



AUTHOR Álvaro Rodríguez	Published by International Sustainable Development Observatory (ISDO) Security and Intelligence Department isdo.ch
Scope Counterintelligence and Economic Security	Date October 9, 2026

Contents

Executive summary

1. Introduction, scope and methodology
2. Anatomy of the threat
3. Developments 2025-2026
4. An intelligence problem, not just a cybersecurity one
5. Exposure of Spanish organizations
6. Warning indicators
7. Controls and roadmap
8. Conclusions and recommendations

Bibliography

Annex. Glossary

Executive summary

North Korea maintains a state network of IT professionals who obtain remote jobs at foreign companies under false or stolen identities. Their salaries are channeled to the regime agencies that fund its nuclear weapons and ballistic missile programs. What began as a revenue fraud has become a multilayered threat: those who land a job obtain legitimate credentials, access to internal systems and, in some cases, the ability to steal intellectual property, extort the employer or support operations by other actors linked to the North Korean state.

On 31 July 2026, the United States and ten other countries issued a joint alert addressed to governments, companies and online platforms. The document acknowledges that these workers integrate artificial intelligence to hide their identity and increasingly rely on intermediaries to create accounts, pass interviews and even establish in-person contact. Spain is not among the signatory authorities, although its business fabric, especially the technology, industrial and defense sectors, shares the exposure factors described in the sources.

This report synthesizes the state of the threat as of October 2026, analyzes its evolution over the last eighteen months and assesses what it means for Spanish organizations. Its central thesis is that **defense cannot rest on the cybersecurity team alone**: it requires coordinating Human Resources, Security, Compliance, Legal Counsel and hiring managers under an identity verification and insider risk management model.

Assessment and priorities. For Spain, the risk should be treated as plausible and high-impact, although without verified public cases. It is the kind of risk where waiting for local evidence amounts to discovering it too late. The recommendations in section 8 are organized into three blocks: governance decisions that management can take within weeks and that require no significant investment (a single owner, an inventory of critical positions, proportionate verification and payment control); controls over the device, access and the supplier, which close the routes that are most profitable for the attacker; and detection, response and sector cooperation capabilities, which take longer but reduce residual risk and prevent re-infiltration. There is no need to wait for NIS2 to be transposed in order to start.

Table 1. Key figures

Indicator	Figure	Source
Countries signing the joint alert	11 (31 July 2026)	U.S. Department of State and FBI
Companies with FAMOUS CHOLLIMA operatives detected by CrowdStrike (12 months to June 2025)	More than 320, 220% more than the previous year	CrowdStrike
Estimated revenue of IT workers abroad (2024)	Between USD 350 million and USD 800 million	MSMT; The Korea Herald
Crypto-assets stolen by North Korean actors	USD 1,190 M (2024) and USD 1,650 M (Jan.-Sep. 2025)	MSMT; The Korea Herald
Countries hosting North Korean workers in violation of UN resolutions	At least 17; between 35,600 and 101,280 people	Japan's Ministry of Foreign Affairs (MSMT)
Intermediary identities managed by a single convicted facilitator	Up to 871, with 40 U.S. companies affected	U.S. Department of Justice

Table 2. Key judgments and confidence level

Analytical judgment	Confidence	Main basis
The threat remains active and adapts to law enforcement and judicial pressure by shifting to new countries and tactics.	High	U.S. Department of State and FBI; Google Threat Intelligence Group; MSMT
Generative AI significantly lowers the cost of fabricating credible identities and passing interviews.	High	U.S. Department of State and FBI; CrowdStrike
Local facilitators are the most vulnerable link and the one with the most convictions.	High	U.S. Department of Justice; CyberScoop; Fortune
Spanish organizations have been or will be targeted by the same operating model.	Medium	Google Threat Intelligence Group; U.S. Department of State and FBI
The real number of infiltrations far exceeds what is publicly documented.	Medium	CrowdStrike; Center for Strategic and International Studies

1. Introduction, scope and methodology

1.1. Context

For years, the debate on threats from North Korea focused on the theft of crypto-assets and on intrusions by groups known as Lazarus. Remote hiring has opened a different path: instead of breaking down the door, the actor applies for the job, passes the selection process and receives a corporate laptop, an email account and a salary. The threat does not enter through the network but through the hiring process.

This dynamic has become more relevant for three reasons. First, remote work and hiring through *freelance* platforms have become normalized. Second, generative AI tools make it possible to produce résumés, professional profiles, translations and, according to several sources, real-time manipulated video. Third, pressure from U.S. authorities has pushed operators to look for markets with less awareness of the problem, Europe among them.

1.2. Scope

The report focuses on the remote IT worker scheme and its implications for insider risk, sanctions compliance and information protection. Outside its scope, except for contextual mention, are offensive crypto-asset theft operations not linked to IT workers, and the North Korean labor program in non-technology sectors, which the Multilateral Sanctions Monitoring Team (MSMT) addressed in its third report.

1.3. Methodology and sources

The analysis is based on open sources. Priority has been given to institutional and primary documents: government alerts, U.S. Department of Justice press releases, MSMT reports, threat intelligence reports from Google and CrowdStrike, and European and Spanish legislation. Journalistic sources and those from commercial vendors have been used as a complement and are identified as such in the bibliography. Where a figure comes from a vendor with a commercial interest, the text says so.

Note on the presence of Spain in the sources. Some Spanish media reported in 2025 that the Google Threat Intelligence Group report cited operations in Spain. The text of the original report expressly cites Germany, Portugal and the United Kingdom as European countries with observed activity. The figure in the report listing the affected countries could not be checked in its graphic version. As a precaution, this report does not claim that confirmed incidents exist in Spain and treats Spanish exposure as a risk analysis, not as a documented fact.

Evidence and judgment. The report distinguishes between what the sources state and what the analyst concludes. The confidence levels in Table 2 refer to the former. The probabilities, the inferences about Spain and the priorities in section 8 are qualitative judgments by the analyst, formulated from documented patterns, and are identified as such in the text. They should be reviewed when new evidence appears, in particular if a case is confirmed in Spain.

2. Anatomy of the threat

2.1. Who is behind it

North Korean IT workers are not independent freelancers. According to the MSMT, they belong to entities subordinate to UN-sanctioned bodies, including the Reconnaissance General Bureau, the Ministry of Atomic Energy Industry, the Ministry of Defense and the Munitions Industry Department, and they remit roughly half of their income to the regime. They operate mainly from North Korea, China and Russia, although also from countries in Southeast Asia and Africa.

These are highly technically qualified professionals. Government alerts note that they look for work in web development, mobile applications, software and blockchain. The MSMT estimates that a typical worker earns between USD 3,500 and USD 10,000 per month, and that top performers earn much more. An analysis by IBM X-Force and Flare describes very long working days, averaging between 11 and 14 hours a day in the cases examined, and meticulous tracking of the volume of applications and messages.

2.2. The operating cycle

Although there are many variants, official alerts and intelligence reports make it possible to describe a common cycle. Table 3 summarizes it in five phases and indicates where an organization can intervene.

Table 3. Operating cycle and points of intervention

Phase	What happens	Possible control point
1. Identity preparation	Creation or purchase of real or synthetic identities, forged documents and profiles on professional and code platforms. Use of proxies that supply images of identity documents.	Reinforced document verification; cross-checking of professional history and verifiable code.
2. Recruitment	Mass applications on <i>freelance</i> platforms and in selection processes. Use of third parties to take part in interviews and of AI for résumés and translations.	Camera-on interviews, unpredictable questions and, for sensitive positions, in-person verification.
3. Onboarding	Receipt of the laptop at an intermediary address (<i>laptop farm</i>) or use of the worker's own device in BYOD environments.	Control of shipment and equipment location; policy of managed corporate devices.
4. Exploitation of access	Ordinary work, access to repositories and data, and in some cases installation of remote access or exfiltration tools.	Monitoring of access anomalies, remote sessions and data transfers.
5. Payment and laundering	Payments to third-party accounts, transfer services or cryptocurrencies, with a commission for the intermediary.	Match between employee name and account holder; rejection of third-party payments.

Analytical reading of the table. The controls in phases 1 and 2 are the cheapest and the ones that act earliest, but they are also the ones under the most pressure from generative AI. Those in phases 4 and 5 are harder to evade, because the operative needs to gain access and get paid, although they act later. No single phase is enough on its own. The defensive value lies in the fact that the scheme is a chain: the operative must get through every phase, while the organization only needs to break one. That is why the recommended design combines a preventive control at the entry point (identity), a structural one in the middle (device and least privilege) and a verification control at the end (payment), so that the failure of one does not compromise the whole. A video interview, on its own, no longer proves identity.

2.3. The facilitator ecosystem

The element that has appeared most often in court proceedings is the local facilitator. The joint alert describes third parties who host *laptop farms*, that is, corporate computers sent by deceived companies to which the operatives connect remotely, which conceals their true location. A senior U.S. Department of Justice official stated in a sentencing memorandum that these schemes would not succeed without U.S. facilitators.

Recent convictions illustrate the scale. A Ukrainian national was sentenced to 60 months in prison for managing

up to 871 intermediary identities and supporting laptop farms that affected 40 U.S. companies. In April 2026, two U.S. citizens were sentenced for operating laptop farms using the stolen identities of more than 80 people, generating more than five million dollars for the regime. In May 2026, two others received 18 months in prison for hosting computers that benefited around 70 companies and generated 1.2 million dollars. The Department of Justice has for years been developing a specific initiative against domestic facilitators.

The phenomenon is not limited to natural persons. A security researcher cited by the U.S. press notes that the networks increasingly use U.S.-based limited liability companies to give the appearance of a legitimate employment relationship. This is a pattern that deserves attention in supplier approval processes.

2.4. Economic dimension

The economic magnitude moves within wide ranges and should be treated with caution, because it comes from estimates and not from accounting records. The MSMT second report estimates that IT workers abroad earned between USD 350 million and USD 800 million in 2024. The third report, published on 16 September 2026, calculates that the North Korean workforce deployed in at least 17 countries, which includes non-IT sectors, generates between USD 450 million and USD 800 million annually. Both ranges correspond to different universes and must not be added together.

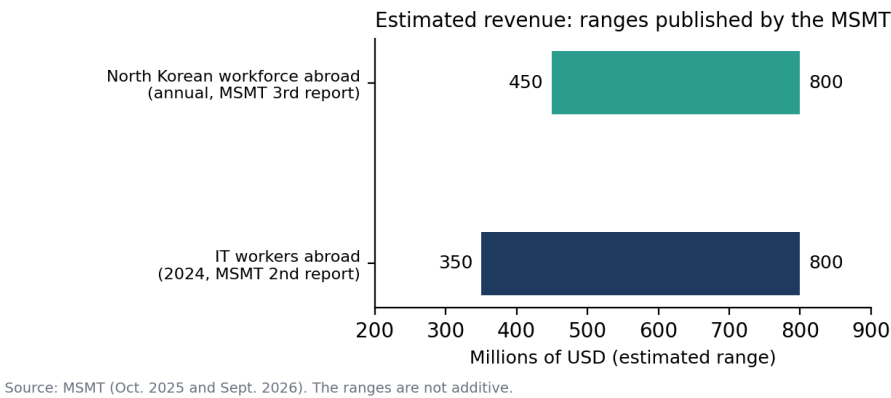


Figure 1. Estimated revenue ranges published by the MSMT. The two intervals correspond to different universes and are not additive.

These revenues fit into a broader cyber war economy. The MSMT attributed to North Korean actors the theft of some USD 1,190 million in crypto-assets during 2024, equivalent to roughly one third of the regime's foreign currency income that year, and a further USD 1,650 million between January and September 2025. A State Department official raised the 2025 figure to more than USD 2,000 million.

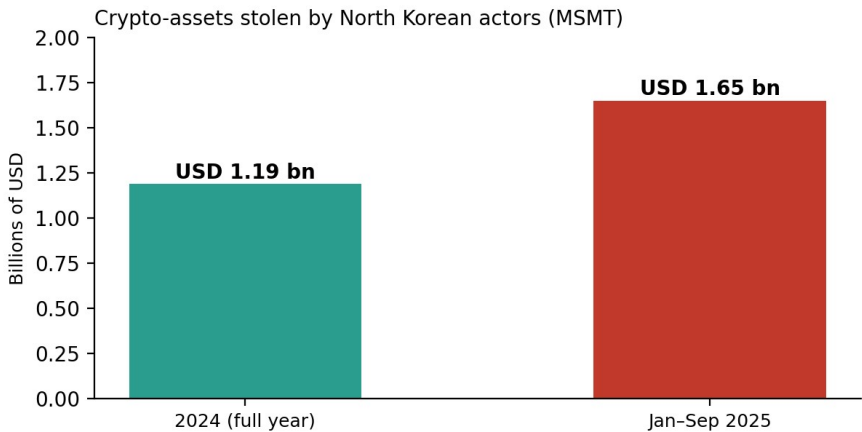


Figure 2. Crypto-assets stolen by North Korean actors according to the MSMT. The 2025 data cover January to September.

3. Developments 2025-2026

3.1. From résumé to synthetic identity: AI as a multiplier

The 2026 joint alert expressly includes the integration of AI among the techniques used to conceal identities and expand global activity. CrowdStrike describes this in detail: according to its 2025 report, the group it calls FAMOUS CHOLLIMA used generative AI at every stage of the hiring and employment process, including résumé writing, programming support and, according to the available data, real-time *deepfake* technology during video interviews.

This has an important defensive implication. Classic indicators, such as grammatical errors or poor English, lose value. The alert itself warns that language models make it possible to produce convincing profiles and communications in a second language. For a Spanish organization, this means that language, which might seem a natural barrier, no longer is one.

The right consequence needs to be drawn. The point is not to buy a deepfake detector that replaces human judgment: automated detectors compete against generation and produce false positives and false negatives. The most robust defense consists of redesigning the process so that identity has to be proven through facts that are hard to simulate remotely and at scale: a document checked against the issuing source where possible, a liveness test with unpredictable interaction, a match between the person who is interviewed, the person who signs and the person who gets paid and, for critical positions, an in-person meeting. AI lowers the cost of appearance, but not that of physical presence or of financial traceability.

3.2. From revenue fraud to espionage, extortion and theft

The Google Threat Intelligence Group (GTIG) concluded that, since late October 2024, IT workers have increased the volume of extortion attempts and gone after larger organizations: after being dismissed, they threatened to leak the employer's sensitive data or hand it to competitors, including source code. GTIG observed that this increase coincided with the intensification of judicial action in the United States and raised a possible causal link: pressure on the workers might be pushing them toward more aggressive tactics.

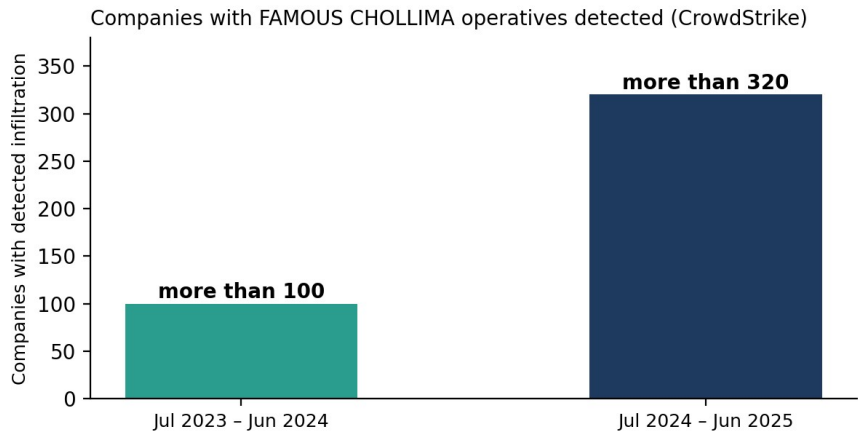
The 2026 alert confirms the insider-threat nature of the problem: these workers take part in data exfiltration, cryptocurrency theft and the removal of sensitive information. An analysis by CSIS adds that they infiltrate defense and critical infrastructure contractors. On 28 July 2026, the FBI confirmed, according to the specialized press, that it is investigating the case of a North Korean who worked as a remote IT worker for a U.S. federal agency.

3.3. Geographic expansion and displacement

In April 2025 GTIG documented an increase in active operations in Europe, confirming the spread of the threat beyond the United States. It attributed this shift to greater public awareness, to Department of Justice indictments and to the difficulty of verifying the right to work in the U.S. In Europe it observed activity linked to Germany, Portugal and the United Kingdom, with projects in web development, bots, content management systems and *blockchain*.

The same report describes a worker who operated at least a dozen different personas in Europe and the United States, with a particular interest in the defense industry and the public sector, and who used false references and other identities under his control to vouch for himself to recruiters. The operatives claimed nationalities as diverse as Italy, Japan, Malaysia, Singapore, Ukraine, the United States and Vietnam, and were hired through platforms such as Upwork, Telegram and Freelancer. Payments were channeled through cryptocurrencies, TransferWise and Payoneer. GTIG also found a corporate laptop destined for New York that was operating in London, revealing a complex logistics chain with facilitators in both countries.

Another vulnerability was identified in policies on the use of personal devices (*bring your own device*, BYOD). When corporate laptops are not distributed, usual traces such as shipping addresses or the software inventory of the machines disappear. GTIG indicated that, since January 2025, the workers have been operating against their employers in environments of this kind.



Source: CrowdStrike, Threat Hunting Report 2024 and 2025. Own elaboration.

Figure 3. Companies with FAMOUS CHOLLIMA operatives detected by CrowdStrike. The figures are minimum thresholds (more than 100 and more than 320).

3.4. Timeline of milestones

Table 4. Relevant milestones, 2024-2026

Date	Milestone	Source
Apr. 2024	The mandate of the UN Panel of Experts on North Korea ends.	Japan's Ministry of Foreign Affairs (MSMT)
Oct. 2024	The MSMT is created to monitor the implementation of UN sanctions.	MSMT; Japan's Ministry of Foreign Affairs
Dec. 2024	The U.S. Department of Justice indicts fourteen North Korean nationals over a fraudulent remote employment scheme.	U.S. Department of Justice
1 Apr. 2025	GTIG confirms the expansion to Europe and the rise in extortion and in the use of BYOD environments.	Google Threat Intelligence Group
Aug. 2025	CrowdStrike reports that FAMOUS CHOLLIMA infiltrated more than 320 companies in 12 months (+220%).	CrowdStrike
22 Oct. 2025	The MSMT publishes its second report on cyber activity and IT workers.	MSMT
Apr. 2026	Two U.S. facilitators are sentenced in Boston for a network that affected more than 80 identities.	CNN; U.S. Department of Justice
May 2026	Two 18-month sentences for hosting laptop farms.	U.S. Department of Justice; CyberScoop
28 Jul. 2026	The FBI confirms an investigation into a North Korean remote worker at a federal agency.	TechCrunch
31 Jul. 2026	Joint alert from eleven countries to governments, companies and platforms.	U.S. Department of State and FBI; Baker McKenzie
16 Sep. 2026	Third MSMT report on the North Korean workforce abroad.	MSMT; Japan's Ministry of Foreign Affairs

3.5. The international response

The 31 July 2026 alert is issued by the State Department and the FBI together with authorities from Japan, South Korea, Australia, Canada, France, Germany, Italy, the Netherlands, New Zealand and the United Kingdom. It asks

platforms to strengthen identity verification, with strict document review and in-person interviews, and to detect suspicious accounts. It also recalls that Security Council Resolution 2397 requires member states to repatriate North Korean nationals who earn income in their jurisdiction, and that hiring and paying these workers may breach national law. A legal analysis notes that companies employing North Korean workers, even unknowingly, may face liability for sanctions and export control violations.

There is a relevant analytical consequence: four of the signatories (France, Germany, Italy and the Netherlands) are European Union member states, and those same countries take part in the MSMT. Spain is outside both mechanisms, so its organizations do not receive the same institutional early-warning signal, which reinforces the need for companies and infrastructure operators to keep themselves informed.

4. An intelligence problem, not just a cybersecurity one

4.1. Hybrid nature

This threat is not well detected with purely technical tools, because the actor operates with valid credentials and, for much of the time, does real work. The IBM X-Force and Flare researchers conclude that defending an organization against this infiltration is not only a matter for security teams: it requires a joint effort by Human Resources, security operations, hiring managers and interviewers. In intelligence terms, the challenge lies in connecting signals that live in different systems: the selection process, access control, payroll and team management.

A useful way to picture the problem is the signal map: each relevant indicator resides in a different system, with a different owner, which rarely talks to the others.

- **Selection (applicant tracking system, HR mailbox):** camera refusal, discrepancies between documents, repeated applications with recycled data.
- **Identity and access (identity management, VPN, endpoint):** locations and schedules incompatible with what was declared, remote access tools, activity peaks.
- **Payroll and finance:** account holder different from the contractor, frequent changes to payment details, requests to be paid in crypto-assets.
- **Procurement and suppliers:** opaque subcontracting, interchangeable staff, recently created companies with no track record.
- **Development teams:** unusual volume of repository cloning, interest in information unrelated to the role.

No single owner sees the whole pattern. The organizational implication is that the analytical value lies in correlation, and that the identity risk desk proposed in section 8 exists precisely for that.

4.2. Attribution and links to other actors

The MSMT documents the deep connections between UN-sanctioned North Korean entities and their cyber activities, which span crypto-asset theft, fraudulent IT work and cyber-espionage. GTIG has also noted that the workers exploit their privileged access to facilitate or carry out intrusions, and that they rely on front companies and facilitators. In November 2025, the U.S. Treasury designated several individuals and entities linked to the laundering of cyber revenue and of IT worker income, among them the Korea Mangyongdae Computer Technology Corporation.

4.3. The problem of persistence

Detecting and dismissing an operative does not close the case. GTIG observed that, in the past, dismissed workers tried to be rehired using references from their other identities, and that post-dismissal extortion became part of the pattern. A recent legal analysis describes a re-infiltration cycle: the workers return the equipment through collaborators, abandon the identity and start again with new profiles. This turns incident management into an intelligence exercise: it is necessary to retain indicators (infrastructure, application patterns, payment accounts, shipping addresses) and share them with the sector.

4.4. What we do not know

It is worth stating the information gaps honestly. There is no reliable figure for the number of active workers, nor for the number of organizations affected in Europe. Data from commercial vendors are neither homogeneous nor independently verifiable. A candidate-verification vendor, for example, analyzed a sample of 175,000 job

applications in the United States and detected risk patterns associated with these schemes, with a concentration of declared addresses in Texas; this is useful as an indication, but it comes from a company that sells detection services. Nor do we know to what extent public data reflect successfully detected cases as opposed to cases that remain undiscovered.

5. Exposure of Spanish organizations

5.1. What we know and what we do not

The primary sources consulted document activity in Germany, Portugal and the United Kingdom, and a general expansion toward Europe. The primary sources examined contain no list of incidents in Spain. That absence does not imply an absence of risk. The operating model rests on factors that do not depend on the country: global hiring platforms, distributed teams, video-based selection processes and international payments. An institutional context helps situate the risk: the North Korean embassy in Madrid closed in November 2023, so the regime has no diplomatic presence in Spain and has more incentive to act through intermediaries and indirect structures. This last statement is an inference by the author, not a documented fact.

5.2. Exposure factors

Table 5. Exposure factors for Spanish organizations

Factor	Why it matters	Most exposed profiles
Remote hiring and <i>freelance</i>	The operatives apply for jobs on global platforms, and the MSMT and the alert point to the use of proxies to register accounts.	Technology companies, <i>startups</i> , consultancies and development agencies.
BYOD policies and virtualized access	Without a corporate device there is no logistics trail and no endpoint telemetry.	Organizations that outsource development and prioritize speed of onboarding.
Strategic sectors	The documented interest in the defense industry, the public sector and critical infrastructure contractors.	Defense, aerospace, energy, transport, public administrations and their suppliers.
Blockchain, fintech and digital assets	This is the sector where the projects and the associated crypto-asset thefts are concentrated.	Payment platforms, <i>exchanges</i> and <i>blockchain</i> development companies.
Supply chain and subcontracting	The operative can arrive through a supplier or a shell company that gives the appearance of verification.	Any organization that buys external development or support.
AI and translation	Language ceases to be a protective barrier.	Organizations that believe Spanish protects them.

Why the direct employment contract does not appear to be the main vector (analyst judgment). An exposure analysis must distinguish between entry routes. Employment under a contract in Spain requires a NIF or NIE tax/foreigner identification number, registration with Social Security, tax withholdings and, as a rule, a bank account in the SEPA area. These are frictions that do not exist, or that can be outsourced, when hiring self-employed professionals, on freelance platforms and in subcontracting to development suppliers. This report therefore infers that the most likely vector in Spain is not the direct employee but the self-employed professional and, above all, the staff of a supplier or subcontractor whose verification the organization delegates. The inference is not documented in the primary sources and should be tested against real cases when they exist, but it directs defensive effort toward third-party contracts, which tend to receive less control than the workforce. There are also factors that may favor the defense: average salaries lower than in the United States, which reduce the relative profitability of the target, and a professional environment in Spanish that, although no longer an absolute barrier, still makes impersonation more costly in roles with a lot of spoken interaction.

5.3. Applicable regulatory framework

The European sanctions framework against North Korea is set out in Council Regulation (EU) 2017/1509, which prohibits, among other measures, transferring funds to and from the DPRK and making funds or economic resources available to the persons and entities listed in its annexes. The flow of salaries to regime agencies through

intermediaries raises possible exposure to these rules, the assessment of which falls to each organization's legal counsel and is not addressed here in a conclusive manner.

On the security side, Directive (EU) 2022/2555 (NIS2) requires covered entities to adopt risk management measures that include human resources security, access control and asset management, as well as supply chain security. An internal infiltration incident may, depending on its scope, give rise to notification and data protection obligations under Regulation (EU) 2016/679 (GDPR) where there is unauthorized access to personal data.

Status of NIS2 transposition. At the time of writing, the sources consulted, which are secondary in nature, indicate that the transposition of NIS2 into Spanish law was still in progress: the Council of Ministers approved the draft Cybersecurity Coordination and Governance Act in January 2025, and the European Commission had asked Spain to complete the transposition. Its current status should be checked in the Official State Gazette (BOE) before basing decisions on it. In the meantime, the management of personnel and third-party risk does not depend on that law: the National Security Scheme, data protection rules and organizations' own information security policies already require or support it within their scope of application, and organizations that prepare now will arrive ahead of the curve when the law enters into force.

5.4. Legal and ethical tensions of verification

Tightening identity control calls for a delicate balance. Measures must respect the principles of data minimization and proportionality under the GDPR and Organic Law 3/2018. The processing of biometric data is subject to especially demanding rules, and the employer monitoring contemplated in Article 20 of the Workers' Statute is admissible only within limits of dignity and proportionality. Law 15/2022 on equal treatment and non-discrimination also prohibits treating candidates unfavorably on grounds of origin or nationality. A U.S. analysis by Holland & Knight reaches a parallel conclusion: hiring, investigation and dismissal decisions should rest on objective, job-related indicators, and not on assumptions about national origin, ethnicity or immigration status.

The practical consequence is that **the screening criterion must be behavior and verifiability, not nationality**. The operatives claim, precisely, third-country nationalities, so filtering by origin would be ineffective and, in addition, discriminatory.

5.5. Plausible scenarios

The following scenarios are analytical hypotheses built from documented patterns. They do not describe verified incidents in Spain.

Table 6. Hypothetical scenarios for Spanish organizations

Scenario	Description	Early signal
A. Subcontracted developer	A development supplier onboards a profile with a European identity who works from his or her own device and accesses the client's repository.	Working hours incompatible with the declared time zone; camera refusal; payments to third-party accounts.
B. Position at a defense or infrastructure company	An operative secures a contract at a tier-2 supplier of a contractor and gains access to technical documentation.	Interest in information unrelated to the role; mass downloads of documentation.
C. Extortion after dismissal	After being detected and dismissed, the operative threatens to leak source code or data.	Recent dismissal of a profile with broad access; contact messages with financial demands.
D. Re-infiltration	The same network applies again for positions with a new identity at the same organization.	Matches in infrastructure, text or application patterns with previous cases.

6. Warning indicators

The 2026 joint alert lists specific indicators. None is conclusive on its own, but a combination of several raises the

probability that the candidate is fraudulent. Tables 7 and 8 organize them by area.

Table 7. Indicators in hiring and in dealings with the candidate

Indicator	Observation
Refusal of video conferences	The candidate avoids camera meetings or repeatedly makes excuses.
Discrepancies in the video	Identity document that does not match, or an image that appears manipulated or artificially generated.
Profile with language errors	Expressions suggesting machine translation. Warning: AI can hide this indicator.
Below-market rates	Job offers far below the average.
Several people behind one account	The person on the other end changes depending on the time of day.
Payment in cryptocurrency	Request to be paid by means that hinder traceability.

Table 8. Indicators on platforms, payments and technical activity

Indicator	Observation
Frequent changes to registered data	Name, contact details or bank account that change frequently.
Account holder different from the employee	The worker's name does not match the name on the payment account.
Reused document	Several accounts created with the same identification document.
Altered documents	Images with signs of editing.
Anomalous IP patterns	Several accounts from the same IP, or one account from many IPs in a short time.
Excessive activity	Sessions open for unusually long periods or unnaturally high accumulated hours.
Unusual remote access	Remote desktop tools, VPN or a device located somewhere other than the declared location.
Fake reviews	Accounts that post false reviews about themselves.

Warning about false positives. Many of these indicators can occur among legitimate workers, for example professionals who refuse to turn on the camera for privacy reasons or who are paid in cryptocurrency. They should be used to trigger additional verification and not as an automatic cause for rejection.

How to combine the indicators. It is proposed to group the signals into three families: identity (documents, video, profile consistency), conduct (working hours, access tools, activity patterns) and money (account holder, changes to payment details, crypto-assets). As a starting rule, a single signal should not block anyone. A coincidence of signals from at least two different families, or of three within the same family, should trigger reinforced verification carried out by someone other than the person who selected or manages the candidate. Confirmation of a material inconsistency in identity or payment should escalate to the protocol in section 7.3. The specific thresholds must be calibrated against each organization's experience and reviewed with the DPO so that the processing is proportionate. This is an analyst judgment, not a rule laid down by the official alerts.

7. Controls and roadmap

7.1. Principles

- **Verify real identity, not just documentary identity.** The joint alert recommends in-person interviews for the highest-risk positions and strict document review.
- **Reduce implicit trust.** Apply the principle of least privilege, segment access to code and sensitive data, and limit new employees' access during an initial period.

- **Control the device and the payment.** Managed corporate devices, no BYOD for sensitive positions, and payments only to accounts whose holder matches the employee.
- **Govern the process as a cross-cutting risk.** A single owner of employment identity risk, with HR, Security, Compliance and Legal Counsel at the same table.
- **Apply proportionality.** Any control measure must comply with data protection, labor and equality law.

7.2. Phased roadmap

Table 9. Proposed roadmap

Horizon	Actions	Expected result
0-30 days	Inventory remote and subcontracted roles with sensitive access. Check whether payment accounts held by third parties exist. Include the indicators from Tables 7 and 8 in interview guides. Brief HR and hiring managers.	Exposure map and basic awareness.
30-90 days	Establish reinforced verification (video, document, professional cross-checking) and an in-person verification criterion for critical positions. Restrict BYOD in sensitive positions. Contractual clauses with suppliers on verification of their staff.	Documented procedure and aligned suppliers.
90-180 days	Monitoring of access anomalies, remote sessions and exfiltration for newly onboarded profiles. Response protocol and evidence preservation. Simulation exercise with HR, Security and Legal.	Proven detection and response capability.
Ongoing	Exchange of indicators with the sector and with the competent authorities. Review of the applicable regulations and of the official bibliography.	Shared intelligence and updating.

7.3. Response protocol when a suspicion arises

In the event of a well-founded suspicion, it is recommended to act in a coordinated and documented manner before saying anything to the employee: preserve records and evidence, restrict access without alerting the suspect where possible, assess with Legal Counsel the notification and data protection obligations, and inform the competent authorities. Once the case is closed, it is advisable to retain the technical and application indicators in order to detect repeat attempts. If the worker had access to personal data, it must be assessed whether a breach notification under the GDPR is required.

It is proposed to structure the response in five phases:

- **1. Initial assessment (hours).** Confirm with a second independent source that the suspicion is well founded, since a single indicator is not enough. Open a restricted-access case file, appoint an owner and limit knowledge of the case to those who need to know. Do not confront or question the person.
- **2. Discreet containment (hours to days).** Reduce privileges and prepare the simultaneous revocation of all access (email, VPN, repositories, SaaS tools, secrets managers). Activate reinforced telemetry on the account, block exfiltration routes and preserve the device and the logs with a chain of custody.
- **3. Investigation (days).** Reconstruct what was accessed and what was sent. Review the code and configuration contributed by the operative for backdoors, dependencies or improper keys. Identify the associated infrastructure (IP addresses, remote access devices, payment accounts, shipping addresses) and assess whether there was access to personal data or sensitive information.
- **4. Legal decision and communication (in parallel).** Assess with Legal Counsel and the DPO the appropriate employment route, the dismissal or suspension of payments, and the notification obligations: in the event of a personal data breach that poses a risk to individuals, the GDPR requires notifying the supervisory authority within a maximum of 72 hours of becoming aware of it. Inform the competent authorities (police forces and the relevant CERT) and assess with Compliance whether the sanctions authority should be notified. Prepare messages for management, clients and affected suppliers.

- **5. Closure and learning (weeks).** Revoke and rotate the credentials and secrets the operative could access, review again the code contributed, record the indicators and share them in the appropriate framework, and correct the control that should have detected the case earlier. Check whether other contractors from the same supplier or of similar origin show similar patterns.

8. Conclusions and recommendations

8.1. Conclusions

- The infiltration of North Korean IT workers is a persistent, adaptive threat recognized at government level, with a joint alert from eleven countries in July 2026.
- It combines identity fraud, insider risk, sanctions evasion and, in some cases, espionage and extortion.
- Generative AI has lowered the cost of fabricating credible identities and has weakened traditional indicators, including language.
- Judicial pressure in the United States has shifted activity toward Europe, where primary sources document cases in Germany, Portugal and the United Kingdom.
- There are no verified public incidents in Spain in the sources consulted, but the exposure factors are the same as in other European countries, and Spain does not take part in the alert mechanisms cited.
- **Analyst judgment (medium-low confidence): the most likely vector in Spain is the third party, not the direct employee.** The frictions of employment (NIF or NIE, Social Security registration, withholdings) do not exist or are outsourced in self-employed work, on freelance platforms and in subcontracting. Defense should start there.
- **Purely technical detection is insufficient.** The actor uses legitimate credentials and does real work. The useful signal emerges by correlating selection, access, payroll and suppliers, which today live in different systems and departments.
- **The cost of inaction is asymmetric.** Identity, device and payment controls are cheap and reusable against other risks (supplier impersonation, account-change fraud, conventional insider risk). An incident, by contrast, combines loss of intellectual property, extortion, sanctions exposure and reputational damage.
- **Persistence turns the response into a continuous intelligence process.** Dismissal does not close the case: extortion may follow, or a new attempt under another identity, which is why institutional memory (indicators, patterns, payment accounts) is part of the defense.

8.2. Prioritization criteria

The recommendations that follow do not carry equal weight. They have been prioritized using four criteria: risk reduction against the scenarios in Table 6, implementation effort and cost, dependence on third parties and legal proportionality. Table 10 assigns each scenario a qualitative rating and indicates which recommendations reduce it most. It is an analyst judgment, not a statistical estimate, and it rests on documented patterns and not on verified incidents in Spain.

Table 10. Prioritization of the scenarios in Table 6

Scenario	Likelihood	Impact	Priority	Key recommendations
A. Subcontracted developer	Medium	Medium-high	High	R3, R4, R5, R6
B. Position at a defense or infrastructure company (tier-2 supplier)	Low-medium	Very high	High, because of impact	R2 (level 3), R3, R4, R7

Scenario	Likelihood	Impact	Priority	Key recommendations
C. Extortion after dismissal	Medium (if an infiltration is detected)	High	High	R4, R7, R8
D. Re-infiltration	Medium-high (after a detection)	Medium	Medium	R6, R7, R9

8.3. Recommendations for management

Nine recommendations are proposed. Table 11 summarizes them with their priority, owner, timeframe and estimated effort; the text that follows explains what is being asked, why and how to check that it works. The timeframes are compatible with the horizons in Table 9.

Table 11. Summary of recommendations

Ref.	Recommendation	Priority	Owner	Timeframe	Effort
R1	Single owner and identity risk desk	Immediate	General management	0-30 days	Low
R2	Proportionate verification by position level	High	HR and Security	30-90 days	Medium
R3	Clauses and due diligence for suppliers and freelancers	High	Procurement and Legal	30-90 days	Medium
R4	Managed device, least privilege and gradual access	High	CISO and IT	30-180 days	Medium-high
R5	Payments only to a verified holder and control of bank detail changes	Immediate	Finance and Payroll	0-30 days	Low
R6	Detection by correlating signals	Medium	CISO and HR	90-180 days	Medium-high
R7	Response protocol, exercise and indicator register	High	CISO, Legal and DPO	30-90 days	Medium
R8	Compliance and documented diligence	Medium	Compliance and Legal	30-90 days	Low
R9	Training and reporting channel	Medium	HR and Security	30-90 days	Low

CISO: chief information security officer. DPO: data protection officer.

R1. Governance: a single owner and a joint desk. Appoint an owner of employment identity risk with a written mandate from general management and set up a desk with HR, Security, Procurement, Finance and Payroll, Legal and the DPO. The failure that explains the success of these schemes is more organizational than technical: each signal sits in a different system and nobody answers for the whole (section 4.1). The desk must have authority to stop or condition a critical hire, meet on a fixed schedule (monthly at the outset) and report quarterly to the management committee. *Success indicator:* mandate approved, first meeting held and inventory of critical positions delivered within 30 days.

R2. Identity verification proportionate to the risk of the position. Classify positions, internal and external, into three levels according to the access they grant (Table 12) and require increasing verification. Two design principles. First, verification is applied by position and not by person: all candidates for the same position go through the same steps, which reduces the risk of discrimination and bias. Second, it is reinforced on the basis of behavior when objective indicators coincide (section 6). For level 3, in-person verification, direct or through a trusted third party with a local presence, is the control that reduces risk the most, because AI can imitate an image but cannot replace a physical person in front of an interlocutor. *Indicator:* 100% of level 2 and 3 hires with verification completed before first access.

Table 12. Proposed verification levels

Level	Positions and access	Minimum verification	Access and supervision
1. Standard	Positions with no access to code, to personal data on a large scale or to critical systems.	Document verification; cross-checking of track record and references through an independent channel; video call with human checking of the document.	Basic access profile; corporate device recommended; ordinary supervision.
2. Sensitive	Development, systems administration, access to repositories, to production or to client data, including staff of suppliers and freelancers.	The above plus a second interview with unpredictable questions and live technical exercises; verifiable track record and code; payment account in the name of the contractor.	Managed device with no BYOD; least privilege; access expanded gradually; reinforced monitoring during the first 90 days.
3. Critical	Access to key intellectual property, to defense or critical infrastructure information, to production keys and secrets or to funds.	The above plus in-person verification (direct or through a trusted third party) and, where an applicable procedure exists, personnel security vetting or clearance.	Temporary privileged access with dual control; strict segmentation; peer code review; continuous monitoring and periodic review of the need for access.

The levels are a reference proposal. Each organization should adapt them to its inventory of positions and validate them with the DPO and, where appropriate, with employee representatives.

R3. Treat suppliers and freelancers as an extension of the workforce. Third parties are the route this report considers most likely in Spain (section 5.3) and the least controlled. It is advisable to require by contract: a named list of the staff assigned, with identity verification carried out by the supplier and evidence available on request; a ban on subcontracting or replacing individuals without prior authorization; a declaration of the location from which work is done; exclusive use of managed devices or of virtualized environments controlled by the client; timely incident notification; and a right of verification. In addition, apply reasonable due diligence to the supplier company itself (age, address, beneficial ownership, references), because the networks use shell companies (section 2.3). *Indicator:* proportion of suppliers with sensitive access that have signed the clauses (indicative target: more than 90% within 180 days).

R4. Control the device and minimize what each identity can do. Start from the premise that a verified identity can nevertheless be malicious or compromised. For levels 2 and 3: managed corporate devices, no BYOD, shipped to a verified address and with a check that the device is where it should be; access conditional on device status, location and expected working hours; least privilege with gradual expansion during an initial period; temporary privileged access with dual control; and segmentation of code repositories, secrets and client data. The benefit is twofold: it limits the damage from this risk and from any other insider risk. *Indicator:* percentage of sensitive access from managed, compliant devices, and average time to revoke access upon termination.

R5. Close the money route. Payment is the purpose of the scheme and a control point that the operative cannot avoid. Pay only to accounts whose holder matches the contracted person or entity; prohibit payments to third parties and in crypto-assets unless an exception is approved by Compliance; verify through an independent channel any change to payment details, with a waiting period before the first payment to the new destination; and set up an alert flow from Payroll and Treasury to the risk desk. It is among the cheapest measures and has one of the best impact-to-cost ratios, and it also reduces bank account change fraud. *Indicator:* 100% of payments to a verified holder, with exceptions documented.

R6. Detection: from isolated signals to correlation. Integrate, even if manually at first, the signals from selection, access, payroll and suppliers (section 4.1) using the combination rules in section 6. On the technical side: endpoint and remote access telemetry on newly onboarded profiles; alerts for remote control tools or hardware remote access devices, for inconsistencies between location or time zone and what was declared, and for unusual volumes of cloning or downloading; and decoys (bait credentials or documents) in repositories and shared resources of critical environments. Effort is best concentrated on the first 90 days of each onboarding, when access is still limited and the anomaly is most visible. *Indicator:* rules active and reviewed, and time from alert to decision.

R7. Prepared response and institutional memory. Approve the protocol in section 7.3, designate a response team with Legal and the DPO, and test it with an annual simulation exercise. Two decisions are best made in advance: who authorizes containment without alerting the suspect, and how evidence is preserved while respecting employment and data protection safeguards. Keep a register of indicators (infrastructure, application patterns,

payment accounts, addresses) to detect repeat attempts, with a legal basis, defined retention periods and minimization of personal data. *Indicator:* exercise carried out, corrective actions closed and recurrences detected.

R8. Compliance and documented diligence. Incorporate the risk into the sanctions compliance assessment, into NIS2 readiness plans and into the risk analysis of the security management system (for example, ISO/IEC 27001 or the National Security Scheme, where they apply). Screening names against sanctions lists is necessary but insufficient, because the identities these operatives use are false or stolen and do not appear on them. It is therefore advisable to document the verification process (what was checked, when and by whom) as evidence of reasonable diligence, and to ask Legal for an opinion on the applicable standard of liability and on the criteria for reporting to the competent authorities. *Indicator:* risk included in the corporate register with an owner, controls and periodic review.

R9. People: brief training and a reporting channel. Train interviewers, team leaders and HR and payments staff in the patterns in section 6, with examples and with an explicit message about false positives and non-discrimination. Provide a way to raise doubts, which may rely on the internal information channel under Law 2/2023 where the organization is required to have one, and protect those who report in good faith. The teams who work daily with the operative may be the first to notice inconsistencies in working hours, knowledge or behavior. *Indicator:* percentage of the target group trained and queries received.

Cost and sequencing. The measures with the highest relative return (R1, R5, R3 and R4) have low or medium cost and are reusable against other risks. The costlier ones, such as detection by correlation (R6) and in-person verification, should be limited to levels 2 and 3. Requiring in-person verification for all positions would be disproportionate and legally questionable. If a choice has to be made, the recommended order is: governance and payments (first weeks), third parties and verification (first quarter), device and response (first half-year) and advanced detection (afterwards).

8.4. What each function does: operational checklist

The recommendations above translate into concrete practices by function. None is conclusive on its own; their value lies in the combination and in someone carrying them out and reviewing them.

Human Resources and selection

- Give interviewers a script with unpredictable, verifiable questions, and require the camera to be on in all phases for level 2 and 3 positions. Include simple interaction tests (changing position, moving a hand in front of the face, sharing the screen while solving a technical problem) and assess the consistency between image, voice and knowledge.
- Cross-check the track record against independent sources: call references at independently obtained numbers, check the age and contact network of professional and code profiles, and detect the reuse of photos, emails, phone numbers or texts across applications.
- Ensure that the person interviewed is the person who joins: repeat a brief identity check on the first day and before handing over credentials and equipment.
- Record inconsistencies using objective criteria and retention periods agreed with the DPO.

Information security and IT

- Detect remote desktop tools and hardware remote access, as well as access from locations or networks incompatible with what was declared.
- Compare activity hours with the declared time zone and investigate abnormally long or continuous working days.
- Alert on mass cloning of repositories, downloads of documentation unrelated to the role, synchronization with personal services and email forwarding rules.
- Revoke access centrally and rotate secrets and keys upon termination; retain telemetry for as long as needed to investigate.
- Maintain a catalog of indicators (IP addresses, domains, devices, payment accounts, application patterns) and check new hires against it.

Procurement and supplier management

- Require a named list of the staff assigned and verification of their identity, and do not accept substitutions without authorization.

- Apply due diligence to the supplier company: age, verifiable address, beneficial ownership, references and consistency between its rates and market rates. Offers far below market price are a warning sign.
- Prioritize suppliers with a verifiable track record when level 2 or 3 access is granted, and periodically review those already working in the organization.
- In public procurement, incorporate these requirements as tender specifications or special performance conditions, within the limits of public sector contracting law.

Finance and payroll

- Reject payments to third parties and bank detail changes requested by email or messaging; verify them by calling a previously known number.
- Hold the first payment to a new account until verification is complete and watch for accounts that receive payments for several identities.
- Escalate to the risk desk any requests to be paid in crypto-assets or through payment intermediaries.
- Bear in mind that sanctions list screening serves to detect payments to designated entities, but does not detect a false identity.

Legal, DPO and Compliance

- Define the legal basis and the information given to candidates and employees for each verification; carry out an impact assessment when the processing is high-risk, in particular if biometric data or automated tools are used, and prefer non-biometric alternatives (human checking of the document) where they are sufficient.
- Check against Organic Law 3/2018 (arts. 87 and 90, on digital devices and geolocation in the workplace) any technical controls that affect workers, and inform or consult their representatives where appropriate.
- Check whether any automated selection tools to be procured fall within Regulation (EU) 2024/1689 on artificial intelligence, which may classify certain personnel selection systems as high-risk, and require the supplier to provide the corresponding documentation.
- Prepare in advance the criteria for notifying authorities and communicating with clients after an incident.

8.5. Adaptation by type of organization

The same framework does not weigh the same everywhere. Table 13 indicates what to prioritize by profile, with the main caution in each case.

Table 13. Priorities by organization profile

Profile	Main risk	Priorities	Caution
Startup or tech SME with a remote team	Fast hiring, freelancers and BYOD.	Managed device for anyone touching code or production; video call with human checking of the document and payment to a verified holder; MFA and least privilege in repositories.	Do not slow down hiring; apply light, proportionate controls.
Consultancy or development agency that subcontracts	Acting as an entry vector to clients or becoming a victim of its own subcontractors.	Documented verification of all staff assigned to clients; control of subcontracting; auditable evidence for clients.	Contractual liability to the client if verification fails.
Defense, aerospace, critical infrastructure and tier-2 suppliers	Espionage and access to technical documentation.	Level 3 by default for roles with access to sensitive information; in-person verification; passing the requirements down the supply chain; a channel with the relevant CERT (for example, ESPDEF-CERT in defense).	Coordinate with existing information security procedures; do not improvise parallel controls.
Fintech, exchanges and blockchain	Asset theft and the sector of greatest documented interest.	Segregation of duties and dual control over keys and treasury; independent review of critical code; strict control of payments and destination accounts.	Make compatible with sector regulation and anti-money-laundering rules.

Profile	Main risk	Priorities	Caution
Public administrations and the public sector	Access to citizens' data and dependence on IT contractors.	Require in tender specifications the verification of the contractor's staff; apply the National Security Scheme; channel with the CCN-CERT.	Public procurement rules limit which criteria can be required and how.

8.6. What to avoid

Some mistakes are common and costly. It is advisable to prevent them expressly in policy and in training.

- **Filtering by nationality, language or surname.** It is ineffective, because the operatives claim third-country nationalities, and discriminatory (section 5.4).
- **Rejecting a candidate on the basis of a single indicator.** It should trigger additional verification, not automatic rejection (section 6).
- **Confronting the suspect or dismissing them immediately.** The opportunity to preserve evidence is lost and the risk of data deletion or extortion increases.
- **Relying on a single tool.** Neither a deepfake detector nor automated document verification is sufficient on its own as a control.
- **Banning remote work or international hiring.** This is disproportionate. The risk is managed by level of access, not by working arrangement.
- **Treating the case as closed after dismissal.** Pending items remain: review of the code contributed, rotation of secrets, follow-up of the extortion and watching for repeat attempts.
- **Collecting more data than necessary.** Mass biometrics or generalized surveillance, without an impact assessment, create a legal risk of their own.
- **Forgetting suppliers.** Controls on the workforce are of no use if access arrives through a third party.

8.7. Recommendations for the sector and the authorities

Part of the risk cannot be solved organization by organization. Six lines of collective action are proposed.

- **Share indicators, not personal data.** Use or create a sector channel, for example through the relevant CERTs (INCIBE-CERT for the private sector, CCN-CERT for the public sector and ESPDEF-CERT for defense), to share technical indicators and application patterns from confirmed cases, with data protection safeguards and with a trust protocol (TLP).
- **A message from the authorities in Spanish.** Encourage the competent authorities to disseminate and adapt to the Spanish context the July 2026 joint alert and to consider their relationship with the international monitoring mechanisms (section 3.5).
- **Common guides and templates.** Business associations, clusters and professional bodies can publish proportionate verification guides and model supplier clauses, so that SMEs do not have to design them from scratch.
- **Demands on platforms.** Call on freelance hiring platforms for robust identity verification, detection of accounts with reused documents and a swift reporting channel, in line with what the joint alert asks for.
- **Clear legal criteria.** Ask the Spanish Data Protection Agency and the labor authorities for guidance on remote identity verification in recruitment, to give legal certainty to reasonable controls.
- **Joint exercises.** Organize sector exercises (defense, energy, technology) involving HR and Legal, not just the technical teams.

8.8. How to measure progress

A recommendation without an indicator cannot be governed. Table 14 proposes a small set of indicators for the risk desk. The targets are indicative and should be adjusted to the reality of each organization.

Table 14. Monitoring indicators

Indicator	What it measures	Indicative target	Frequency
Coverage of the inventory of remote and subcontracted positions	Percentage of positions with sensitive access classified by level.	100% within 30 days	Quarterly
Verification before access	Level 2 and 3 hires with verification completed before first access.	100%	Monthly
Payments to a verified holder	Payments to accounts whose holder matches the contractor.	100%, with exceptions documented	Monthly
Aligned suppliers	Suppliers with sensitive access that have signed verification clauses.	More than 90% within 180 days	Quarterly
Compliant devices	Level 2 and 3 access from managed, compliant devices.	100%	Monthly
Containment time	Hours between confirmation of a well-founded suspicion and restriction of access.	Less than 24 hours	Per case
Quality of reinforced verifications	Verifications triggered and the proportion that turn out to be false positives.	Monitoring and calibration, no fixed target	Quarterly
Simulation exercise	Annual exercise with HR, Security and Legal and closure of corrective actions.	1 per year	Annual

8.9. Residual risk, assumptions and review signals

Once the recommendations are applied, the risk does not disappear. An actor with a solid local facilitator and a high-quality stolen identity can get past remote controls. The realistic goal is to raise the cost of entry, shorten detection time and limit the damage a malicious identity can cause through least privilege and control of the device and the payment.

Assumptions of this analysis

- The operating model observed in Germany, Portugal and the United Kingdom is transferable to Spain (medium confidence).
- There are no verified public cases in Spain; if they appear, the likelihood of scenarios A and B should be revised upward.
- The legal framework described is the one in force as of October 2026. According to the secondary sources consulted, the transposition of NIS2 into Spanish law was still in progress; its status should be checked in the BOE before basing decisions on it.

Signals that would justify revisiting this judgment

- A first confirmed case in Spain or in a neighboring country with a similar business structure.
- New reports from the MSMT, GTIG or European authorities, or a specific alert from Spanish authorities.
- Evidence that real-time video techniques are defeating live interview controls.
- Changes in the verification practices of hiring platforms, or criteria from the data protection authority on remote identity verification.

8.10. Future lines of research

Several questions remain open and deserve follow-up: the existence of confirmed cases in Spain, the role of European *freelance* platforms, the evolution of real-time video manipulation techniques and the effect of the 2026 alert on the behavior of the networks. To these are added the real effectiveness of the proposed controls after the first year of application, the role of Spanish development outsourcing providers and the legal framework for the exchange of indicators between organizations. It is recommended to update this report when new reports from the MSMT, GTIG or European authorities are published.

Bibliography

A. Primary and institutional sources

- [1] U.S. Department of State, FBI and authorities from ten other countries (31 July 2026). *Alert to Countries, Companies, and Other Entities Regarding North Korean IT Workers*. <https://www.ic3.gov/CSA/2026/260731.pdf> (State Department version: <https://www.state.gov/releases/office-of-the-spokesperson/2026/07/alert-to-countries-companies-and-other-entities-regarding-north-korean-it-workers>)
- [2] Google Threat Intelligence Group (1 April 2025). *DPRK IT Workers Expanding in Scope and Scale*. Google Cloud Blog. <https://cloud.google.com/blog/topics/threat-intelligence/dprk-it-workers-expanding-scope-scale>
- [3] Multilateral Sanctions Monitoring Team (22 October 2025). *Joint Statement on the Report Covering DPRK Cyber and IT Worker Activities*. U.S. Department of State. <https://www.state.gov/releases/office-of-the-spokesperson/2025/10/joint-statement-of-the-multilateral-sanctions-monitoring-team-msmt-on-the-report-covering-dprk-cyber-and-it-worker-activities> ; Japan's Ministry of Foreign Affairs: <https://www.mofa.go.jp/press/release/presssite00000101758.html>
- [4] Japan's Ministry of Foreign Affairs (16 September 2026). *Release of the Third Report of the Multilateral Sanctions Monitoring Team (MSMT)*. <https://www.mofa.go.jp/press/release/presssite00000102663.html>
- [5] CrowdStrike (4 August 2025). *CrowdStrike 2025 Threat Hunting Report: AI Becomes a Weapon and a Target*. <https://www.crowdstrike.com/en-us/blog/crowdstrike-2025-threat-hunting-report-ai-weapon-target/>
- [6] CrowdStrike (2024). *2024 CrowdStrike Threat Hunting Report: Nation-States Exploit Legitimate Credentials to Pose as Insiders*. <https://ir.crowdstrike.com/news-releases/news-release-details/2024-crowdstrike-threat-hunting-report-nation-states-exploit>
- [7] U.S. Department of Justice, U.S. Attorney's Office for the District of Columbia. *Ukrainian National Sentenced in 'Laptop Farm' Scheme That Generated Income for North Korean IT Workers*. <https://www.justice.gov/usao-dc/pr/ukrainian-national-sentenced-laptop-farm-scheme-generated-income-north-korean-it-workers>
- [8] U.S. Department of Justice (May 2026). *U.S. Nationals Sentenced for Facilitating Fraudulent Remote Information Technology Worker Schemes to Generate Revenue for the Democratic People's Republic of Korea*. <https://www.justice.gov/opa/pr/two-us-nationals-sentenced-facilitating-fraudulent-remote-information-technology-worker-0>
- [9] U.S. Department of Justice. *Fourteen North Korean Nationals Indicted for Carrying Out Multi-Year Fraudulent Information Technology Worker Scheme*. <https://www.justice.gov/archives/opa/pr/fourteen-north-korean-nationals-indicted-carrying-out-multi-year-fraudulent-information>
- [10] U.S. Department of State (January 2026). *Multilateral Sanctions Monitoring Team (MSMT) Update* (Foreign Press Center). <https://www.state.gov/briefings-foreign-press-centers/multilateral-sanctions-monitoring-team-update-2>
- [11] Council of the European Union (2017). Regulation (EU) 2017/1509 of 30 August 2017 concerning restrictive measures against the Democratic People's Republic of Korea. OJ L 224, 31.8.2017. <https://eur-lex.europa.eu/eli/reg/2017/1509/oj/eng>
- [12] Council of the European Union. *EU sanctions against North Korea*. <https://www.consilium.europa.eu/en/policies/sanctions-against-north-korea/>
- [13] European Parliament and Council (2016). Regulation (EU) 2016/679 (GDPR). <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- [14] European Parliament and Council (2022). Directive (EU) 2022/2555 (NIS2). <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>
- [15] Spain. Organic Law 3/2018 on the Protection of Personal Data and the guarantee of digital rights; Royal Legislative Decree 2/2015 (Workers' Statute); Law 15/2022 on equal treatment and non-discrimination. Official State Gazette (BOE): <https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673> ; <https://www.boe.es/buscar/act.php?id=BOE-A-2015-11430> ; <https://www.boe.es/buscar/act.php?id=BOE-A-2022-11589>

B. Complementary sources

- [16] Holland & Knight (26 August 2026). *Hidden in Plain Sight: Labor, Employment and Cybersecurity Risks of DPRK IT Worker Infiltration*. <https://www.hklaw.com/en/insights/publications/2026/08/hidden-in-plain-sight-labor-employment-and-cybersecurity-risks>
- [17] CNN (15 April 2026). *Two Americans sentenced to prison for North Korean tech worker scheme*. <https://www.cnn.com/2026/04/15/politics/americans-sentenced-prison-north-korean-tech-worker-scheme>
- [18] CyberScoop (May 2026). *American duo sentenced for hosting laptop farms for North Korean IT workers*. <https://cyberscoop.com/north-korea-it-worker-scheme-laptop-farm-facilitators-sentenced/>
- [19] Fortune (25 April 2026). *North Korean IT workers are stealing remote jobs and raking in billions—and Americans are helping them do it*. <https://fortune.com/2026/04/25/north-korean-it-worker-scheme-american-facilitators/>
- [20] Fortune (1 September 2026). *Half of remote IT job applications now carry North Korean fraud patterns, startup Endorsed finds* (data from a commercial vendor). <https://fortune.com/2026/09/01/north-korean-it-worker-remote-job-applications/>

- [21] 38 North (December 2025). *Assessing the MSMT's DPRK IT Worker Threat Report*. <https://www.38north.org/2025/12/assessing-the-msmts-dprk-it-worker-threat-report/>
- [22] Chainalysis (2025). *Five Key Takeaways from MSMT's Report on North Korean Cyber Operations* (includes an update on OFAC designations, 4 November 2025). <https://www.chainalysis.com/blog/msmt-report-north-korea-dprk-cyber-threats/>
- [23] The Korea Times (22 October 2025). *Sanctions watchdog links N. Korean hackers to \$1.65 bil. in crypto theft this year alone*. <https://www.koreatimes.co.kr/foreignaffairs/northkorea/20251022/sanctions-watchdog-links-n-korean-hackers-to-165-bil-in-crypto-theft-this-year-alone>
- [24] The Korea Herald (October 2025). *N. Korea has stolen \$2.84b in crypto since 2024 as China aids cash-out: report*. <https://v.daum.net/v/znkQffXSI3?f=p>
- [25] Help Net Security (19 March 2026). *Elite members of North Korean society fake their way into Western paychecks* (research by IBM X-Force and Flare). <https://www.helpnetsecurity.com/2026/03/19/north-korean-remote-it-workers-corporate-infiltration-scheme/>
- [26] Center for Strategic and International Studies (2026). *Responding to the Evolution and Global Expansion of the DPRK IT Worker Threat*. <https://www.csis.org/analysis/responding-evolution-and-global-expansion-dprk-it-worker-threat>
- [27] TechCrunch (11 August 2026). *North Korean remote IT staffer worked for US government agency, says FBI*. [Link pending verification]
- [28] El País (1 November 2023). *Corea del Norte cierra su Embajada en España* (in Spanish). <https://elpais.com/internacional/2023-11-01/corea-del-norte-comunica-que-cierra-su-embajada-en-espana.html>
- [29] El Español (2 April 2025). *Google advierte a Europa: un ejército de hackers norcoreanos se infiltra como trabajadores remotos para atacar a empresas* (in Spanish). https://www.lespanol.com/omicrono/software/20250402/google-advier-te-europa-ejercito-hackers-norcoreanos-infiltra-trabajadores-remotos-atacar-empresas/935906578_0.html
- [30] Baker McKenzie (2026). *Multiple Governments Issue Joint Alert on North Korean IT Workers*. Global Sanctions and Export Controls Blog. <https://sanctionsnews.bakermckenzie.com/multiple-governments-issue-joint-alert-on-north-korean-it-workers/>

Annex. Glossary

Term	Definition
DPRK	Democratic People's Republic of Korea (North Korea).
North Korean IT worker	North Korean IT professional who obtains remote employment under a false or stolen identity to generate income for the regime.
Laptop farm	Address where a facilitator receives corporate computers and allows operatives to access them remotely in order to hide their location.
Facilitator	Person or company that provides services to the operatives: identities, accounts, hosting of devices, laundering of payments.
BYOD	<i>Bring your own device</i> : policy that allows access to corporate systems from personal devices.
FAMOUS CHOLLIMA	CrowdStrike's name for the DPRK-linked group that carries out these infiltrations.
MSMT	Multilateral Sanctions Monitoring Team: an eleven-country mechanism created in October 2024 to monitor UN sanctions on North Korea.
GTIG	Google Threat Intelligence Group.
TLP:CLEAR	Information classification protocol that allows unrestricted disclosure.
CISO	Chief information security officer of an organization.
DPO	Data protection officer, a role provided for in the GDPR.
Least privilege	Principle whereby each identity receives only the access necessary for its function and only for as long as necessary.
Decoy (honeypot)	A fake credential, document or record placed so that its use or access triggers an alert.
Identity risk desk	Joint committee of HR, Security, Procurement, Finance, Legal and the DPO that governs employment identity risk.