk to people.

Cookies have their own Spanish rule: Article 22.2 of the information society services law (*Ley 34/2002*, LSSI) requires informed consent before storing cookies that are not strictly necessary. The AEPD's cookie guide (updated in May 2024) adds that rejecting must be as easy as accepting. That is what you checked in steps 4 and 5.

NIS2 in Spain

NIS2 replaced the first NIS directive (2016/1148). As of October 2026, **Spain has not yet transposed it**: the government approved the draft *Ley de Coordinación y Gobernanza de la Ciberseguridad* on 14 January 2025, and on 8 July 2026 the European Commission referred Spain (with Ireland, France and the Netherlands) to the EU Court of Justice for not transposing it. Meanwhile, *Real Decreto-ley 12/2018*, which transposed the first NIS directive, is still in force. **Check the BOE** when you write your deliverable: this may have changed.

Does it apply to my company?

Question	If yes
Does the company process personal data of people in the EU (customers, employees, patients)?	**RGPD** and, in Spain, **LOPDGDD** apply. Almost every company answers yes.
Does its website use cookies that are not strictly necessary?	**LSSI** Article 22.2: consent first
Is it in an NIS2 Annex I sector? Energy, transport (air, rail, water, road; ports and airports), banking, financial market infrastructure, health, drinking water, waste water, digital infrastructure, ICT service management, public administration, space	Possibly **essential** (if large) or **important** entity
Is it in an Annex II sector? Postal services, waste management, chemicals, food (industrial production, processing and wholesale distribution), manufacturing of some products, digital providers, research	Possibly an **important** entity
Is it at least medium-sized: 50 employees or more, or annual turnover and balance sheet above €10 million?	Needed, in general, for NIS2 to apply; smaller companies can still be affected as **suppliers** of an entity that is covered

A hotel chain: RGPD and LOPDGDD yes; tourism is not an NIS2 sector. A water company: RGPD and LOPDGDD yes, and drinking water is in NIS2 Annex I.

For your project

The passive audit is **section D** of Deliverable 5 (the fourth member's section). The question "which of RGPD, LOPDGDD and NIS2 apply, and why" is the **group part**, together with the risk table: each risk, which pillar of the triad it threatens, its level and the measure that reduces it.

Key takeaways

- Security protects **confidentiality**, **integrity** and **availability** (the CIA triad).
- Measures act at **device**, **system** and **global** level; the human factor (**phishing**) crosses all three.
- A **passive** audit only looks at what any visitor sees: headers, cookies, banner, privacy policy. Never scan or try logins on a real company.
- The **RGPD** (Regulation (EU) 2016/679) and the **LOPDGDD** (Ley Orgánica 3/2018) protect people's personal data; **NIS2** (Directive (EU) 2022/2555) protects the networks and systems of key sectors.
- As of October 2026 Spain has not transposed NIS2; Royal Decree-law 12/2018 is still in force.
- Cookies that are not strictly necessary need consent first (LSSI Article 22.2).

Quick check

1 A denial-of-service attack takes the booking website offline for a day. Which pillar is hit hardest?

- **A** Confidentiality
- **B** Integrity
- **C** Availability
- **D** None: no data were stolen

2 Encrypting a laptop's disk is a measure at which level?

- **A** Device
- **B** System
- **C** Global
- **D** None: encryption is not a security measure

3 Which of these is allowed in this course's security activity?

- **A** Scanning the company's server ports to see what is open
- **B** Trying common passwords on the staff login page
- **C** Reading the response headers and the cookies the site sets in your own browser
- **D** Sending strange input to the contact form to see if it breaks

4 Which law applies directly in every EU state without being transposed?

- **A** The RGPD, Regulation (EU) 2016/679
- **B** NIS2, Directive (EU) 2022/2555
- **C** The LOPDGDD, Ley Orgánica 3/2018
- **D** Real Decreto-ley 12/2018

5 A booking app asks for date of birth, ID number and food allergies just to book a table. Which RGPD principle does it break most clearly?

- **A** Portability
- **B** Data minimisation
- **C** Accuracy
- **D** Availability

6 When you load a site in a private window, before touching the banner, DevTools already shows a `_ga` analytics cookie. What does it suggest?

- **A** Nothing: all cookies are allowed until you click
- **B** A cookie that is not strictly necessary may have been set before consent, which LSSI Article 22.2 does not allow
- **C** The website has been hacked
- **D** The RGPD does not cover websites

7 Your project company is a medium-sized drinking-water utility in Mallorca with an online customer area. Pick the two true statements.

- **A** RGPD and LOPDGDD apply, because it processes customers' personal data
- **B** Only NIS2 applies, because water is infrastructure
- **C** Drinking water is an NIS2 Annex I sector, so it is likely an entity under NIS2 once Spain transposes it
- **D** No law applies until Spain transposes NIS2

You have now covered the whole unit. Put it together for your company in Deliverable 5 · Data and security brief.

Solutions

1. C · Nobody read or changed the data, but the service did not work when it was needed. That is **availability**.

2. A · It protects **one device**. Network segmentation or tested backups for the whole company would be **system** level.

3. C · Only **passive** checks: looking at what the site already shows to any visitor. The other three probe the company's systems without permission.

4. A · An EU **regulation** applies directly. A **directive** such as NIS2 must be transposed by each state, and the LOPDGDD and the royal decree-law are Spanish laws.

5. B · **Data minimisation**: collect only what the purpose needs. An allergy is also health data, a special category.

6. B · Analytics cookies are not strictly necessary, so consent should come **first**. It is a finding to report politely with evidence, not proof of an attack.

7. A, C · The laws **add up**: personal data bring in the **RGPD** and **LOPDGDD**, and the sector and size bring in **NIS2**. The RGPD applies today regardless of the NIS2 transposition.