Computrabajo

Information Security and Data Protection

Computrabajo

We are world leaders in digital HR solutions

Our mission is clear: to help people find better jobs and companies find the best talent. That is why we created **Computrabajo**, the leading job site in Latin America, with 128+ million monthly visits and 27+ million company ratings.

These figures reflect the trust our users place in us. We honour and preserve that trust every day with our information security and data protection measures.

Table of Contents

Information Security

ISO 27001 Certification 4
Cloud Computing 5
Operations Security 6
Secure Development 7
Availability and Continuity 8
Vulnerabilities Management 9
Services Security 10

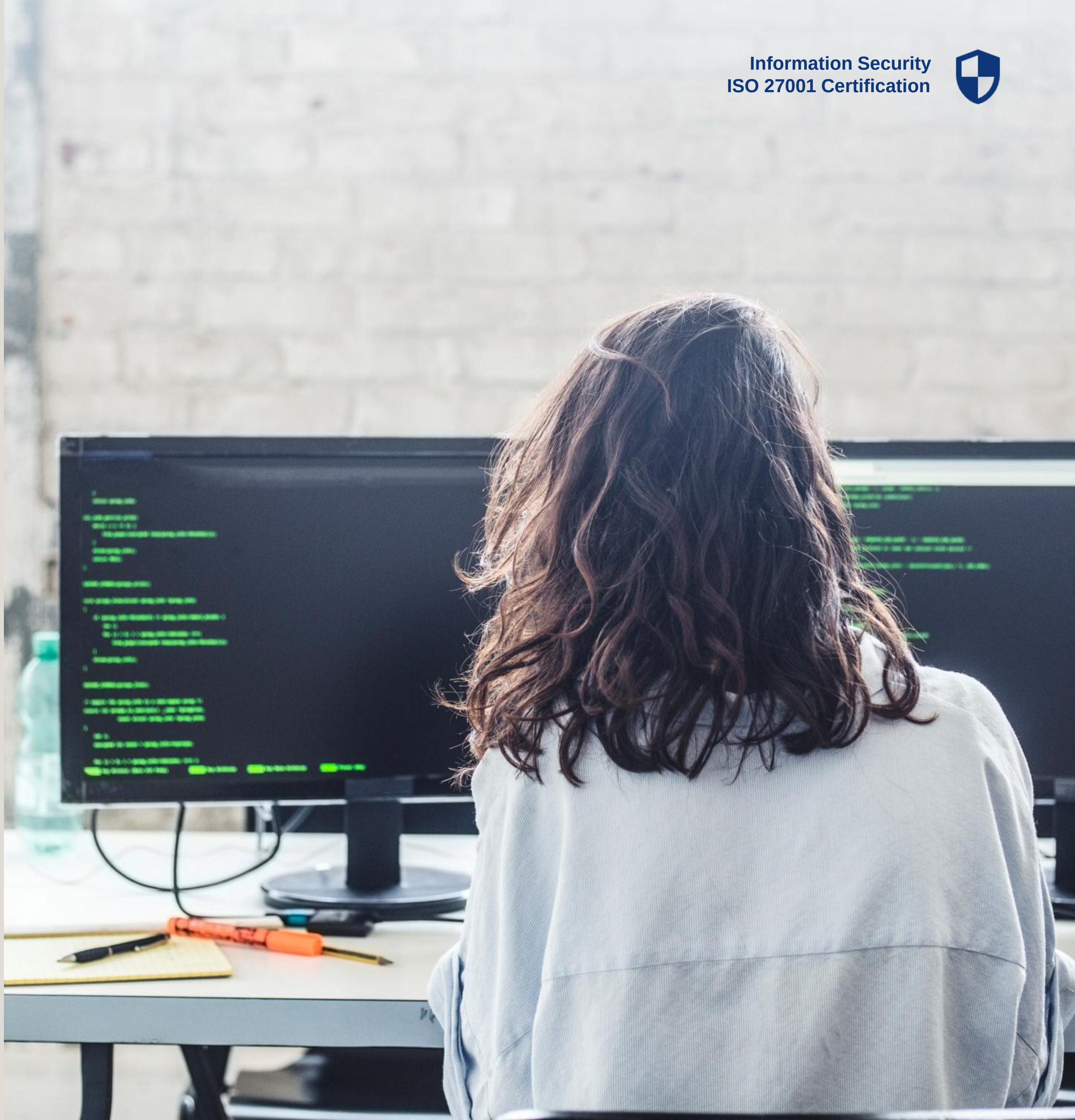
Data Protection

Pledge 12
Principles 13
Controller 14
Privacy by Design and by Default 15
Processing 16
Purposes 17
Rights 19
Retention 20
Transfers 21
Processors 22
Security 23
Breaches 24

We are committed to information security in our services

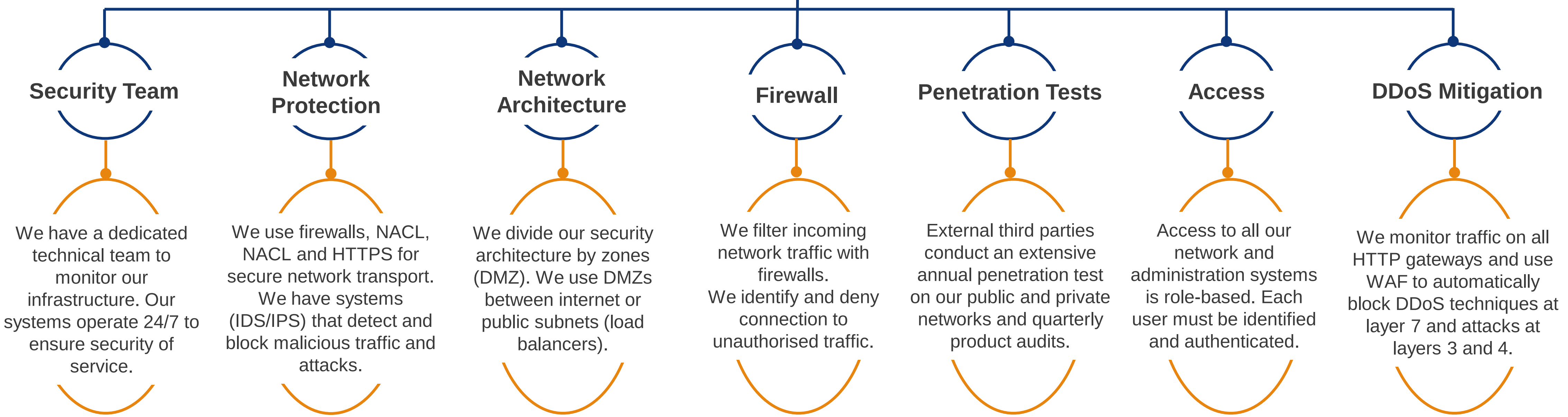
We have an Information Security Management System (ISMS) certified under the **ISO/IEC 27001:2022** standard for the services that we offer. This includes **Computrabajo**.

Our processes and systems are subject to regular audits, penetration testing, intrusion detection and prevention. We monitor and improve our technology, infrastructure and processes to ensure maximum quality, efficiency and security.



Cloud Computing

AWS and **Azure** are **our cloud computing providers.**
We draw on the expertise, resources and reputation of Amazon and Microsoft to ensure secure, robust and reliable cloud operations.



Security Team

We have a dedicated technical team to monitor our infrastructure. Our systems operate 24/7 to ensure security of service.

Network Protection

We use firewalls, NACL, NACL and HTTPS for secure network transport. We have systems (IDS/IPS) that detect and block malicious traffic and attacks.

Network Architecture

We divide our security architecture by zones (DMZ). We use DMZs between internet or public subnets (load balancers).

Firewall

We filter incoming network traffic with firewalls.
We identify and deny connection to unauthorised traffic.

Penetration Tests

External third parties conduct an extensive annual penetration test on our public and private networks and quarterly product audits.

Access

Access to all our network and administration systems is role-based. Each user must be identified and authenticated.

DDoS Mitigation

We monitor traffic on all HTTP gateways and use WAF to automatically block DDoS techniques at layer 7 and attacks at layers 3 and 4.

Operations Security

Change Management

We manage all system changes through a change management procedure. We monitor changes, analyse their risks and approve their impacts.

Updates

With Azure DevOps, we automate updates through pipelines. We test to deploy new versions and do automatic rollbacks if there are service failures.

Resources Management

We monitor current and future demand for technology resources to optimise performance, plan capacity and manage demand for services.

Malware Control

We implement anti-malware solutions that we continuously update. We constantly monitor our assets to protect them from cyber threats.

Response to Security Incidents

Upon alerts, our 24/7 operations, network and security teams escalate incidents. We inform our customers of any security impact within 48hrs maximum.

Logging and Monitoring

We collect extensive event logs. Our system alerts the security team to correlated events for investigation and response.

Encryption in transit

We encrypt all our communications with the Transport Layer Security (TLS) protocol over public networks with new, non-weak cipher suites.

Encryption at rest

We encrypt all files and data stores with key management systems based on robust algorithms and industry-standard rotation schedules.

Secure Development

As part of our Secure Development Life Cycle (SDLC), we have several tools that we use at every stage of software development to ensure the security of our services from conception to implementation and maintenance.

Language

Our software stack is based on various programming languages for our websites and APIs. Azure DevOps supports programming languages with high scalability, reliability and security.

Security Training

We train our developers internally on code security, design, following best practices to combat common attacks and using security controls.

Quality Assurance

Our QA team reviews and tests our code, integrating various manual and automated tests so that only code that has been evaluated and approved is implemented.

Audit Logs

We keep records of all accesses and changes made by each user (audit logs). Logs are stored under restricted access and can only be consulted in the event of an incident.

OWASP Security Checks

We align our software development with OWASP industry practices. These include controls that reduce our exposure to Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF) and SQL Injection (SQLi), among others.

Isolated Environments

We physically and logically separate test, staging and development environments. We do this separation through network isolation, firewalls and NACL. We do not use real production data in the development or test environments.

Availability and Continuity

Redundancy

Our production services infrastructure has redundancy to avoid single points of failure. If a primary system fails, redundant hardware relieves it. We use service bundling and network redundancy to reduce single points of failure.

Backup

AWS/Azure provide our backup infrastructure that resides in long-term data stores behind logically secured and encrypted private networks at rest. We back up data from production environments daily and weekly, through a random check, we verify the integrity of the backup.

Disaster Recovery

Our plan ensures availability and disaster recovery of services, through a robust technical environment and recovery plans with vendor redundancy, according to the RTOs and RPOs we define.

Vulnerabilities Management

We have a number of tools that allow us to detect technical vulnerabilities

Internal Dynamic Vulnerability Scanning

We employ qualified third-party security tools to continuously and dynamically scan our applications against OWASP rules, among others. All HTTP controllers have an active WAF that blocks all known OWASP and major known rules in real time.

External Dynamic Vulnerability Scanning

We use industry-standard, customised scanning technologies to efficiently test infrastructure and software while minimising the potential risks associated with active scanning. We perform testing and on-demand scans as needed. Scans are performed during non-peak windows.

Static Code Analysis

Our source code repositories are continuously scanned at test and review stages in CI/CD Pipelines and Flow (continuous integration) and are integrated with all QA flows.

Security Penetration Testing

We rely on external third-party security experts to perform detailed penetration testing and dynamic code analysis.

Security Features in Our Services

These features allow us to preserve the security of the information that circulates or is stored through the use of our services.

Feature	Description
Options for authentication	For Web GUI applications, we offer account login with 2FA. For product APIs and/or customer integrations, we offer an authentication flow with API keys and/or secret/tokens to authenticate and authorise all API calls and actions with the backend. Users accessing the tool are uniquely and uniquely identified through the mandatory authentication system, consisting of a unique user and a password. The system automatically generates an initial key or password that must be changed on 2-factor authentication (2FA) is required for all users. 2FA authentication provides another layer of security to your account, making it difficult for someone else to log in as you. For security reasons, the key or password will be required to contain a specific format to avoid weak keys.
Two-factor authentication (2FA)	2-factor authentication (2FA) is required for all users. 2FA authentication provides another layer of security to your account, making it difficult for someone else to log in as you.
Password policy	Passwords can only be reset by the end user with an email address. The end user can generate a temporary password reset URL on the login page. Password policies follow the main recommendations to ensure your security.
Secure credential storage	We follow best practices for secure storage of credentials. All passwords are stored encrypted, i.e. they are never stored in human-readable form. A secure one-way hash is used, with encryption at rest and of all operations in transit to the backend.

Security Features in Our Services (cont.)

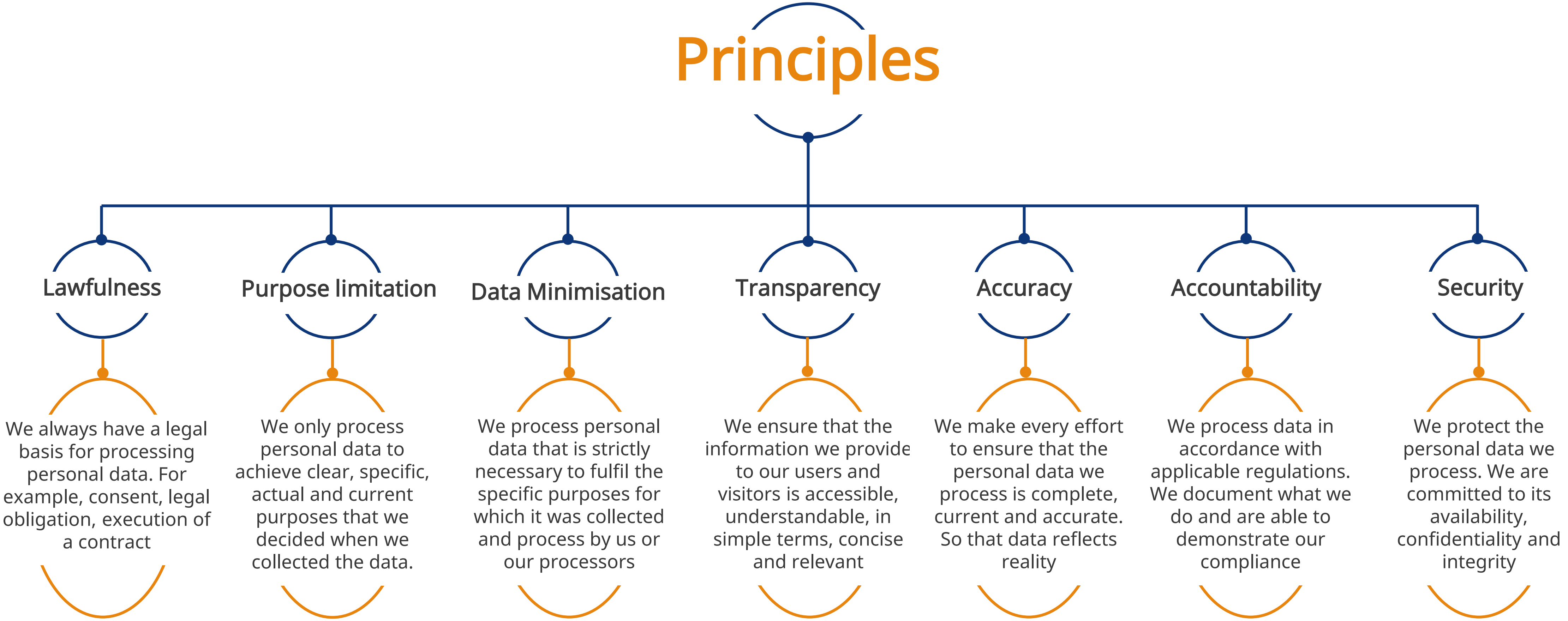
These features allow us to preserve the security of the information that circulates or is stored through the use of our services.

Feature	Description
Access privileges and roles	Access to data is governed by access rights and can be configured to define granular access privileges. Applications have various levels of permissions for users (owner, administrator, agent, end-user, etc.) and a granularity of roles per group.
High availability and accessibility of the product	To ensure low latency and high availability in content delivery, a content delivery network (CDN) is used, which ensures low latency and high availability.
Customer data	Each customer's data and documentation is stored in encrypted form in its own independent logical space.
Private attachments	By default, all instances of our applications are protected, all assets and attachments are private and require a login and permission/role. In addition, all assets and attachments are stored in an encrypted data store.

Protecting our users' personal data is our priority

At **Computrabajo**, we are committed to protecting the personal data of our users. From the beginning, we have focused on developing solutions that protect personal data.

This means that we develop tools, implement measures and provide information so that our users can make informed decisions and always have control over their personal data.



Principles

Lawfulness

We always have a legal basis for processing personal data. For example, consent, legal obligation, execution of a contract

Purpose limitation

We only process personal data to achieve clear, specific, actual and current purposes that we decided when we collected the data.

Data Minimisation

We process personal data that is strictly necessary to fulfil the specific purposes for which it was collected and process by us or our processors

Transparency

We ensure that the information we provide to our users and visitors is accessible, understandable, in simple terms, concise and relevant

Accuracy

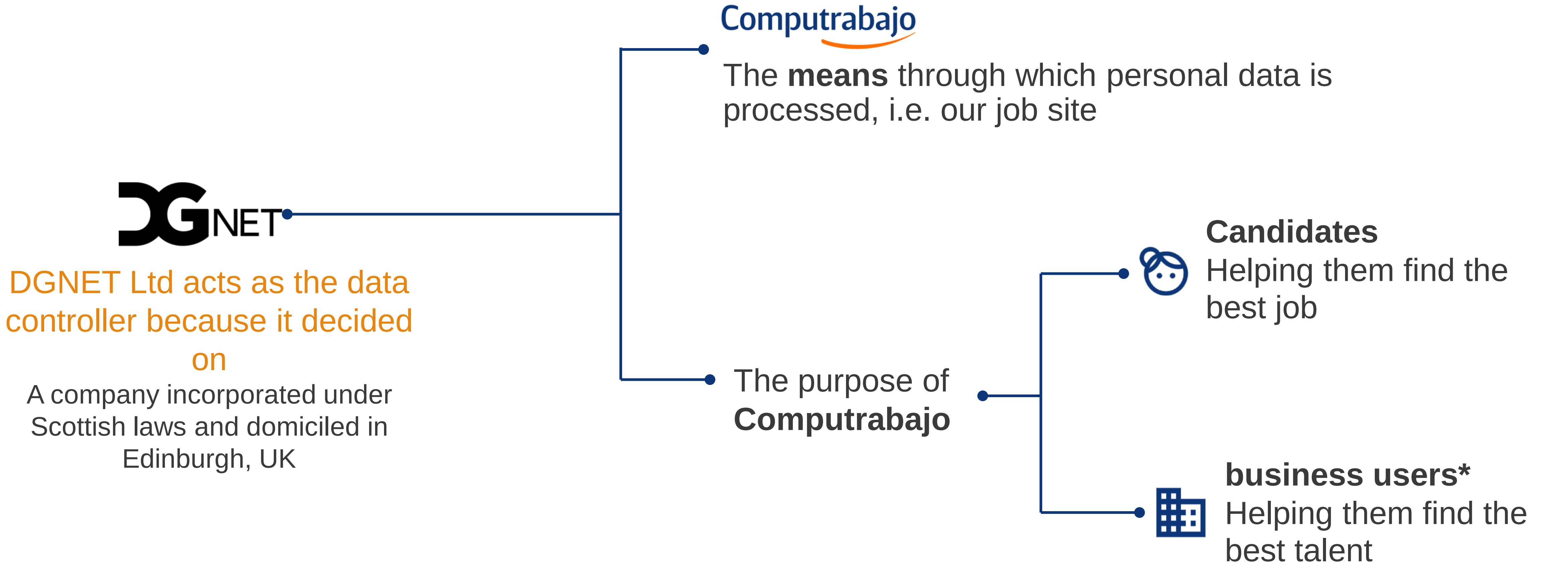
We make every effort to ensure that the personal data we process is complete, current and accurate. So that data reflects reality

Accountability

We process data in accordance with applicable regulations. We document what we do and are able to demonstrate our compliance

Security

We protect the personal data we process. We are committed to its availability, confidentiality and integrity



DGNET Ltd acts as the data controller because it decided on

A company incorporated under Scottish laws and domiciled in Edinburgh, UK

Computrabajo

The **means** through which personal data is processed, i.e. our job site

The purpose of **Computrabajo**

Candidates
Helping them find the best job

business users*
Helping them find the best talent

* Also called ‘companies’. For data protection purposes only, when we refer to business users, we mean the individual who creates and manages the Computrabajo account in the name and on behalf of a company.

Computrabajo is *privacy-friendly*

We have designed and developed **Computrabajo** so that our users are always in control of their personal data and know what we are doing with it. We do not tolerate invasive, misleading, confusing, deceiving practices that affect our users' privacy.

Privacy by Design

At each stage of development, we have taken decisions to:

- Guarantee the confidentiality, integrity, availability and permanent resilience of systems and services
- Restore availability and access in case of security incidents
- Verify, evaluate and continuously assess the effectiveness of our technical and organisational measures

Privacy by Default

Computrabajo's original account setup is privacy friendly:

- Our users decide how and when to share their data
- Our users can easily exercise their rights
- We ask for the information strictly necessary for the correct provision of our service

Processing

What do we do with the data?

Compilation
Register
Organisation
Storage
Preservation
Extraction
Consultation
Use
Updating
Blocking
Deletion
Transfer
Access

Whose data are they?

Candidates
Registered job seekers

business Users
Registered talent seekers

Visitors
People browsing without registering

What data do we process?

Identification
Contact
Personal characteristics
Image
Education
Curriculum
Means of payment
Technical Info
Location
Interactions
Communications

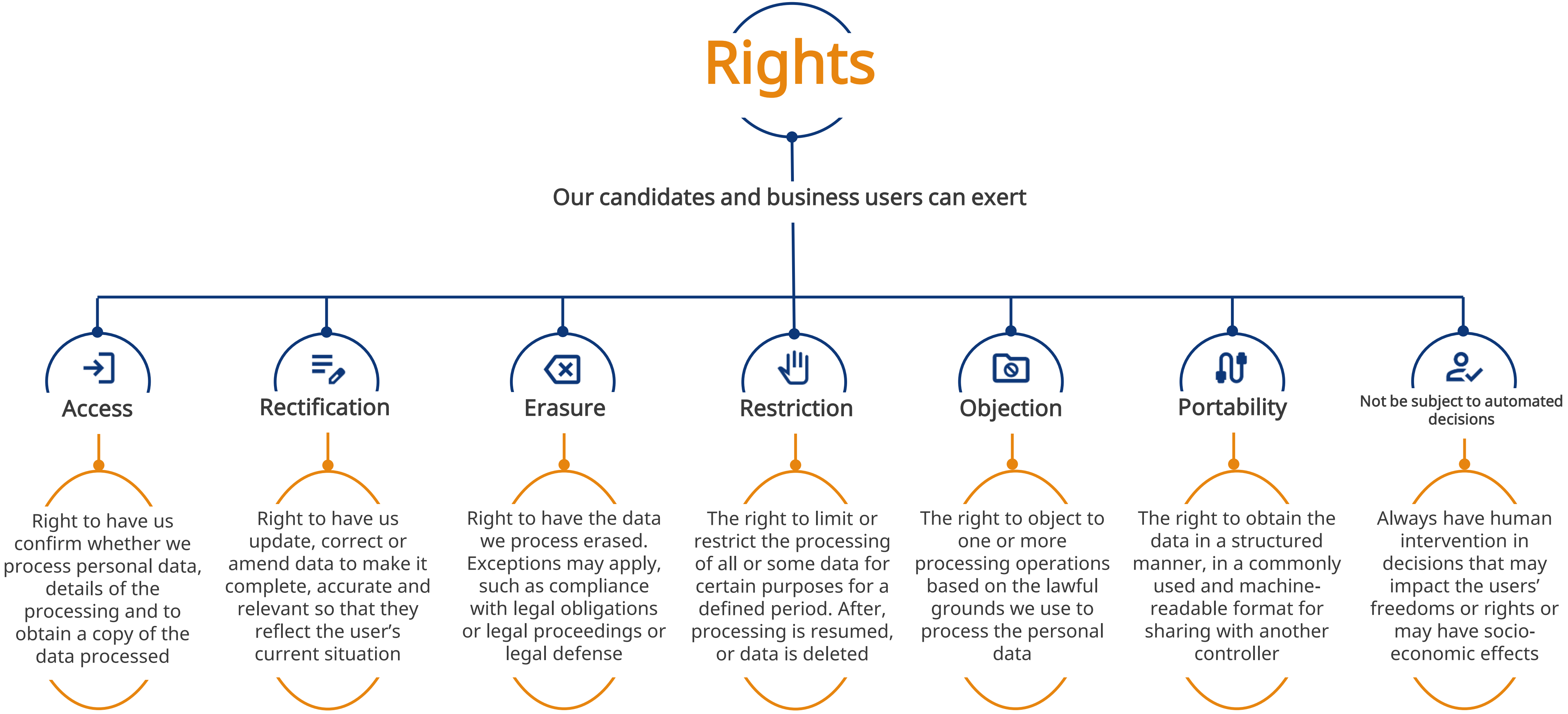
Purposes

After reviewing the purpose-limitation principle and the purposes of **Computrabajo**, here we detail what that purpose means and the legal grounds we have for processing personal data.

Purposes	Legal grounds
Management of services, such as: • Account creation, management and editing • Contact between candidates and business users • Sending of communications related to **Computrabajo's** functioning	Execution of contract
Subscription management and content moderation	
Improvement of our services	Consent
Display of personalised advertising	
Sending newsletters and promotions of other services we offer	
Generation of aggregated information for statistical and analytical purposes	Legitimate interest
Prevention of fraud and abuse	
Compliance with orders of official authorities in the course of their competence	Legal obligation

The Computrabajo portal has a strict privacy policy that all users must agree to before creating an account.

This allows our clients, registered in Computrabajo as business users, to search for candidates, contact them and receive the CVs of those candidates who have applied to published vacancies.



Rights

Our candidates and business users can exert

Access

Right to have us confirm whether we process personal data, details of the processing and to obtain a copy of the data processed

Rectification

Right to have us update, correct or amend data to make it complete, accurate and relevant so that they reflect the user's current situation

Erasure

Right to have the data we process erased. Exceptions may apply, such as compliance with legal obligations or legal proceedings or legal defense

Restriction

The right to limit or restrict the processing of all or some data for certain purposes for a defined period. After, processing is resumed, or data is deleted

Objection

The right to object to one or more processing operations based on the lawful grounds we use to process the personal data

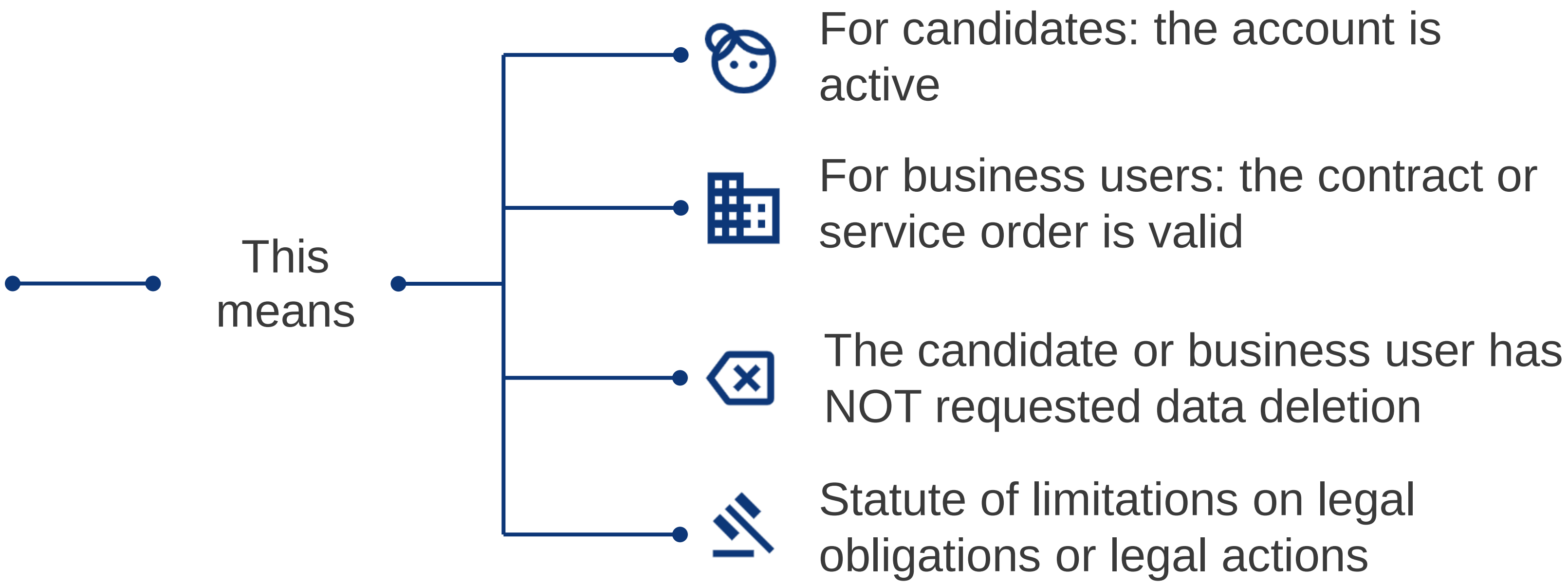
Portability

The right to obtain the data in a structured manner, in a commonly used and machine-readable format for sharing with another controller

Not be subject to automated decisions

Always have human intervention in decisions that may impact the users' freedoms or rights or may have socio-economic effects

We keep the data only for the time necessary to achieve Computrabajo's purposes



This means

- For candidates: the account is active
- For business users: the contract or service order is valid
- The candidate or business user has NOT requested data deletion
- Statute of limitations on legal obligations or legal actions

We share data only when necessary to fulfil Computrabajo's purposes

These are the third parties with whom we share personal data. Sometimes these third parties are in countries other than that of our users.

We make our best efforts to have suppliers that are in countries declared adequate by data protection authorities. In the absence of such a declaration, we implement standard contractual clauses or other mechanisms to maintain the same level of protection as the data has from its place of origin.

Processors

These are third parties or companies within our corporate group which, under our instruction, carry out processing activities. For example: cloud, support, marketing.

Official authorities

They are public entities that in the exercise of their legal competence may order us to share personal data of our users.

business Users (only applicable for candidates)

When a candidate applies for a job vacancy, we share their CV with the business user who posted the vacancy.

About our data processors

As we told you, to provide the **Computrabajo** service, we contract with third parties who, under our instructions, process personal data. These third parties are personal data processors. These are the measures we have in place with respect to them:

Due Diligence

At a minimum, our legal, security and data protection experts review:

- Cybersecurity policies, processes and procedures
- Technical and organisational data protection measures
- Service and support agreements

Reputation

We focus on suppliers that:

- Have international cybersecurity or quality certifications
- Have no fines or investigations for security incidents within the past 5 years
- Publish internal and/or external audit reports
- Are reputable and globally known
- Located in a adequate country

Contract

We draft Data Processing Agreements (DPA) that have as a minimum:

- Obligation to follow instructions from the controller
- Audits
- Communication of incidents
- Support for resolving requests to exercise rights
- Protection for international data transfers
- Authorisation for sub-processors

Follow up

After executing the DPA, we monitor the relationship with the manager to:

- Update changes in the business relationship
- Include new legal obligations in the contract
- Monitor data retention policies
- Recognise amendments in sub-processors

Security Measures

These are the practices and tools we implement to ensure the confidentiality, integrity and availability of candidates‘ and business users’ personal data.

Organisational Measures

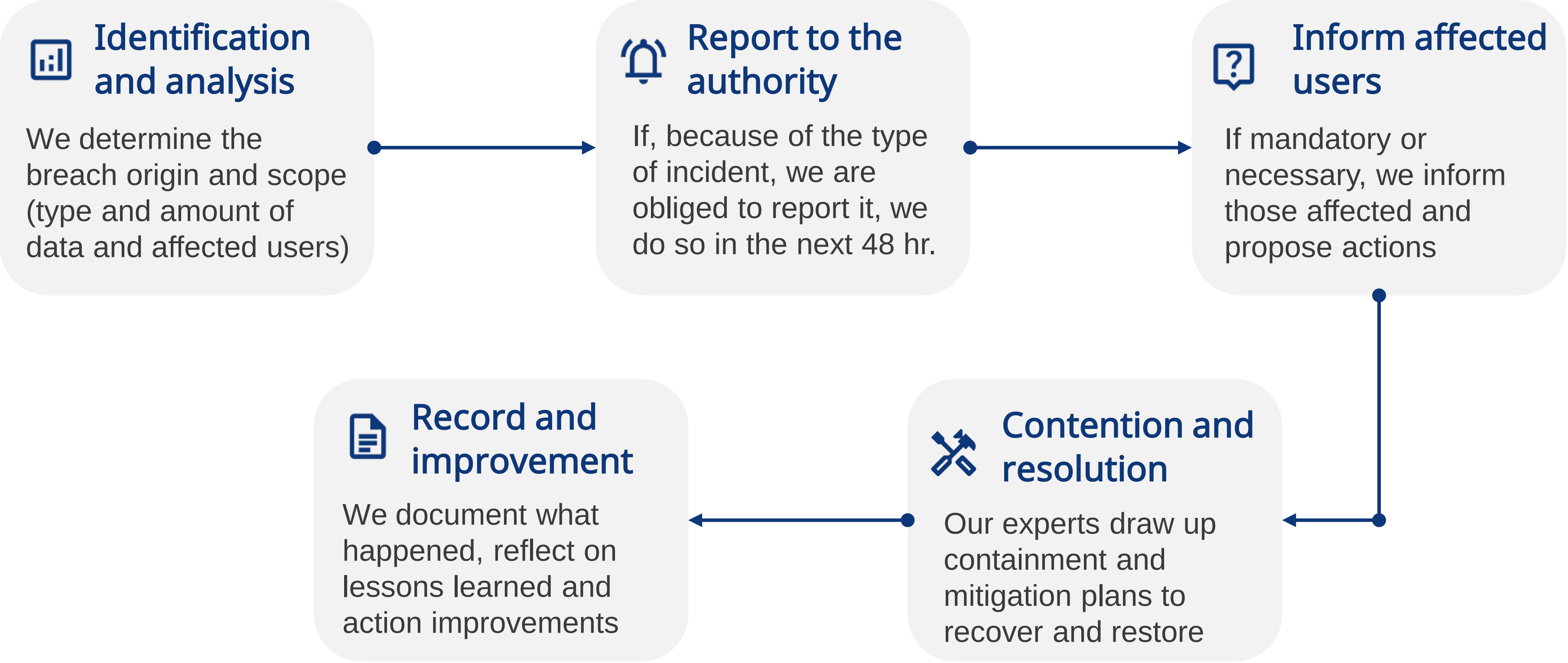
- **Computrabajo's** data protection policy is available for public consultation.
- We have a Data Protection Officer
- We carry out Data Protection Impact Assessments for high-risk processing
- We train our employees
- We have an information security policy
- We maintain a register of processing activities
- We focus on collecting and processing only the minimum necessary data
- We follow applicable incident management regulations

Technical Measures

- We encrypt data in transit (TLS 1.2) and at rest (AES 256)
- We control access to the portal through user authentication
- We have firewalls, intrusion detection/prevention systems (IDS/IPS)
- We update our antivirus
- Implement DLP technologies
- We store personal data in AWS (ISO 27001)
- We implement automatic monitoring systems to detect and respond to suspicious activity
- We implement separate, pseudonymisation, masking or other techniques as required

Data Breach Management

We take the security of the personal data of our candidates and business users very seriously. We never skimp on protection, but we know the risk is never zero. Something can happen. But when it does, this is what we do:



Identification and analysis

We determine the breach origin and scope (type and amount of data and affected users)

Report to the authority

If, because of the type of incident, we are obliged to report it, we do so in the next 48 hr.

Inform affected users

If mandatory or necessary, we inform those affected and propose actions

Contention and resolution

Our experts draw up containment and mitigation plans to recover and restore

Record and improvement

We document what happened, reflect on lessons learned and action improvements

Thank you for trusting Computrabajo. The leading job site in Latin America.

If you have any questions, please contact your appointed account executive.

Computrabajo