nH | HOTEL GROUP

INFORMATION SECURITY FRAMEWORK

Document details

Document Name

Information Security Framework

Document Number

ALLNH-NOR202-EN

Version	**Date**	**Status**
1.0	November 2018	Approved
Author	**Content Reviewed by**	**Approved by**
Information Security	Head of Information Security	Information Security
Owner	**Confidentiality Label**	
Information Security	Internal use	

Version Change History

Version	Last Reviewed	Author	Changes/Comments
1.0	November 2018	Information Security	Initial version

Contents

1. INTRODUCTION

The evolution of Information Technology and its extensive implementation have exponentially increased the risks posed to organizations derived from the main threats of these new technologies. This increased risk leads to the need to implement adequate and proportionate security measures in order to ensure effective and comprehensive protection of information and communication, taking into account operational dynamism as well as the organizational structure of NH Hotel Group (hereafter "NH Group" or "NH").

It is mandatory for NH to ensure compliance with the current legislation, as well as to preserve the confidentiality, integrity and availability of the information, as well as that of the information systems and communications that hold or transmit information that is under the responsibility or owned by NH.

2. OBJECTIVES

The aim of this document is to define the necessary control objectives by developing each of the information security principles included in the NH Security Policy.

3. SCOPE

The current regulations are applicable to the employees of Group NH, its companies and any third parties that, as part of an employment or commercial relationship, may process information that is owned or under the responsibility of NH.

The scope of the regulations includes information and communications systems, IT services and technologies that support the business processes, services and functions of the NH's business, regardless of the location of the treatment or the means employed to process the information.

4. DEFINITIONS

The definitions and terms used in these regulations have been detailed in the Glossary of Terms and Definitions.

5. DETAIL

Below are the control objectives structured by information security domain:

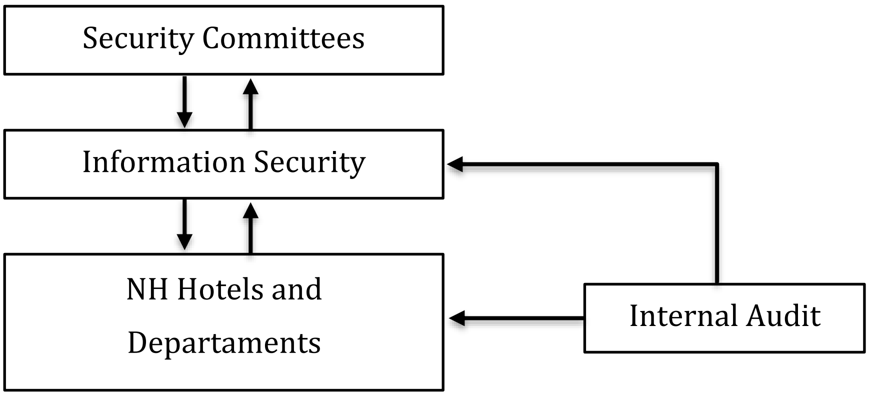
5.1. INFORMATION SECURITY ORGANIZATIONAL STRUCTURE

5.1.1. Internal organization

Protecting the information owned or under the responsibility of NH is a shared responsibility for all employees and internal and external collaborators.

The responsibility for applying the guidelines set out in the NH Security Policy lies with the Hotel Directors, the heads of each NH department and the members of the governing bodies of the companies and other entities that are part of the NH Group.

In order to govern the information security in the NH Group, the NH Management has defined and established the following solid and compact organizational structure:



The organizational structure applicable to NH's information security aims to comply with the following principles:

- Security as an integral process: security will be managed as an integral process, comprised of all the technical, human, material and organizational elements related to information security.
- Security management coordination: through the coordination of Information Security with the different Divisions, Departments, Areas and Business Units of the NH Group, as well as the collaboration of different functions towards a common goal.
- Sufficient authority and adequate resources: the Security Committee and the Information Security Committee have the required authority in the organization to carry out the functions and responsibilities assigned to them, as well as the adequate resources to implement them.
- Effective system for internal governance: security responsibilities will be differentiated and distributed over three different levels, known as lines of defense. The first line of defense consists of hotels and departments that take and assume risks, as well as limiting and carrying out operational and

administrative verifications. The second line of defense contributes to independent risk control, which includes Information Security. Finally, the third line of defense provides an independent, objective and critical review of the first two lines, and it is performed by Internal Audit.

Security Committees

The organization of information security within the NH group is coordinated through the following management bodies: Security Committee and Security Monitoring Committee.

Security Committee

The Security Committee, due to its composition, is the highest management and decision-making body in the NH Group in relation to information security.

The Committee's objective is the continuous improvement of security, ensuring a homogeneous minimum level that is in accordance with the needs of each business.

The guidelines established to run this Committee are:

- The Coordinator of the Committee is the Head of Information Security.
- The Secretary of the Committee is a member of the Information Security department, who will be in charge of taking minutes of the meetings held.
- Its composition is decided by the Committee itself, taking into account operational and business criteria, geographical factors and sufficient representation of the NH Group companies. At least, the following functions must be represented in the Committee:
  - Head of IT & Systems
  - Head of Legal Affairs
- Committee members may, exceptionally, delegate their assistance to one of their collaborators.
- Members of Internal Audit may be invited to Committee meetings, but only as observers.
- The Committee must meet at least annually.
- The convening of the Committee must be performed by the Secretary of the Committee at the request of the Coordinator of the Committee, through telematic means accompanied by the meeting agenda, as well as all the required documentation.

The functions and responsibilities of the Committee are as follows:

- To assume responsibility for ensuring compliance with the corporate information security principles described in the NH Security Policy.
- To define the relevant actions required to adequately manage information security and business continuity risks, ensuring the alignment with the NH Group's business objectives.
- To propose to the NH Management changes to the Security Policy, as well as information security principles in order to ensure the suitability and effectiveness of the policy.
- Periodic review of the Security Policy, prior to its review and approval by NH Management.
- To ensure and foster compliance with the Security Policy and with the regulatory standards that derive from it and that are mandatory for the entire NH Group, as well as its regulatory development.
- To approve and ensure compliance with a comprehensive security strategy that is directly linked to the business objectives, defining corporate information security objectives on an annual basis.

- To periodically report to NH Management on the status of corporate information security objectives and residual risks.
- To allocate the necessary resources to plan, implement, operate, supervise, review, maintain and improve information security management.
- To approve the initial assignment and periodic review of information security roles and responsibilities, and establish criteria to ensure segregation of duties.
- To establish an information security training program for all NH employees.
- To promote periodic audits to verify compliance with the NH Group's legal, regulatory and contractual obligations regarding information security.

Security Monitoring Committee

The Security Monitoring Committee, due to its composition, is the body in charge of implementing a more exhaustive monitoring of the different initiatives related to information security within the NH Group.

The objective of the Monitoring Committee is to achieve a continuous improvement of security management, ensuring the involvement of IT & Systems, more specifically the Applications and Infrastructure Areas.

The guidelines established to run this Committee are:

- The Coordinator of the Committee is the Head of IT & Systems.
- The Secretary of the Committee is a member of the Information Security department, who will be in charge of taking minutes of the meetings held.
- Its composition is decided by the Committee itself, taking into account operational and business criteria, geographical factors and sufficient representation of the NH Group companies. At least, the following functions must be represented in the Committee:
    - Head of IT & Systems
    - Head of Applications of IT & Systems
    - Head of Infrastructure of IT & Systems
- Committee members may, exceptionally, delegate their assistance to one of their collaborators.
- The Committee must meet at least quarterly.
- The convening of the Committee must be performed by the Secretary of the Committee at the request of the Coordinator of the Committee, through telematic means accompanied by the meeting agenda, as well as all the required documentation.

The functions and responsibilities of the Committee are as follows:

- To review and approve the security standards deriving from the Security Policy that are mandatory for the NH Group.
- To propose to the Security Committee the allocation of the necessary resources to plan, implement, operate, supervise, review, maintain and improve information security management and compliance with laws, regulations and contractual obligations regarding information security.
- To approve the initial assignment and periodic review of roles and responsibilities, as well as to establish criteria to ensure segregation of duties.
- To prioritize information security activities when resources are limited.

- To review the development of approved risk management projects.
- To report regularly on the progress of information security in the NH Group to the Security Committee.
- To promote continuous improvement in relation to information security management.
- To coordinate the Continuity Plans of the Divisions, Departments, Areas and Business Units of the NH Group, to ensure effective action in the event that they need to be activated.
- To promote periodic reviews to verify compliance with the NH Group's legal, regulatory and contractual obligations regarding information security.

Information Security

Information Security is the area of the NH Group responsible for ensuring compliance and regular update of the NH Security Policy.

The functions and responsibilities of the Committee are as follows:

- To report on the progress of information security in the NH Group to the Security Committee.
- To promote and advocate NH's information security guidelines so that they are aligned with the NH Group's business needs.
- To develop the Security Policy, ensuring its implementation and alignment with the remaining regulatory bodies of the NH Group.
- To perform risk analyses in order to define the required organizational and technical security measures, in a proportionate manner, to mitigate the risks to which the NH Group is exposed.
- To provide support during the implementation of organizational and technical security measures.
- To ensure the implementation of organizational and technical security measures that comply with the applicable security standards.
- To monitor compliance with the security controls defined in the regulatory standards that make up the Security Policy.
- To define and manage metrics and reporting on information security.
- To define the necessary procedures for crisis management and ensure business continuity.
- To define and manage the NH Group's Information Security Training and Awareness Plan.
- To define and manage the annual review plans and exhaustive security analyses of NH's information and communications systems and IT services.
- To define and operate the security systems implemented in the NH Group that are responsible for monitoring and controlling the proper operation of information and communications systems of the NH's IT services.
- To manage and respond to information security incidents. If necessary, coordinate computer forensic analysis.
- To manage requests, problems and changes in relation to information security.
- To manage identities and access control within the IT systems.
- To establish and maintain contact with stakeholders and forums and initiatives in the field of information security.

Information Security should also establish contact with information security authorities and specific stakeholders so that it can increase its level of excellence in information security, keep up to date with the latest trends and share knowledge in sectoral forums. For this reason, Information Security interacts with:

- Professional associations for information security (e.g., ISACA - Information Systems Audit and Control Association, ISMS Forum, CSA - Cloud Secure Alliance, etc.)
- Public bodies related to information security (e.g., INCIBE - National Institute of Cybersecurity, CCN-CERT - National Cryptology Centre - Computer Emergency Response Team, ENISA - European Union Agency for Network and Information Security, etc.).
- Events related to information security, organized by professional associations, private sector companies, public bodies or non-profit associations.
- Law enforcement agencies engaged in the investigation of information security incidents, including information leaks (e.g., EC3 Europol European Cybercrime Centre, GDT - Grupo de Delitos Telemáticos de la Guardia Civil de España, etc.).

The Head of Information Security is responsible for Information Security. He is therefore responsible for managing the aforementioned functions and responsibilities of Information Security.

NH Hotels and Departaments

NH Hotel staff and members of the NH Departments

Hotel staff and members of Departments, regardless of whether they are internal or external employees or collaborators, who handle information owned by or under the responsibility of NH, have the following information security functions and responsibilities.

- To read, understand, and comply with the NH Security Policy, as well as the normative standards that derive from it.
- To actively protect the information assets assigned to them.
- To guarantee the confidentiality and integrity of the information to which they have access and to be aware and apply the criteria for classifying information and the measures to properly process it.
- To guarantee the confidentiality of the access credentials provided by NH that were assigned to them.
- To report any security incidents or unusual events that are observed during the operation of NH's information and communications systems, as well as IT services.

Hotel Managers and Department Heads

Hotel Managers and Department Heads, or those designated by them, must assume the following functions and responsibilities with regard to information security:

- To define the proper use of information assets under their responsibility.
- To authorize the use of information assets by employees and internal and external collaborators of the NH Group.

- To ensure that all employees and internal and external collaborators who organizationally belong to or provide services to the Hotel or Department are aware of and apply the NH Security Policy.
- To ensure that risk analyses and organizational and technical security measures are implemented in its Hotel or Department, as well as developing the information security procedures necessary to adapt the NH Security Policy to its daily operations, notifying Information Security of any situation that requires a substantial modification with respect to what is indicated in the security standards.
- To properly coordinate and manage the processing of information within its Division, Department, Area or Business Unit.
- To coordinate the security projects assigned, totally or partially, to their Division, Department, Area or Business Unit.
- NH employees who hold the roles of information owner or business process manager, in accordance with regulatory security standards, are the owners of information risks and business process risks.

IT & Systems

The functions and responsibilities of IT & Systems relating to information security are as indicated below:

- To collaborate with the Head of Information Security in order to coordinate and control organizational and technical security measures applicable to information and communications systems, ensuring the proper operation of the security management process.
- To ensure the analysis, design, coding, testing and maintenance of software products, to meet the needs of customers and users, ensuring compliance with security requirements established in regulatory standards.
- To apply or collaborate in the application of controls and organizational and technical security measures that ensure the confidentiality, integrity and availability of NH's information assets throughout their life cycle.
- To provide support in the selection, implementation, configuration and operation of the appropriate mechanisms and tools to apply the Security Policy.
- To define policies and procedures that ensure compliance with the functions and responsibilities assigned to IT & Systems in the NH Security Policy, as well as the regulatory standards that derive from it.
- To establish continuity plans, carrying out periodic tests to guarantee their effectiveness.
- To notify security incidents affecting information and communications systems under its responsibility, as well as collaborate in their investigation.

Legal Affairs & Compliance

The functions and responsibilities of Legal Affairs & Compliance with regard to information security are as follows:

- To provide advice on legal, regulatory and contractual requirements regarding information security to which the NH Group is subject.

- To collaborate and provide support in the identification of the initiatives that Information Security should coordinate or be involved in and that will enable the supervision of the operation and compliance with the crime prevention model implemented in NH.

Operations

The functions and responsibilities of Operations with regard to information security are as follows:

- To define and implement physical access control measures to NH buildings.
- To establish and maintain the relationship with the Law Enforcement Agencies.

People

The functions and responsibilities of People with regard to information security are as follows:

- To determine profiles and responsibilities in the employee selection process, as well as to review and verify employee data prior to hiring.
- To establish internal disciplinary processes.
- To determine the responsibilities of employees in the event of termination of the employment relationship, in accordance with the NH Security Policy.
- To initiate the process of withdrawing employees' rights of access to NH information in the event of termination of the employment relationship.
- To ensure the signing of confidentiality agreements and contractual clauses on information security, as well as privacy, between the NH Group and its employees prior to their incorporation.

Internal Audit

Internal Audit is the department that ensures objectivity, independence and confidentiality of the NH Group's auditing processes.

The functions and responsibilities of Internal Audit with regard to information security are as follows:

- To provide assurance in the evaluation of the effectiveness of security risk management and the controls implemented in this area.
- To evaluate the operation of security controls implemented through audits and to issue an opinion based on the associated risks and findings detected, establishing the appropriate recommendations.
- To promote the inclusion in the NH Group Audit Plan, which is approved by the Audit and Control Committee, of the appropriate audits based on the risk analyses carried out by Information Security, as well as on its own risk analyses.
- To collaborate with Information Security for the alignment with NH's Corporate Assurance Model.
- To attend Security Committees as a guest and observer in order to periodically identify activities related to the NH Group’s security.
- To monitor identified deficiencies or recommendations.

5.1.2. Risk analysis and management.

Information Security employs an information security risk analysis and management methodology that takes into account the sensitivity and criticality of information assets. This methodology identifies the organizational and technical security measures required to mitigate the identified risks.

The scope of this methodology only affects information security risks and not other types of risks that may affect the NH Group (e.g., credit, market, fraud, etc.).

Based on the control objectives of the security domains of ISO/IEC 27001, an assessment of the maturity level of the processes and systems within the scope is performed. Threats and vulnerabilities to which processes and systems within the scope are exposed are identified. The admissible risk threshold is determined and action plans are established to minimize the impact of the risks to be mitigated. For all risks whose maturity level is higher than the admissible risk threshold, Information Security and affected Departments (e.g., IT & Systems, Hotel Management, etc.) are responsible for establishing the necessary security controls and actions that would enable the improvement of the maturity level. Once an action plan has been proposed, the Security Committee is responsible for approving it.

5.1.3. Information security in project management

NH Hotels and Departments are responsible for the planning and execution of their projects.

All projects or tasks that require a technological development will necessarily require the involvement of IT & Systems in the life cycle of the project or task. In turn, IT & Systems must involve Information Security as they deem necessary.

IT & Systems must involve Information Security when one of the following criteria is met:

- The project or task requires the implementation of a new information system or modification of an existing one.
- The project or task requires hiring a service from an external supplier to the NH Group.

Similarly, the involvement of Information Security may also be necessary as a result of regulatory changes affecting the security of NH information. When Legal Affairs, Compliance and/or the Data Protection Officer (DPO) of the NH Group detect such a case in a project or task, they must notify Information Security.

5.1.4. Mobile Devices

Corporate Mobile Devices

Prior to the delivery of a corporate mobile device, employees and internal and external collaborators must sign a document accepting legal clauses regarding the acceptable use of corporate NH mobile equipment and devices (such as laptops, telephones, tablets, etc.).

Employees and internal and external collaborators should consider the following aspects when using a corporate NH mobile device:

- Never lose sight of the device.
- Activate, and keep activated, the device lock every 10 minutes of inactivity, and the request for a password or biometric control to unlock the terminal.
- Use strong, complex passwords to protect the device.
- Do not unlock or tamper with device components.
- Do not open or accept files from unknown senders.
- Install software previously authorized by NH.
- Do not install applications of unknown or unreliable origin.
- Do not use external and removable memory cards.
- Activate, and keep activated, the remote erasure system, whenever possible.
- Do not leave communication protocols activated if unused. In particular, disable Bluetooth and WiFi if not in use.
- Do not connect to unknown wireless access points (WiFi networks).

A mobile device management solution (MDM) agent can be installed to secure, monitor and manage corporate mobile devices remotely. This agent will be installed upon request from Information Security. The agent will provide the following functionalities:

- Installing and running applications remotely.
- Application of control policies over the device and applications.
- Remote location of the device.
- Remote locking of the device or functions.
- Remote erasure of information.
- Automatic scanning of virus or malicious software.

Non-corporate mobile devices

Unless expressly authorized, non-corporate devices (i.e., personal devices, third party devices or devices not owned by the NH Group) may not be used for the processing or storage of information owned by or under the responsibility of NH.

If authorized, Information Security must approve non-corporate devices prior to the start of processing or storage of NH information.

Employees and internal and external collaborators must ensure the following guidelines for non-corporate devices:

- The use of the devices must adhere to NH's internal policies (especially Human Resources or People policies) and to current and applicable legal and regulatory requirements.
- The device should not be shared with another person (especially family, friends, etc.).
- Devices must be securely kept and protected outside NH facilities.
- In the event of loss or theft of the device, Information Security should be notified immediately via email infosec@nh-hotels.com.

Additionally, internal and external employees and collaborators must ensure that the devices are prepared to meet the following requirements

- Devices must have an original operating system provided by the manufacturer or developer installed at all times (i.e. no operating system modifications, rooted or jailbroken devices, etc.).
- The operating system of the devices must be kept up to date according to the specifications of the manufacturer or developer.
- Device passwords must be set according to the requirements defined in this NH Security Policy. Especially with regard to minimum length, complexity, etc.
- Devices must be set to systematically force screen lock after ten (10) minutes of inactivity.
- Mobile devices should be set to automatically apply deletion of all stored information after ten (10) failed login attempts. This deletion must return the device to its original default settings.
- Devices must have an approved full disk encryption solution installed and in use at all times.
- The devices must have an anti-malware/antivirus solution installed and updated.

In addition, Information Security may require the installation of a mobile data management solution (MDM) agent on the mobile device.

NH must request access to non-corporate devices and must protect the privacy of such devices at all times.

5.1.5. Teleworking

Only previously authorized internal and external employees and collaborators can perform telework, i.e., connect to NH's information and communications systems from a location outside the NH Group's facilities allowing them to work under the same conditions as if they were physically at NH's own facilities.

Employees and internal and external collaborators must ensure the following aspects in relation to teleworking:

- Connection to NH's information and communication systems must be by means of a VPN authorised by NH. In no case may connections to NH systems be established from a public network (such as the Internet) without having been authenticated to a VPN service authorized by NH.
- Never lose sight of the device when the device is connected to NH information and communications systems.
- In public places or with people outside of NH, use privacy filters on device screens.
- Prevent individuals not authorized by NH from handling the device.
- Prior to connecting to NH's information and communications systems, ensure that the antivirus is active and up to date.
- Do not connect to unknown wireless access points (WiFi networks).
- Do not copy, move, and store information classified as Restricted or Confidential on local disk drives and removable electronic devices unless explicitly authorized. Copying, moving and storing payment data (e.g., account numbers, bank card numbers, cardholder names, service codes, expiration dates, etc.) is expressly prohibited.

5.2. HUMAN RESOURCES SECURITY

5.2.1. Prior to employment

NH, for the proper performance of its business activities, will require hiring of employees and internal and external collaborators, which include the following natural or legal persons:

- Employees of the NH Group, regardless of the type of contract that determines their employment relationship, the position they hold or the geographical area in which they carry out their work.
- Interns.
- Executives of the NH Group, regardless of the type of contract determined by their employment or commercial relationship, position they hold or the geographical area in which they perform their work. Executives of the NH Group are: members of the Senior Management (defined as those who report directly to the Board of Directors or to the Company's Chief Executive Officer and, the internal auditor), all the directors and department heads and hotel directors.
- Members of the administrative bodies of the companies and other entities that make up the NH Group, regardless of the composition, form and operating regime of the body in question.
- Suppliers, collaborators and any other stakeholder that, although not specifically mentioned, has a direct link with the operations of the NH Group.

Background check

The call for a role to be filled must state the security requirements considered relevant.

As soon as a curriculum vitae with identifying data of a candidate is obtained, Human Resources (or People) of the NH Group must provide the interested party with the information indicated below:

- Identity of the party responsible for processing personal data (in most cases, the corporate name of the NH Group).
- Simple description of the purposes of the processing of personal data.
- Legal basis for the processing of personal data.
- Whether or not it is expected that there will be transfers or assignments of the personal data to third countries.
- Making a reference to the possibility of exercising the right to request from the controller access to personal data, and its rectification or deletion, or the limitation of its processing, or to oppose processing, as well as the right to data portability; as well as the right to withdraw consent at any time, without this affecting the lawfulness of processing based on consent prior to its withdrawal; or the right to file a complaint to a supervisory authority.
- If the information does not come from the data subject, indicate the data source.
- Reference should also be made to where the data subject can find the following additional information:
    - Contact details of the person responsible for processing personal data (in most cases, the NH Group's corporate mailing address).
    - The contact details of the data protection officer, if designated by NH.
    - Extended description of the purposes of the processing.

- The period during which the personal data will be kept or, where this is not possible, the criteria used to determine this period.
- If automated decisions are to be made, the profiles and the logic applied.
- Inform of the possible consequences of not providing the personal data requested by NH, as the communication of such data is a necessary requirement to be able to enter into a contract.
- Recipients or categories of recipients of transfers of personal data.
- Decisions on adequacy, guarantees, binding corporate rules or specific situations applicable to transfers to third countries.
- How to exercise rights of access, rectification, deletion and portability of personal data, and limitation or opposition to processing.
- How to exercise the right to withdraw consent.
- How to exercise the right to complain to a Supervisory Authority of a Member State of the European Union.
- If the information does not come from the data subject, detailed information on the origin of the data, including whether they come from publicly accessible sources.
- If the information does not come from the data subject, categories of data being processed.

During the candidate selection process, NH Human Resources should perform, if applicable, reference checks, especially work experience and training. Such checks should be carried out in accordance with current and applicable legislation, as well as NH's internal codes of ethics, in a manner proportional to the classification of the information to which access is required.

Employments terms and conditions

As part of their contractual obligations, employees must accept and sign the terms and conditions of the employment contract, which must set out their responsibilities in complying with the Code of Conduct and internal information security procedures, and include contractual clauses on confidentiality and duty of secrecy. It should be noted that the NH Group Code of Conduct establishes, among others, the employee's responsibility in relation to the confidentiality of NH’s information.

Specifically, the contractual clauses should develop the following aspects:

- Information on the processing of personal data
    - In particular, the employee must authorize the NH Group to process his or her personal data for the following purposes: payroll and payment management, and to carry out the necessary activities in accordance with the applicable laws and regulations on risk prevention and health surveillance.
    - Should it be necessary to request accreditation for events or before private entities or Public Administrations, the employee must authorize the NH Group to communicate the data required by third parties exclusively for the indicated purpose.
- Functions and obligations in relation to the processing of personal data.
- Duty of professional secrecy and legal duty to maintain absolute confidentiality with respect to the data to which the employee has access or is aware of.
    - Employees must also be informed that they are subject to the duty of confidentiality even after the termination of their employment relationship with the NH Group, as established in the generic right of "contractual good faith" included in both the Workers' Statute (Art. 5.a) and the Civil Code (Arts. 1258 and 7.1).

- Functions and obligations deriving from the NH Security Policy, especially aspects relating to:
  - Credentials management
  - Information confidentiality
  - Management of security incidents
  - Intellectual and industrial property
  - Use and removal of equipment and devices
  - Backup copies
  - Use of Internet access, email, and collaborative tools
- Disciplinary or sanctioning process in the event of non-compliance with current and applicable laws and regulations, as well as NH Group internal codes and standards, regarding information security.

5.2.2. During employement

Responsibilities and obligations during employment

Employees and internal and external collaborators must be respectful and ethical in all communications, always bearing in mind that they are representing NH. Similarly, any statement to media should be declined, referring the query to the Communication Department of the NH Group.

Employees and internal and external collaborators should refrain from treating NH information in public or private places where it may be heard by third parties who do not have access to such information.

It is forbidden for employees and internal and external collaborators to disclose information about customers or employees of the NH Group to a third party outside of NH. It is especially forbidden to communicate stays at NH Group facilities, timetables or provide contact information to third parties who identify themselves as family members or friends of NH customers or employees.

The sending or forwarding of discriminatory information, chain letters and obscene or tasteless material is explicitly prohibited.

Information Security must periodically evaluate the fulfillment of the information security responsibilities of employees and internal and external collaborators.

Disciplinary Procedure

Employees and internal and external collaborators may be sanctioned for labor non-compliance, in accordance with the type of offences and sanctions established in the legal provisions or in the applicable collective agreement.

The assessment of offences and the corresponding sanctions is the responsibility of People (Human Resources). This Department, as the highest responsible body, must agree on the corresponding disciplinary measure in the event that an investigation into the alleged facts may be concluded as a breach of internal or external regulations.

Training and awareness-raising

Talent, Learning & Development and Information Security must provide employees with the necessary tools and training to guarantee, depending on their work activity, the correct fulfilment of their responsibilities with regard to information security.

The following types of training activities will be considered:

- Awareness, regarding the risks to which NH information is subject and the best practices and standards to be considered when processing information (e.g., security alerts, newsletters, news, etc.).
- General training on security operating procedures to be considered in information management (e.g., management of secure information exchange tools, how to report security incidents, how to encrypt or sign emails, etc.).
- Technical training for IT & Systems personnel, related to aspects directly related to the safe operation and maintenance of systems and applications. Implementing technical training should also be considered for members of Information Security, such as the regular attendance to courses or lectures on information security given in specialized forums.

The Security Committee, at the proposal of the Security Monitoring Committee, must approve a Security Training Plan that includes training sessions on security of information systems for employees, training activities and awareness-raising campaigns. This Plan must have an annual detail of activities and may be revised at a later date if deemed necessary, in order to incorporate or replace training initiatives. Similarly, the Security Monitoring Committee must evaluate the results obtained, so that the effectiveness of the training actions carried out can be objectively measured and contribute to the process of continuous improvement of the NH Group's security.

5.2.3. Termination of employment or change of roles and/or responsibilities

Return or deregister of information assets

May it be by decision of NH, the employee or collaborator, or both parties, the termination of the employment relationship must be carried out in accordance with the provisions of the applicable collective agreement or, if not available, in the Workers' Statute.

The person directly responsible for the specific employee or collaborator must notify the decision to Human Resources of the NH Group.

Employees and internal and external collaborators must return all assets of NH, especially user credentials, that are in their possession at the end of their employment or change in position. Human Resources must coordinate the return of physical information assets.

In addition, Human Resources should, as soon as possible, notify IT & Systems and Information Security about the need to remove the access permits to the NH Group's information and communications systems. IT & Systems and Information Security must inform Human Resources when access permits have been withdrawn.

Change of roles and/or responsibilities

Change of roles and/or responsibilities within the NH Group, such as promotions or relocations, are not considered employee termination cases. However, Human Resources is required to notify IT & Systems and Information Security to ensure the removal of access permits to the NH Group's information and communications systems.

Confidentiality agreements after termination of employment

According to the applicable collective agreement, in the event of a serious breach or violation of applicable laws or regulations, as well as the NH Group's internal rules, a disciplinary process may be applied that could result in dismissal. The need to initiate legal action should be assessed by the NH Group's Management, Legal Affairs and Human Resources, and appropriate action should be taken based on applicable laws and regulations.

If breaches of confidentiality agreements that could compromise the security of the NH Group's information are detected, Legal Affairs and Human Resources must inform the Security Committee.

5.3. MANAGEMENT OF INFORMATION ASSETS

5.3.1. Responsibilty for information assets

Inventory of information assets

NH information assets must be identified and inventoried.

The NH Group information asset inventory must be maintained by IT & Systems. This inventory must maintain all relevant minimum information in order to properly manage information security. Among others, this database will contain information about the IP address and/or URL of the information asset, the operating system, its version, and interdependencies with other assets. The contact information of the owner of the information asset must also be provided.

Assets ownership

NH owns all information assets made available to its employees for the performance of their duties.

In turn, NH information must have an information owner assigned. The owner must be an internal employee of the NH Group.

The owner of the information is responsible for defining for what uses and purposes the information assigned to him/her can be processed.

The owner of the information is responsible for its classification and protection in accordance with the NH Security Policy.

Acceptable use of information assets

Users of NH's information assets are responsible for ensuring that they are used in accordance with the NH Security Policy and applicable, current legislation. Generally, the use of NH's information assets for purposes that are not approved or authorized as NH Group operations or activities constitutes misuse.

The use of NH information and information assets for purposes other than those strictly related to the normal performance of job duties and responsibilities at NH is expressly prohibited. Their use is also subject to monitoring and auditing by NH, within the limits set by current legislation.

The use of corporate IT services, such as Internet browsing or e-mail service, must be restricted to employees who strictly need it to carry out their work activity.

The installation of software on NH equipment or devices that are not duly authorized by NH, as well as the modification of settings and the installation and execution of malicious programs, is prohibited.

Unless expressly authorized, the equipment or devices of external collaborators must not be connected to the corporate networks of NH or third parties. In particular, the connection of equipment or devices of external collaborators to NH communication equipment in hotels without prior authorization is expressly prohibited.

5.3.2. Categorization of information

Types of information assets

Primary information assets are:

- Information generated by own means or by third parties that support the functions and services of the NH Group, regardless of the information carriers containing it.
- Information systems and IT services that support the management of the NH Group's activity and/or the provision of services and that the information they process cannot be classified as a primary information asset.

Support information assets are:

- Data structures in which information is kept, such as databases, files, document managers.
- Servers and systems in which information is stored.
- Information systems and IT services used for information processing.
- Communications equipment and systems between information systems, IT services or third party systems.
- Hardware or information carriers that allow the processing of information (workstations, USB sticks, hard disks, etc.).
- People who process information.
- Physical facilities in which the information assets are located.

Categorization of information assets

Primary NH information assets should be categorized in order to determine the level of protection to be applied.

The categorization of primary information assets should be carried out according to the following criteria:

- Availability: it assesses the impact of interrupting access to information at the time it is required.
- Confidentiality and Integrity: determined by the sensitivity of the information and how it is processed.

Based on these criteria, a categorization level of availability (or level of availability) will be assigned to a primary information asset:

- Low: When the business process manager accepts that the target recovery time (TRO) is equal to or greater than twenty-four (24) hours. TRO is defined as the maximum acceptable time for the business process or service to be stopped from the time an incident occurs until it is recovered (worsened, if necessary); taking into account the legal, operational, economic and brand image impacts.
- Medium: When the person in charge of the business process accepts that the TRO is equal to or greater than one (1) hour and less than twenty-four (24) hours.
- High: When the person in charge of the business process accepts that the TRO is less than one (1) hour.

Based on these criteria, a categorization level of confidentiality and integrity (or level of confidentiality) will be assigned to a primary information asset:

- Public: Information that does not require protection in its disclosure. Either because its disclosure, intentional or accidental, does not imply any type of negative impact for the NH Group; or because the information is accessible by people outside the NH through public sources.
- Internal Use: Internal information necessary for the adequate performance of NH. The information needs protection, but is not classified as Restricted or Confidential. The intentional or accidental disclosure of the information cited may have a minor economic impact on the NH Group (more than 1% of the annual budget), risk of a minor sanction according to the laws or regulations, not significantly deteriorating the corporate image, not threatening the rights of natural or legal persons.
- Restricted: Internal information, to which only certain groups of employees, collaborators, departments or business areas must have access. Such information needs protection, but it is not classified as Confidential. The intentional or accidental disclosure of such information may have a serious economic impact on the NH Group (more than 5% of the annual budget), risk of serious sanctions in accordance with laws or regulations, significantly deteriorating the corporate image, or directly affecting the rights of natural or legal persons.
- Confidential: Internal information, to which only small groups of employees, collaborators, departments or business areas must have access. Such information needs maximum protection. The intentional or accidental disclosure of this information can have a very serious economic impact on the NH Group (more than 10% of its annual budget), very serious risk of sanction according to laws or regulations, or significantly deteriorate corporate image.

Generally, in the absence of categorization of an information asset, the security measures required for assets categorized as Level of availability “Low” and Level of confidentiality “Internal Use” will be applied.

The categorization levels of a primary information asset must be transferred to the supporting information assets that intervene in its processing. When a supporting information asset supports more than one primary information asset, the categorization levels that are more restrictive must be applied.

Categorization process

The categorization of new primary information assets must be carried out prior to the start of a new processing.

The owner of the information has to review the categorization of the information assets under his responsibility on an annual basis or in the event of any change involving a modification in the type of information, information processing, purpose of the information or in the parties involved in the processing. As a result of the aforementioned review, the following actions may be taken:

- Modify the categorization levels assigned to an information asset.
- Generate a new information asset with the categorization levels different from those of the original asset from which it was created.

The owner of the information has to inform Information Security, as well as the Data Protection Officer (DPO) of the NH Group (or Legal Affairs in its absence), in the event of a new categorization of an information asset under its responsibility or in the event of a change in the categorization level of an asset.

Responsibilities

In each Hotel or Department of the NH Group, specific employees must be designated to assume the role of information owners.

Information owners are responsible for ensuring that the information assets for which they are responsible are inventoried and categorized in accordance with the NH Security Policy, as well as the regulatory standards that derive from it.

The information owner may delegate the operational task of inventorying and categorizing an information asset, but may not delegate its responsibilities in this regard.

The information owner is responsible for making employees and internal and external collaborators aware of the categorization levels of the information assets they are dealing with in accordance with their roles and responsibilities.

In addition, Information Security is responsible for informing IT & Systems of the categorization levels of the information assets they are dealing with in accordance with their roles and responsibilities.

The application of organizational and technical security measures by employees and internal and external collaborators of NH must take into account, among other reasons, the categorization levels assigned to the information assets. These security measures are detailed in the NH Security Policy, as well as the regulatory standards that derive from it.

5.3.3. Management of information carriers

Labelling of information carriers

Information carriers (inter alia, hard copies, laptops, USB sticks, external hard disks, CDs, DVDs, etc.) of the NH Group should be labelled in such a way that the most restrictive level of confidentiality of the information asset is clearly and visibly indicated.

On electronic information carriers, information should be labelled using watermarks indicating the categorization level of the document and by means of text included at the document's heading.

On physical information carriers, the information must be labelled with tags or labels indicating the level of categorization of the information.

Management of information carriers

Information categorized with a level of confidentiality "Internal Use" or higher must be accessible and processed only by employees and internal and external collaborators authorized to do so. Therefore, information carriers containing classified information should be guarded and stored to prevent unauthorized access.

Information carriers that the NH Group holds within the framework of a legal contract or agreement must be protected in accordance with the terms specified in that contract or agreement.

Employees and internal and external collaborators must comply with the archiving criteria established in the NH Group.

Distribution

Unless expressly authorized by the information owner, employees and internal and external collaborators must not extract or share information categorized as "Confidential", "Internal Use" or higher outside the NH Group facilities, regardless of the information carrier in which it is found.

The information owner must authorize only those cases in which transportation or distribution is unavoidable for the proper operation of NH's business processes.

Where authorized by the information owner, the internal or external employee/collaborator who will guard the information carrier during transportation shall consider the following aspects:

- Information carriers must be secured during the entire journey.
- Prior to the delivery of an information carrier labelled as "Restricted" or "Confidential", the identity of the recipient must be confirmed.
- Information carriers labelled as "Confidential" must be traceable from distribution to receipt.

Generally, technical details and software copies shall not be sent or transmitted to other countries or states. If this is unavoidable for the proper operation of NH's business processes, Legal Affairs should be consulted beforehand to confirm that no import/export regulations, industrial or intellectual property laws or regulations would be violated.

Printing

Employees and internal and external collaborators who print information categorized as "Internal Use", "Restricted" or "Confidential" must make all reasonable efforts to ensure that the information carriers remain safe throughout the print life cycle. This includes, but is not limited to:

- Printing information categorized as "Restricted" or "Confidential" on printers located in the user's viewing area.

- Do not leave documents on photocopiers, scanners, printers or faxes.
- Securely dispose of unnecessary documents.
- Avoid unnecessary generation and accumulation of printed documents. As far as possible, process information electronically.

Copying

Employees and internal and external collaborators should consider the following aspects when copying information carriers with NH information:

- Information carriers containing information categorized as “Restricted” or “Confidential” may only be copied with the permission of the information owner.
- Copies of information carriers must be categorized by default with the same categorization levels as the original information carrier.

Storage

With respect to the physical storage of information carriers containing information owned by or under the responsibility of NH, employees and internal and external collaborators must take into account the following aspects:

- Information carriers containing information categorized as “Restricted” or “Confidential” must be stored in a locked room or, if not available, in a locked filing cabinet or safe.
- Information carriers containing information categorized as “Restricted” or “Confidential” must be stored in a restricted area (i.e., non-public area).
- Employees and internal and external collaborators must follow a “clean desks” policy, i.e.:
    - Avoid leaving information carriers on desks or shelves at the end of the working day or during a long absence.
    - No information carriers should be stored in public areas.
    - Information carriers shall not be left in meeting rooms, and flip charts and whiteboards/blackboards or similar shall be erased when leaving the room.
    - Rooms where information carriers are stored must be locked at the end of the working day or during a long absence.

With respect to digital storage, in those cases where the information carrier is removable and contains information categorized as “Restricted” or “Confidential”, the data stored on it must be encrypted.

Secure erasure

Employees and internal and external collaborators must securely destroy unnecessary paper documents. In general, NH security bins for confidential information or NH paper shredder shall be used. It is expressly forbidden to dispose of information carriers in unprotected paper bins and to reuse paper documents that contain sensitive NH information.

Information carriers should also be destroyed or securely erased when it is no longer necessary to retain the information for commercial or legal reasons.

5.4. ACCES CONTROL

5.4.1. Business requirements for access control

Employees and internal and external collaborators must have access only to the NH information, information systems and IT services that is required for the proper execution of their functions and responsibilities in the NH Group.

Access permits should be granted as they are required, ensuring that employees and internal and external collaborators have access to data from IT systems and services necessary for the proper execution of their tasks and only for the period of time necessary to do so. In addition, access permits must always be assigned according to the principle of minimum privilege, i.e. everything that is not expressly allowed is forbidden.

5.4.2. User access management

Identification

By default, user accounts are nominative, i.e. there is a unique relationship between a user account and the person responsible for it. The use of generic accounts is prohibited. The creation of such accounts must be authorized by Information Security, and a record of such exceptions will be kept.

With regard to the development pattern of the user identifier, different patterns will be defined according to the types of users existing in the systems (e.g., hotel staff, external collaborators, IT & Systems staff, etc.) hence easing user administration tasks and reducing the probability of potential errors.

Privilege assignment

The assignment of privileges and permissions must be controlled and restricted. The following aspects must be taken into consideration:

- Principle of minimum privilege: users must be assigned a user profile corresponding to their job, which must contain the minimum privileges for the proper development of their functions and responsibilities. No user account should be created and no access privileges should be granted until the authorization process has been completed.
- Role-based access control: privileges must be assigned in accordance with the roles associated to the users' job position. The definition of roles must take into account the following aspects:
  - Granularity: it is possible to allow different levels of access.
  - Segregation of duties: it allows identifying and avoiding the simultaneous assignment of privileges to a user in order to reduce the risk of inappropriate use during the development of certain work tasks or areas of responsibility.

Registration, cancellation and modification of access permits

The People Department (Human Resources) of the NH Group is responsible for initiating the process of registering or cancelling access permits for internal employees. Similarly, it is responsible for initiating a process to change access permits for internal employees.

In the case of registrations, cancellations or modifications of access permits for external collaborators, the person responsible for initiating the process is the employee who is responsible for the supplier within the NH Group (i.e. NH internal staff).

When the processing of a request for registration, cancellation or modification of access permits is started, the identity of the applicant and his/her level of responsibility must be verified, so that it is ensured that the request is made by authorized personnel.

Once the initial application has been approved, the user management process consists of the following phases:

- Registration: the creation of the user in the corresponding repositories will preferably be carried out automatically, based on the information available in the authorization sources. When creating users with a known validity date (temporary contracts, external personnel, etc.) and provided that the system has such functionality, the automatic expiration date of the user should be established.
- Cancellation: Cancellation or blocking of the user in the application system. Similarly to registration, the cancellation will be carried out by means of automated processes, whenever possible. If it is foreseen that the reason for the cancellation may lead to a conflictive situation, the beginning of the request for the cancellation of the user account should be made prior to the formal communication to the employee, indicating its immediate effect.
- Modification: The modification of a user's privileges can be done in two different manners:
    - Modification of the roles assigned to a job position. By default, all the privilege modifications in the systems will be attempted maintaining the role model.
    - The specific assignment of privileges to that user.

All actions associated with the process of user management and privileges should be recorded in order to have a record of the requests answered and serve as support for future periodic reviews. In addition, Information Security will periodically coordinate the execution of reviews of the process of assigning users and privileges in NH's information systems and IT services.

5.4.3. Responsibilities

The access credentials generated by NH are the property of the NH Group.

Employees and internal and external collaborators must keep passwords and access codes confidential, even when requested by another employee or collaborator.

Access credentials are for the exclusive use of the employee or collaborator to whom they belong. When confidential information is involved, credentials must be stored according to the established categorization level. In addition, internal and external employees and collaborators must change passwords whenever it is probable (or it is suspected) that they have been revealed.

5.4.4. Access control to systems and applications

All NH information systems and IT services must prevent access to NH Group information if the user or process has not been previously identified and authenticated.

Authentication

In general, validation of user identity in NH information systems is performed by combining the user ID and password. To this end, the access control to information systems and IT services dealing with NH information must comply with the following aspects:

- Obligation to periodically change the password, access code or similar, and the possibility of changing it at any time by application users. In general, passwords should be changed every sixty (60) days maximum.
- Obligation to set complex passwords: minimum length, including different types of characters (uppercase, lowercase, numbers, special characters, etc.), restricted words, etc.
  In general, passwords must have a minimum length of six (6) characters, which must contain alphanumeric characters combining upper and lower case.
- User account blocking after five (5) failed access attempts.
- Restriction of setting the last used passwords.
  In general, the last three (3) previous passwords must be prevented from being used again.
- Obligation to randomly generate a first temporary password for access to the application and, after the first successful login, request its change.
- Delegate, as far as possible, the management of the authentication process in the corporate repositories of users of the NH Group, thus avoiding the use of repositories specific to each application.
- Do not store passwords in authentication repositories, source code or scripts.

For non-privileged user accounts employed in systems and services that process payment data (e.g., account numbers, bank card numbers, cardholder names, service codes, expiration dates, etc.), passwords must be at least seven (7) characters long and the last four (4) previous passwords must be prevented from being used again.

In the case of accounts with administration privileges and generic accounts, passwords must have a minimum length of twelve (12) characters and must be changed every thirty (30) days at maximum.

Any exception that involves the application of a less robust authentication policy than that defined above must be authorized by Information Security, and a record of such exceptions will be kept.

Secure login procedures

Access to NH information and information systems should be controlled through a secure login procedure. Such a procedure should ensure that passwords, access codes or similar are not displayed during the login process.

Depending on the risks and categorization levels of the information, two-factor authentication will be considered. This authentication method combines two of the following three factors:

- Knowledge factor: something the user **knows** (e.g., passwords, access codes, etc.)
- Ownership factor: something the user **has** (e.g., device, access card, etc.)
- Inherent factor: something the user **is** (e.g., fingerprint, iris, etc.)

For remote access outside the NH Group's internal networks to any information system or IT service where payment information is involved (e.g., account numbers, bank card numbers, cardholder names, service codes, expiration dates, etc.), as well as remote access to such systems and services for administration tasks, a two-factor authentication must be used.

Traceability

In information systems and IT services where NH information is processed, records (logs) that allow for the traceability of the actions carried out must be generated.

Information Security may collaborate in the definition of the requirements regarding the generation of records by the systems and services, as part of their collaboration in the development of the application's lifecycle.

However, the Project Manager must indicate the following during the requirements definition stage:

- Transactions to be recorded.
- Storage time of the transactions recorded.
- Procedure for exploitation of the records: on request, in the event of suspicion of security incidents or periodically.
- Additional requirements imposed by specific regulatory requirements (e.g., PCI DSS, laws and regulations on personal data protection, etc.).

5.5. CRYPTOGRAPHY

5.5.1. Implementation and use of cryptography

Cryptographic methods

The decision on the use of cryptographic methods has to be based on the classification levels of the information.

With reference to the encryption of information, the following aspects should be taken into account:

- The information categorized as Confidential should always be encrypted in order to store it.
- Transfers of information categorized as Restricted or Confidential to DMZs or public networks (e.g., Internet) should be encrypted.
- The Information categorized as Confidential that contains means of payment (e.g., account numbers, bank card numbers, cardholder names, service codes, expiration dates, etc.) should also be encrypted in communications between information systems in NH's internal networks.

Selection of cryptographic methods

Only cryptographic methods whose security and strength have been previously assessed by experts should be used. Mainly, best practices with regard to the cryptographic algorithm and the length of the key should be taken into account.

Only cryptographic methods that are documented and accessible to the public should be used.

For all systems and applications supporting means of payment, no weak cryptographic algorithm or protocol should be used.

To ensure robust protection, different cryptographic methods can be applied:

- Confidentiality:
  - Symmetric cryptography (e.g., AES)
  - Asymmetric cryptography (e.g., RSA)
  - Hybrid cryptography (e.g., RSA together with AES)
- Integrity:
  - Hash Algorithms (e.g., SHA-2) together with asymmetric signatures (e.g., RSA)
  - Message Authentication Codes (MAC)
- Non-repudiation:
  - Passwords
  - One Time Passwords (OTP)
  - Asymmetric signatures
  - Biometric methods (e.g., fingerprints, iris recognition)

Cryptographic methods can also be used at different layers of the OSI model:

- Level 3: Network layer (IPSEC)
- Level 6: Presentation layer (TLS)
- Level 7: Application layer (S/MIME)

Secure algorithms and protocols are listed below:

- Symmetric encryption algorithms:
  - AES (with minimum key length of) 256 (bits)
  - Triple DES 168
  - RC5 256
  - RC6 256
  - Twofish 256
  - IDEA 128
- Hash algorithms:
  - SHA-2 256
  - SHA-2 512
  - Whirlpool 512
- Asymmetric encryption algorithms:
  - RSA 4096
  - Ed25519
- Cryptographic protocols:

  - TLSv1.2
  - WPA2
  - SSHv2
  - L2TP/IPsec

A cryptographic product is a product that implements cryptographic methods. Prior to the acquisition of a cryptographic product, the following criteria must be taken into account:

- The product must have been certified (e.g., according to FIPS requirements) by an independent expert.
- Cryptographic products must be characterized by their ease of use in order to avoid errors during the administration and use of the product.
- It must be decided whether cryptographic measures are implemented at the hardware, firmware or software level. This decision should be made by Information Security.
- European products should be selected in preference to products from foreign manufacturers

Availability and compatibility

When using cryptographic methods, it is important to ensure the availability of the service, especially when the use of strong cryptographic algorithms may cause compatibility problems in the systems.

When using cryptographic methods, it must be verified that the products are compatible with most of the standards, and that the migration to another product or another provider does not imply great efforts or complications.

Therefore, it is important to migrate to strong cryptographic algorithms in testing environments before its implementation in the production.

Profitability

In addition to the costs of implementing cryptographic methods (product licenses, implementation and integration costs), operating costs must be taken into account:

- Training courses
- Technical support
- Maintenance
- Additional resources (e.g., CPU)

Influence of other safety mechanisms

Data encryption and the establishment of encrypted channels can have a negative effect on security, e.g. protection against malware. For this reason, it is necessary to involve Information Security in order to perform a risk assessment and, if necessary, implement compensatory controls. For example:

- Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) cannot detect patterns in encrypted traffic. For this reason, TLS traffic inspection modules should be used.
- Web content filtering systems must be able to inspect encrypted traffic.

Decryption keys should not be associated with user accounts. These must be accessible to the least number of necessary custodians. Also, an encryption period associated with each key should be defined, and they should be destroyed when they are no longer needed.

Use of cryptographic products

Employees and internal and external collaborators who operate or implement cryptographic products should receive specialized training on how to manage the product. These employees should know the use and benefits of different cryptographic methods and have an overview of the basic concepts of cryptography.

If a security incident related to a cryptographic product occurs, Information Security must be informed immediately. Therefore, it is important that operators and implementers know the procedures for managing security incidents.

Cryptographic products should be configured as securely as possible, preventing a user from easily circumventing security measures.

5.5.2. Key management

The administration, transmission, storage and updating of cryptographic keys should be carried out in a secure manner, in accordance with the following principles:

- Encryption solutions must generate strong keys.
- Encryption solutions must distribute keys securely, i.e., they are only delivered to identified custodians and are never distributed in clear text.
- Cryptographic key custodians must formally declare that they have understood and accept their responsibilities as key custodians.
- Encryption solutions should be stored securely (e.g., encrypting keys with applicable key encryption keys).
- An encryption period should be defined for each type of key, based on the underlying algorithm, key size and length, key risk hazard, and the confidentiality of the encrypted data. At the end of this period, the keys must be changed.
- Encryption solutions should provide a process for key replacement.
- Keys that are no longer used or needed, or those suspected of being compromised, should be securely removed or destroyed.
- Split knowledge and double key control should be used in manual key management operations.
- Encryption solutions should not allow the substitution of keys by unauthorized sources.

5.5.3. Management of certificates

The administration of electronic certificates must be carried out in a secure manner, in compliance with with the following aspects:

- The certificate validation process must confirm that certificates are neither revoked nor expired. Likewise, the process must also confirm that a trusted Certification Authority (CA) signs it.
- The implementation and use of an internal CA must be approved by Information Security.

- If there is a need to use external certificates in information systems, IT services or for users, Information Security must be notified of this need.
- Certificates issued by external CA should not be installed in workstations of internal and external employees and collaborators.

5.6. PHYSICAL AND ENVIRONMENTAL SECURITY

5.6.1. Secure areas

Typologies of areas

NH has implemented a series of mechanisms to guarantee the security of the facilities in which its information is located and/or treated.

When considering the measure of physical security to be implemented, three types of locations may be considered:

- Public areas: Include those rooms, offices or similar that are freely accessible to NH customers. These areas are mainly located in NH Group hotels.

- Work area: Include those rooms, offices or similar, regardless of their location, in which NH Group information is stored or guarded and that are exclusively accessible to employees and internal and external collaborators of NH. Hotel offices, documentation files and offices where NH Group employees are located should be classified as work areas.

- Technical areas: Include those rooms where computer and communications equipment is located, excluding workstations. These are the locations where data processing centres; communications rooms, etc. are located. These areas must be exclusively accessible to previously authorized employees and internal and external collaborators of NH.

It should be noted that these areas may be located in the NH Group's own facilities or in third party facilities where certain services have been outsourced. In any case, regardless of the location, security measures equivalent to those detailed in the NH Security Policy must be applied, as well as the regulatory standards that emerges from it.

Security measures

NH has implemented different physical security measures depending on the type of locations from which information assets are processed, depending on the level of risk of each type. This is determined on the basis of the following variables:

- Information assets located or treated, assessing the impact of their loss or damage.
- Level of exposure to potential threats, according to the level of accessibility to the site, its isolation from other areas of the facility or from the outside, frequency of access by external collaborators, etc.

The physical security mechanisms implemented in each of the locations can be classified into the following categories:

- Physical access control, corresponding to the measures established to prevent and detect unauthorised access.
- Volumetric detection systems.
- Closed-circuit television (CCTV) systems.
- Physical surveillance, using security guards.
- Environmental security, which includes environmental protection mechanisms and external and environmental threats.

Operations is responsible for defining the protection measures to be applied in public, work and technical areas.

Public areas

In public areas, the necessary and proportional security measures must be implemented to guarantee physical access control to equipment, devices and media that contain NH information.

Employees and internal and external collaborators must adequately guard all media containing NH information under their responsibility, especially in the public areas of the NH Group facilities.

Work areas

Security measures must be implemented in work areas to prevent unauthorized access to equipment, devices, supports and NH internal networks. Among others, the following security measures must be implemented:

- Mechanisms for identifying NH employees and internal and external collaborators (e.g., access cards, biometric sensors, etc.).
- Identification mechanisms used by visitors, which must be able to clearly differentiate between internal and external NH employees and collaborators.
- Periodical review of physical access permissions.
- Mechanisms that limit physical access (e.g., locked doors, code control, access card readers, biometric controls, etc.).
- Use of secure storage devices (e.g., locked cabinets for storage of documentation and media, etc.).

For work areas that, for any reason, present specific risks, additional safety measures may be considered. In this sense, the use of the following measures is contemplated:

- Implementation of video-surveillance systems. In general, the recordings of these systems must be stored for less than thirty-one (31) days, unless another law or regulation in force provides for a shorter retention period.
- Installation of doors with electric locks.
- Volumetric sensors.
- Security guards.

Technical areas

Related to technical areas, two types of installations are distinguished:

- Data Processing Centre (DPC).
- Reduced system and communications infrastructure rooms (e.g., communications cabinets, communications room, server rooms, etc.).

In relation to DPCs:

- Mechanisms for identifying NH employees and internal and external collaborators (e.g., access cards, biometric sensors, etc.)
- Identification mechanisms used by visitors, which must be able to clearly differentiate between internal and external NH employees and collaborators.
- Procedures in order to assure that visits are accompanied at all times.
- Periodical review of physical access permissions.
- Implementation of logging of access attempts (both authorized and denied).
- Mechanisms that limit physical access (e.g., locked doors, code control, access card readers, biometric controls, etc.).
- Use of specific secure storage devices for servers and communications devices (e.g., Key RACK)
- Implementation of protections or devices to alleviate the lack of electricity supply (e.g., UPS, generators, etc.).
- Implementation of emergency lighting systems in the event of a complete failure of the electricity supply.
- Implementation of video-surveillance systems that record uninterruptedly 24 hours a day. In general, the recordings of these systems must be stored for less than thirty-one (31) days, unless another law or regulation in force provides for a shorter retention period.
- Volumetric sensors.
- Security guards.
- Implementation of fire-fighting systems, in accordance with the laws and regulations in force.
- Environmental measures to ensure the proper functioning and condition of equipment, devices and supports.
- System for monitoring environmental conditions, such as minimum temperature and humidity.
- Energy efficiency measures.

As for rooms with reduced systems and communications infrastructure, mechanisms must be in place to limit physical access to them (e.g., use of lockable doors, locked cabinets, code control, etc.) and the environmental measures necessary to ensure the proper functioning and condition of equipment, devices and media.

5.6.2. Equipment security

Location and protection

In public areas, employees and internal and external collaborators should not place the equipment within the reach of third parties, such as customers or visitors, in order to avoid theft or manipulation. Special care must be taken to ensure that equipment connectors, where USB sticks can be connected, are not located within the reach of third parties.

Equipment and devices that handle or contain NH information, whether it is computer or paper documentation, must be stored in work areas or technical areas, which can only be accessed by duly authorized personnel.

Equipment and devices must be protected against any problems that may cause failures in support utilities (e.g., power supply or ventilation failures). For proper management of support utilities, the following measures is contemplated:

- Comply with the specifications of the equipment manufacturer.
- Monitor malfunctions.
- Tener redundancia de enlaces eléctricos.
- Have electrical redundancy.
- Communications equipment must be connected to at least two communications links from different suppliers.
- Ensure water supply that supplies air conditioning systems.

Besides this, support utilities should be inspected periodically to ensure proper operation and reduce the risk of failure.

Wiring security

Communications and power cabling must be protected to prevent possible data loss, interception or damage. The following requirements should be considered:

- Telecommunications and electric power lines must be physically protected (e.g., with pipes, canals, etc.) or installed underground.
- Redundancies of connections, both electrical and telecommunications, must not share the same location or access conduit to the building.
- Electrical wiring must be separated from telecommunications cables to avoid interference and possible damage.
  Wiring must be correctly identified and labelled to avoid errors in handling it.

Maintenance

The maintenance of equipment and devices must be carried out in a proper way in order to avoid possible failures and thus guarantee their availability. The following requirements must be considered:

- Only authorized internal and external employees and collaborators should carry out maintenance and inspection tasks on the equipment.
- If equipment is removed due to a fault, it must be replaced as soon as possible in order to continue the development of the NH Group's business processes.
- Maintenance tasks must be carried out according to the specifications recommended by the manufacturers.

Withdrawal of equipment

Equipment, devices, software, or other information assets should not be removed without prior authorization. To prevent withdrawal of equipment without authorization, the following requirements should be considered:

- Employees and internal and external collaborators who are authorized to remove equipment must be clearly identified.
- It must be recorded when an information asset is removed and when it is returned to its place of origin.

Before reusing or removing equipment, all information contained in the equipment must have been destroyed or erased, using techniques that prevent retrieval of the information, rather than using standard erasure options that do not overwrite the memory.

5.7. SECURITY OF OPERATIONS

5.7.1. Operational procedures and responsibilities

Documentation of operational procedures

The procedures related to the operation and administration of the information systems are formalized and available to all those users who need them to carry out their job functions.

Change management

Operational change is defined as those changes made to systems, services, equipment or procedures that affect NH facilities and information systems and IT services in production environments.

During change management, the following principles should be established:

- Identify NH information systems that may be directly or indirectly impacted by change.
- Evaluate the impact that the implementation of the change may have on a possible loss of integrity, confidentiality or availability of the information.
- Perform a risk analysis to identify and manage the risks associated with the change.
- Develop a return plan (roll-back) that allows to recover the state prior to the implementation of the change.

Prior to the implementation of changes in production environments, the effectiveness of the changes applied in a controlled testing environment must be tested, verifying its correct implementation.

All changes affecting systems, applications and data in the NH production environment must be approved and authorised in advance by a Change Committee. Also, operational changes must be identified and recorded, with the record available for review if necessary. This record should include the scope of the changes, systems affected by the implementation of the change, failures and recovery processes.

Capacity management

The capacity management process allows planning the dimension of technological and human resources needed to manage business needs. The capacities of the technological and human resources must be continuously monitored in order to carry out an adequate dimensioning and anticipate possible future saturations.

For that purpose, key indicators (e.g., CPU utilization statistics, memory, disk space, etc.) should be established to track the technological resources of the NH Group. These indicators should make it possible to continuously monitor NH resources and information systems and analyze the causes that may provoque an excess or defect of the capacity initially planned, with the aim of adapting them and guaranteeing the established requirements.

It is also necessary to identify the most critical systems for the business, which will be the most priority in order to determine the immediate actions to ensure the correct dimensioning of resources based on the needs of the NH Group.

Separation of development, testing and operational resources

Productive and non-productive environments must remain separate to reduce the risks of access or unauthorized changes in the operational environment. This separation of environments is important for the NH Group's business, due to the additional security control it contains.

In order to stablish an adequate segregation of functions during the development life cycle of an application or system, the environments are classified into the following typologies:

- Non-productive environments:
  - Development environment: oriented to the personnel in charge of the development of the programming of their projects. Developments take place in this controlled environment, which does not affect NH's normal work. Work must be done with a modified sample of data, as well as with programs and processes that are copies of the production ones, where the programmer cannot alter the information of that environment and the changes in it do not have consequences.
  - Test environment: optional environment created according to the needs of the project. In this environment, tests are carried out to verify the correct functioning of the functionalities implemented in the development environment. The analyst or programmer, who must return to the development environment if he has to make new changes to the processes, cannot modify this environment.
  - Integration environment: optional environment where system tests, stress tests, integration tests, user tests, etc. are carried out. This environment must simulate the productive environments, so that the tests carried out in it are as truthful as possible. Likewise, in this environment the interaction with other applications or systems can be verified. The analyst or programmer, who must return to the development environment if he has to make new changes to the processes, cannot modify this environment. In this environment the analyst of programmer works with a sample of information more complete than in the previous environments.
- Productive environments: in these environments the real NH processes are executed. These are environments where there is no room for testing of any kind, as any error can have serious consequences for NH of immediate result. Any activity performed on them should be properly recorded and reviewed periodically.

5.7.2. Protection against malicious software (malware)

Any NH information system is potentially vulnerable to malicious software (malware). The consequences of an infection on NH information systems can be serious and directly affect the business. For this reason, these information systems must be protected to prevent, detect and respond to these types of threats.

Preventive measures

NH employees and internal and external collaborators should participate in training and awareness programs for the identification and methods of action against malware. It is the responsibility of Information Security to carry out such awareness programs.

Technical solutions (antivirus, anti-malware) must be implemented on NH equipment, devices and information systems. In order to do this, the following aspects must be taken into account:

- NH information systems must have an anti-malware solution installed, especially those that are affected by malicious software (e.g., end user posts, servers, etc.).
- The anti-malware solutions must be able to detect and remove all known types of malware.
- Anti-malware solutions must be updated to their latest version and run periodic scans. Updates must be installed in a test environment before being distributed in the production environment.
- The configuration of anti-malware solutions must be properly protected. You must ensure that NH employees and internal and external collaborators cannot deactivate or modify the anti-malware solution without prior authorization from Information Security to justify it.
- Any NH information system in which an anti-malware solution is not installed must be documented and justified. Such exceptions must be authorized by Information Security.
- NH information systems within the payment environment (e.g., account numbers, bank card numbers, cardholder names, service codes, expiration dates, etc.) should be evaluated periodically to identify and evaluate potential malware threats.

Detection measures

Detection measures should be implemented to identify malicious code that may affect NH information systems. Among these measures, the following stand out:

- Periodic scans should be run on all NH information systems. These scans will be more stringent on business-critical information systems.
- Antivirus alerts should be monitored and logged.
- Any unsigned updates that should be applied to NH information systems should be inspected to ensure that they do not contain malicious code.

Response measures

If a malware infection is detected in an NH information system, it should be catalogued as a security incident. In this case, Information Security should act quickly to secure the infected system and prevent the spread of malware to other information systems by quarantining these infected systems.

Employees and internal and external collaborators should notify Information Security of the detection or identification of malware in an NH information system as quickly and efficiently as possible.

5.7.3. Backups

In order to enable the retrieval of NH information systems and the information contained therein, backups should be made, specially of systems that handle information owned by or under the responsibility of NH. To this end, the necessary guidelines should be established for the making, protection, verification and recovery of the backup copies.

Making backups

The following considerations should be taken into account when making backups:

- The extent and frequency of the backup should be defined by the information system administrator, based on the classification of the information stored in the information system. Similarly, it is necessary to define the required retention time in accordance with the legal and contractual requirements to which you are subject.
- Guidelines should be defined for the description of how backups should be made based on the information systems from which the copy is made.
- The execution of the backups should be monitored in order to detect possible failures during their execution.
- Whenever possible, backups should be made outside working hours so there is no interruption in the service.

Backup protection

Backups must be properly protected. To this end, the following measures must be implemented:

- Backups must be stored in a location other than the location of the associated information systems. The distance between the two locations should be sufficient in order to prevent a disaster that may affect the main location from also affecting the location where the backups are stored.
- Access to backups should be controlled, allowing only authorized personnel the access to them.
- An inventory of the backups should be maintained in order to identify the backups.
- Information that is stored in encrypted form should remain encrypted in the backups.

Verification of backup copies

Backup recovery tests should be conducted periodically so that the following can be verified:

- The effectiveness of the mechanisms for making and protecting backups.
- Level of updating of the procedures used for managing backups.
- Proper operation of NH's information systems once they are recovered.

In particular, on a semi-annual basis backup restoration tests should be performed on those NH information systems that process personal data. These tests must be documented by identifying the date of the test, the person responsible for carrying it out, the information recovered, the path of the recovered file, the file to which the information belongs and the result of the test.

Backup Recovery

In order to carry out the backup recovery process, guidelines should be established that include the steps to be followed to recover the required information. For the recovery of such information, the following information must be documented:

- Person requesting the recovery.
- Responsible for approving the recovery.
- Which NH information and information systems recovery is requested.
- Responsible for executing recovery tasks.
- Justification for requesting information retrieval.

5.7.4. Records and monitoring

Information systems or IT services dealing with information owned by or under the responsibility of NH classified as Restricted or Confidential must generate records to allow their follow-up and ensure their proper functioning. In general, the following categories of events are established:

- General events:
    - Users management: authorized and unauthorized access by users, password changes, user profiles and privileges, login, use of administration accounts, access at atypical times.
    - Systems management: changes in policies, use of administration programs, system shutdown and startup, operating errors.
    - Network management: access to communications networks (authorized and unauthorized), policy changes.
    - Incident management: alerts for intrusion prevention, maintenance of the life cycle of incidents (open incidents, created, solved), operating system vulnerabilities.
    - Antivirus: antivirus instances disabled, registration of infected information systems.
- Specific events:
    - Firewalls: attempts to execute rules that are not allowed, modification of the policy, traffic allowed in systems that store confidential information, access and disconnection of the firewall administrator user.
    - VPNs: authorized access and unauthorized access attempts, VPN access configuration changes, users blocking.
    - Internet access: attempts of unauthorized connections, access outside working hours, downloads of files larger than 10MB.
    - Email: mailbox at 90% of capacity, identification of known viruses, origin and destination of emails with suspicious attachments or that exceed the maximum size of the messages.

Records (*logs*)

NH information systems must generate minimum records. These records should generally contain the following information:

- IP address or name of the information system that generated the event.
- Identifier of the user or process.
- Date and time.
- Type of event.
- Description or reason for the registered event.

If it corresponds to an access event, the following information must be registered:

- Resource accessed.
- Type of access (read, write, delete).
- Whether access has been authorized or denied.

In particular, those records that affect the payment card data environment must record the following information:

- Actions performed by administrator users.
- Access to system logs.
- Invalid logical access attempts.
- Changes of user permissions and passwords.
- Access to card data.
- Creation or withdrawal of objects from the environment.
- Remote accesses.
- Changes in system logs.

Storage and retention of records

The storage of records (logs) is necessary for future investigations if required, always respecting the legal conformities that may exist around the privacy and conservation of information.

To this end, the retention period for such records should be defined. In general, the period of retention of records will depend on the information contained and the level of criticality of the information, adapting to the legal conformities to which they are subject.

In particular, those records associated with the payment card data environment should be kept with a minimum of one (1) year, being the first three (3) months of immediate availability for analysis.

Protection of records

Logs should be protected and distributed as securely and appropriately as possible. The following aspects should be taken into account:

- Records should be protected from unauthorized access.
- Access rights to records should be granted on a need-to-know basis.

- Systems involved in the processing of records should be physically located in secure areas and adapted for this purpose.
- Transfers of records should be protected by mechanisms to ensure the integrity of the records.
- Transfers of records on public networks should be encrypted.

Clock synchronization

All NH Group information systems and IT services that have a log record must have the exact and synchronized date and time for the event logs to be correct and consistent with each other.

To this end, reliable external time sources must be used for the synchronization of timeservers, which are used for the synchronization of internal systems.

In order to avoid unauthorized modifications to the configuration of information system clocks, only authorized personnel should have access to the configuration of clock synchronization systems.

Under no circumstances should employees or internal and external collaborators modify the clocks of information systems owned by NH.

It should be periodically checked that the information systems have the correct time. Special consideration should be given to changes in time stations and changes resulting from software updates or configuration changes.

5.7.5. Management of technical vulnerability

NH should establish a process to identify security vulnerabilities in NH-owned IT systems. All vulnerabilities must be classified according to the criticality and level of affectation in those systems.

Vulnerability scan and intrusion test

Periodic scans and vulnerability analyses should be performed on NH's information systems and IT services, especially those that are critical to the NH Group. Such analyses must be authorised by NH Management and must be carried out by qualified personnel. The periodicity of the scans will depend on the criticality of the information systems to be analysed.

As a general rule, vulnerability scans should not be performed on NH information systems during working hours, as this could lead to loss of availability of the systems.

In particular, the information systems within the scope of PCI-DSS, should run quarterly periodic scans using specific tools and approved for it (ASV). Also, intrusion tests on these systems should be run annually or after a significant change in infrastructure has been implemented.

Vulnerability mitigation

Vulnerability scans and intrusion tests should generate reports that gather information associated with each vulnerability found, with the aim of identifying and mitigating that vulnerability. The following information must be compiled:

- Affected information system.
- Description of the vulnerability.
- Impact of vulnerability.
- Service affected.
- Level of criticality of the vulnerability.
- Recommendation

Information Security is responsible for ensuring that these vulnerabilities are corrected according to the level of criticality.

Patch management

Information Security must be subscribed to security newsletters in order to be aware of the latest security patches published by the software and hardware manufacturers of the NH Technology Platform. These patches must be analysed and installed in the different NH information systems in order to keep them updated.

The changes applied for the correction of the identified vulnerabilities must be approved and verified after their implementation, guaranteeing the correct solution adopted for the correction of the vulnerabilities.

Exception management

It may be the case that it is not possible to correct an identified vulnerability, either because there is no known countermeasure or because the countermeasure affects the availability of the information system. In this case, security measures must be implemented to mitigate the risk of emergence of this vulnerability, for example:

- Increase the monitoring of the identified information system.
- Disable characteristics of the service that are not necessary and are related to the identified vulnerability.
- Installation of utilities that help mitigate the risk of emergence of the vulnerability.

These exceptions must be inventoried, reviewed and approved by Information Security.

5.8. COMMUNICATIONS SECURITY

5.8.1. Network security management

Segmentation

The NH Group has defined, as a general principle for the secure design of its internal communications networks, the segmentation criterion according to which:

- Different types of networks are defined from a security point of view, depending on variables such as the functionality offered by the systems located in the network, the users of these systems and the type of information exchanged, the level of exposure, etc.
- The level of visibility between the different networks is limited to what is strictly necessary.
- Connections between networks of different nature are made through appropriate filtering devices and are monitored by Intrusion Detection System (IDS).

According to the previous criteria, NH has defined the following network typologies:

- DMZ Networks: offering services accessible from public networks. The services located in this type of network are those that must be visible from the Internet, or must be directly connected to the Internet, such as web portals, web browsing proxies, mail gateways, remote access for employees and collaborators, etc.
- Production networks: in which are located, in an isolated way, the servers that house the business logic of the applications and their information assets, common infrastructure such as LDAP servers, as well as the interconnection networks with third parties.
- Development and quality networks: in which are located the systems that integrate the different non-productive environments used in the Software Development Life Cycle.
- Hotel and office networks: which allows access to NH's information systems to employees and internal and external collaborators through their equipment and devices.
- Management networks: oriented towards systems that allow remote monitoring and administration of communication elements and servers that support NH's technological infrastructure.

The general safety requirements defined by NH for the network types described above are as follows:

- Communications devices (e.g., switches, Wi-Fi access points, etc.) and security devices and systems (firewalls, IDS/IPS, etc.) are configured prior to installation.
- Changes to NH's internal networks at the design and/or configuration level (e.g., installation of new servers, installation of communications devices, modification of filtering rules, etc.) must be notified in advance to Information Security for information security risk management.
- Mechanisms have been defined to prevent the disclosure of private IP addresses, information about internal network routing, and information about devices to the Internet.
- The components of all NH networks, with the exception of those located in the public part of the DMZ networks, use private addressing and unique local addresses.

DMZ Networks

Services located in DMZ networks are divided into the following groups according to their typology:

- Public services: services offered by NH for access through public access networks.
- Remote access: remote access to the NH Group's information systems located in internal networks by workers and/or suppliers.

NH considers these networks to be high-risk, given their high level of exposure to potential attackers. For this reason, the NH Group has applied the principle of defence in depth in the design of the security architecture of these networks and has defined a filtering system based on a double layer of firewalls.

In the case of remote access to NH's information systems by employees and internal and external collaborators, the following security measures have been established:

- Connection through VPN tunnels. Two-factor authentication policy (username and password together with a software generated token or hardware device).
- The level of user privileges (accessible subnets, Internet browsing, etc.) is managed through groups. These privileges are limited to the minimum necessary, according to the criterion of minimum privilege.
- Prohibition to use "split tunnelling" in the client equipment, so that only the fixed network security requirements are applied in such equipment.
- Automatic disconnection after a period of inactivity of 60 minutes of the user.

Production networks

In production networks, there are two different typologies:

- Information system networks: in which are located the servers that house the business logic of the applications, their information assets and the common infrastructure (LDAP servers, etc.).
- Means of payment networks: in which the NH information systems that support operations are located within the scope of PCI-DSS.

Information system networks

Within the networks of information systems, different networks are defined depending on the level of sensitivity of the systems located in them.

These networks are always isolated from the rest of NH networks by a filtering element, at two levels:

- The connectivity between the different types of networks is restricted by default. Only the strictly necessary connections are allowed in those cases where an application has to communicate with a system located in a different type of network.
- In each of the network types, connectivity within the network is restricted by defining subnets. Visibility between the defined sub-networks is limited to what is strictly necessary for the correct functioning of the systems and services.

Means of payment networks

Means of payment networks are those in which the devices from which payment media transactions are processed are located, as well as the servers through which the information associated with these means of payment travels (e.g., account numbers, bank card numbers, cardholder names, service codes, expiration dates, etc.). These networks are subject to PCI-DSS compliance. In order to limit the effort associated with compliance with said regulations, an attempt will be made to maintain a high level of isolation of this type of devices and servers with respect to the rest of NH networks.

The diagram of the means of payment networks must allow the identification and location of the elements and systems.

Periodically, Information Security must evaluate the level of isolation applied to these networks, as well as the security measures applied to the connections maintained from/to these networks from the rest of the internal networks of the NH Group.

Development and quality networks

Development networks contain systems located in non-productive environments. Security considerations are as follows:

- By default, connectivity to this environment is restricted and access has to be previously authorized.
- The connection between production and development environments is expressly prohibited.
- The only connections allowed between environments of these networks are those necessary to generate test, and those connections that are established for the promotion of software.

Hotel and office networks

These networks include user devices used directly by NH employees and internal and external collaborators, as well as office servers. User networks implement the first control point in access to NH's information assets and, therefore, access to these networks must implement the following security measures:

- Network access ports located in public locations accessible by non-HN personnel should be restricted. By default, access to the network through these ports should be restricted and only be enabled when strictly necessary. In any case, control of user access to the network is done through protocols that transmit user credentials in encrypted form through the network.
- Different subnets must be defined to restrict the visibility of the systems located on these networks (e.g., office automation users, office automation servers, guests, PCs managed by external collaborators).

The exposure of wireless networks (Wi-Fi) makes them one of the weakest links in network security. For this reason, the following requirements must be taken into account:

- The installation of wireless networks is prohibited without prior authorization from Information Security. Information Security will be able to carry out revisions in order to identify and detect unauthorized Wi-Fi access points.
- Secure protection systems (WPA2) must be used and wireless networks cannot be created without protection or using protection mechanisms considered insecure (e.g., WEP, WPA).
- The guest network is completely segregated from NH's internal network and only provides access to the Internet access service, independent of the one used by NH employees.
- The use of the guest network by NH employees and collaborators through equipment that connects to NH's internal networks is prohibited.
- Accounts provided for access to the guest network must have a defined expiration period.
- If captive portals are used for user authentication, it must be ensured that the passwords used in such portals comply with NH's password policy.
- The use of self-signed certificates in captive portals for user authentication in guest networks should be avoided.

Management networks

Traffic with origin and/or destination in/to a management network must travel isolated from data traffic through dedicated networks for that administration traffic.

Due to the sensitivity of the actions performed on the management networks, especially in terms of administration, the following additional security measures have been defined:

- The connection of a user to a management network must be previously authorised by Information Security and must be carried out through a hopping system, which must be subject to a special monitoring level.
- Subnets must be defined for the administration of particularly sensitive systems and platforms (e.g., means of payment networks).
- Visibility between the different sub-networks that make up the management networks is restricted.
- User authentication credentials are transmitted encrypted within these networks and on connections established with elements of other internal NH networks.

5.8.2. Information exchange

Authorization

In general, the exchange of information owned by or under the responsibility of NH with third parties outside the NH Group is prohibited.

When NH employees and internal and external collaborators identify the need to carry out an exchange of NH information with a third party outside the NH Group, they must request the authorisation of the owner of the information. It is the responsibility of the information owner to assess the need and, if turns out that the exchange is necessary, it is necessary to inform Information Security of that need.

Information Security will keep a record of the exchanges of information classified as Confidential identified, with the aim of including them periodically in its risk analysis.

Prior to initiating an exchange of NH information with third parties outside the NH Group, the owner of the information must guarantee that the exchange has been regulated in a contractual or legal agreement with the third parties, where at least the following aspects are developed:

- The conditions under the exchanges take place.
- The mechanisms defined to facilitate the management of these exchanges.
- The legal responsibilities and obligations of the parties when exchanges are carried out, especially those affected by regulatory requirements.
- Responsibilities for control and notification of the sending, transmission and receipt of information.
- The need to return and/or destroy the information exchanged once the contractual relationship has ended.
- Responsibilities in the event of security incidents.

The owner of the information must be in contact with Legal Affairs in order to ensure compliance with NH internal rules and applicable laws and regulations.

Exchange through public networks

The exchange of information through public networks should be carried out taking into account the following guidelines:

- In general, secure information exchange mechanisms provided by NH and authorized by Information Security (e.g., SFTP servers, NH collaborative tools, NH document managers, etc.) should be used.
- The exchange of information classified as Restricted or Confidential through channels that do not guarantee the security of the exchanges (e.g., unencrypted e-mail, public information exchange services, SMS, etc.) will be avoided. In cases where the exchange takes place through insecure channels, security tools that guarantee the confidentiality and integrity of the exchange and that comply with the cryptographic controls defined in the NH Security Policy, as well as the regulatory standards emanating from it, must be used.
- In situations where a NH employee or collaborator needs to use exchange systems managed by a third party through public networks, Information Security is responsible for performing a risk analysis of these exchange systems and, depending on the result, authorizing or denying its use.

Exchange systems

The information systems through which information exchanges take place offer the possibility of restricting the visibility of shared information only to authorized users, offering different levels of granularity (e.g., between internal employees, between employees of several Departments, between internal employees and external collaborators of several Departments, etc.).

It is the responsibility of the users to define and administer the permissions for access to the information by other users.

Security measures

The information systems through which information is exchanged must take into account the security considerations contained in the NH Security Policy, as well as in the normative standards that emanate from it; in particular:

- They must implement cryptographic information protection mechanisms.
- They must be configured according to the secure configuration guidelines authorized by NH.
- They must generate sufficient security events to allow proactive analysis and forensic investigation of possible security incidents.
- They should be incorporated into the vulnerability management process.

In general, information exchange systems will be considered as temporary repositories of information. In this way, it should be taken into account that:

- They should not be used as information storage services. Due to the level of exposure of this type of services, an attempt will be made to minimize the volume of information available in these systems.
- The information exchanged through these services, insofar as it is information in transit and copies of other original information, will not be protected by the backup policies of other systems.
- There will be periodic procedures of erasure of the information exchanged through these systems, in order to minimise the risk of information theft.

Physical exchange

With regard to exchanges of information that take place through means commonly used for the storage of information (optical media, removable storage devices, etc.), the following considerations should be taken into account:

- It will only be carried out through suppliers approved by NH and with whom a formalised agreement is maintained. In addition, a register of entry and exit of supports will be maintained.
- Packages used in transport must protect the contents of the sending from any physical damage during transport and from unauthorised access (e.g. sealed envelopes).
- Additional security measures will be established such as the encryption of the media included in the shipment.

5.9. ACQUISITION, DEVELOPMENT AND MAINTENANCE OF INFORMATION SYSTEMS

5.9.1. Security requirements for information systems

The incorporation of Information Security in the life cycle of the development of any computer project is intended to:

- Ensure that the security level of information assets is at all times aligned with NH's business and operational needs, through the continuous identification of potential risks and the correct application of the corresponding security measures.
- Minimize the cost of protecting information assets, trying to identify in the early stages of any IT project the security measures that must be implemented and the role that Information Security must play.

It is responsibility of the Project Manager to notify Information Security of the start of any IT project once it has been approved by any of the approval channels addressed in the NH Group.

For such projects, Information Security determines the level of involvement to be adopted in each of the stages of the project life cycle, based, among others, on the following variables:

- Whether it is the development of a totally new information system or the evolution of an existing one.
- Information assets affected by the development of the new project, from the point of view of:
  - The level of exposure of the information assets.

  - The applicable regulatory requirements (e.g., PCI-DSS, GDPR, etc.).
  - The magnitude and relative complexity of the project.

Information Security notifies the Project Manager of the need for his/her participation in the project work team, as well as the degree of involvement in each of the project phases. In any case, the Project Manager, at the beginning of the project and based on his/her greater knowledge of its scope, may require greater involvement of Information Security during the development of the project.

Definition of security requirements

For the formalization of security requirements, the following tasks should be performed during the Requirements Definition phase:

- Identify, depending on the information processed, whether the IT project to be developed is affected by regulatory requirements relating to information security. In particular, if personal data is processed, the necessary and proportional requirements must be identified to guarantee privacy by design and by default.
- Perform an analysis to identify the risks that, from an information security point of view, can introduce the changes associated with the development of the project. The risk analysis should consider not only purely technical but also functional risks, linked to the business operation itself and to the use of the information assets to be carried out by the users.
- Formalize the list of security requirements to be satisfied, which will be incorporated as part of the non-functional requirements of the project. The definition of security requirements will not only focus on the development of the project itself, but will also try to anticipate the requirements to be taken into account during the subsequent operation and maintenance of the project. In the event that any of the security requirements could lead to conflicts that block the development of the project, the Project Manager will require Information Security to carry out a formalised risk analysis, which will evaluate whether the associated risk is or is not acceptable and, where appropriate, determine the application of compensatory security measures.

Solution design

From a security point of view, in the Design phase, Information Security will be able to collaborate in the execution of the following tasks:

- To support and/or validate the design of the proposed solution, from the point of view of compliance with the defined security requirements.
- If the project requires it, collaborate in the design or selection of possible specific security solutions necessary to meet the defined security requirements.
- Define cases of abuse.
- Designing the security-testing plan.

With respect to the test plan, although the test plan will vary depending on the nature of the IT project, NH has established as a minimum requirement, for all projects affecting systems exposed to the Internet and/or affected by the PCI-DSS standard, the inclusion of security tests in the test plan.

The security tests will be conducted using a white box approach and are as follows:

- Revision of the source code, using static code analysis tools.
- Vulnerability scans and penetration tests, at both network and application level, prior to the production of the new solution.

Development and construction

During the development phase, the project development team should:

- Apply best practices in the construction of systems
    - When it comes to software development projects, ensuring that development teams know and apply safe programming guidelines.
    - When it comes to system projects, through the secure system configuration guides provided by the system manufacturers themselves.

    It is the responsibility of Information Security to facilitate and train IT & Systems regarding best practices in the development of secure systems.

- Run specific security tests, following a white box approach

It is the responsibility of the Project Manager to provide a necessary environment for the tests performed to simulate as far as possible the security configuration of the production environment (e.g., ports used by the application for its operation, files and/or folders to be excluded from antivirus scanning, etc.).

It is the responsibility of Information Security to approve the tools and procedures that support the execution of these tests and to review their proper execution.

Tests

Before going into production, safety tests must be performed in non-productive environments using a white box methodology. These tests identify possible security vulnerabilities present in the information systems affected by the changes made during the development of the project.

Systems for which serious security vulnerabilities have been identified during the development of the project may not be put into production without the express approval of Information Security or without an action plan proposed by the project team that allows these vulnerabilities to be corrected within a limited period of time.

Production readiness

Independently of its involvement during the development life cycle of the project, prior to the production of a new system or application, Information Security may require an audit of the project to verify compliance with each of the considerations previously made in this standard. As a result of this audit, Information Security may propose stopping the production of the new development or system.

Once the production of the new development or system is approved, the following steps must be taken:

- Update the necessary information to execute disaster recovery procedures.
- Update the information needed to execute the procedures for managing technical vulnerabilities.

5.9.2. Security in development and support processes

Security measures in non-productive environments

An adequate level of control must be maintained in those technological elements and infrastructure that support the development of systems. To this end, the following security measures, among others, must be established:

- There should be an adequate segregation between non-productive and productive environments in order to adequately isolate and characterize the different functions and activities during development.
- Development environments should be kept protected against:
  - Unauthorized configuration changes.
  - Unauthorized software installation.
  - Malicious code.
  - Unauthorized access.
- As far as possible, Internet access will be controlled from the development systems.
- A consistent policy of updates and patches should be applied to equipment in non-productive environments.
- Backup and recovery management procedures should be implemented, properly documented, and known to the development team members.
- A code control system or versions over the source code should be used, so that the changes made to the productive systems can be traced.

Software libraries must have an identified and assigned owner, who will define which users will have access to them and which users will have authorization to modify them. Likewise, they must establish an adequate version control and user management that allows:

- To identify all the libraries belonging to a system.
- To control the allowed accesses.
- To document the changes made.
- To delimit changes made between two source code versions.

Source code libraries will not be published in the production environment, except in cases where non-productive environments do not allow compiling source code. Libraries whose executable code is in production environments should not be modified directly, and should work on a copy of them.

Segregation of environments

Non-productive and productive environments must be separated with the purpose of achieving an adequate segregation of them, thus avoiding incidents in the elements of the production environment and guaranteeing the stability and integrity of the systems.

To this end, the following requirements shall be taken into account as far as possible:

- Segregation of environments:
  - Non-productive and productive environments must be differentiated and separated through the dedication of different infrastructures, located in different security segments.
  - The only communication allowed between non-productive and productive environments must be the one related to data transfer, systems and services from non-productive to productive environments.
  - It will be necessary to establish mechanisms that allow maintaining traceability of any activity carried out in the development process.
  - It will not be allowed, in the production environments, the installation of systems development tools, such as compilers, code editors, etc.
  - Under no circumstances will the activities associated with system testing carried out in the production environment.
  - Non-productive information systems should, as far as possible, display identification messages associated with the non-productive environment to which they belong, in order to reduce the risk of unintentional human errors during the activity of personnel.
- Segregation of dutties:
  - In general, profiles of users with development functions may not alter or modify in any way the code hosted in the production environment.
  - Developers will not be able to access the production environment to analyze anomalies and/or possible incidents, debug the operation of applications and services, or to carry out any activity related to the development function itself. They will only be able to access the production environment using an end user profile of the application.
  - In exceptional cases in which, due to force majeure, it is essential for personnel with development functions to have access to the production environments, this must be limited by a series of control measures. Among others, the permanent blocking of the user and unblocking during a reduced time of access and, in addition, it will have to be reviewed periodically and regularly.

If in any case it is not possible to guarantee the segregation of environments and/or functions, security mechanisms and controls will be defined to properly mitigate the risks derived from this situation. Among these controls, the following shall be implemented:

- Review of production steps.
- Alerts through monitoring tools.
- Disabling developer users and enabling change windows.

Steps to production

The production environment is the environment in which the NH Group operates. For this reason it is critical to adequately protect it, not only against access or attacks, but also against an inadequate change management process. Therefore, it is necessary to define a series of measures to control and limit the changes made to production systems. To this end, the following security measures are defined:

- Changes in production must be properly identified and controlled.
- There must be a log of all changes in production systems. To this end, and as far as possible, it is recommended to carry out the production steps using tools designed for this purpose.

Every step to production must be requested and, if positive, approved based on the result of the tests carried out, i.e. whether it meets the functional and safety requirements specified at the start of the production step.

- There shall be a version control over the version of the system installed in production.
- Application updates in production systems must be previously executed in a test environment.

5.9.3. Test data

In order to achieve a proper segregation of non-productive and productive environments, restrictions should be placed on copying and access to actual data from the production environment.

The following aspects should be taken into account:

- As far as possible, the transfer or copying of actual data from a production environment to a non-productive environment should be avoided. Tests carried out in non-productive environments should be carried out with datasets created for this purpose.
- If, for development reasons, it is imperative to test production data, the following security measures shall be taken into account:
    - The process of transferring or copying data should always be carried out following a formal procedure, even if it is done urgently.
    - As far as possible, dissociation or masking mechanisms will be applied to avoid identification.
    - If real data is used in a non-productive environment, it should be pseudo anonymised or anonymised prior to the transfer of these data to the non-productive environment.
    - Data transferred or copied from the production environment to any other environment should be deleted from the latter when they are no longer necessary or the reasons for the exception are no longer applicable.
    - In the case of personal data, and in order to ensure adequate compliance with laws and regulations on the protection of personal data, it must be ensured that the security measures implemented in the environment in which they are stored, processed or transmitted are equivalent to those required for production environments.
    - Under no circumstances data related to means of payment (account numbers, bank card numbers, cardholder names, service codes, expiry dates, etc.) will be processed in non-productive environments.

5.10. SUPPLIER RELATIONSHIP

5.10.1. Security in relations with suppliers

NH, for the correct provision of its services, may outsource such services by contracting a supplier, maintaining a contractual relationship between both parties. NH's approach to managing the relationship with its suppliers is based on the definition of a control framework that covers the entire life cycle of the relationship with these providers.

Contracting

The recruiter, an internal employee of NH, must complete an initial approval questionnaire to identify the controls applicable to the supplier's approval. Likewise, based on these responses, the risk will be evaluated by Information Security once the outsourcing is catalogued. In order to carry out this analysis, those responsible for contracting must inform Information Security of the start of any process of contracting a supplier.

Information Security is responsible for analysing the risks associated with outsourcing a service to a supplier. This risk analysis will include, among others, the following variables:

- Type of service provided.
- Information assets affected by the service.
- Way of working and access of the supplier, distinguishing between:
    - Service provided at the facilities of NH and/or at the facilities of the supplier.
    - Access to information through equipment owned and managed by NH vs. the supplier's own equipment.

Taking into consideration the conclusions of the preliminary risk analysis carried out by Information Security, it will be possible to determine, in each case, additional considerations from the point of view of the security of the information to be taken into account:

- During the supplier selection process, introducing new variables or requirements that from a security point of view will need to be evaluated, either in the form of a technical solvency requirement or as part of the bid evaluation criteria. For example, they may be considered:
    - The need to provide different information security certifications.
    - Security measures available to the provider for the provision of its services.
- During the contracting process, imposing security requirements and procedures, in addition to the minimum requirements established by NH for any contract, described later in this standard.

Contractual regulation of safety requirements will be one of the main ways in which NH manages its relationship with its suppliers. Therefore, in the process of contracting suppliers, the contracts that will govern the relationship must include the safety requirements that the supplier must guarantee in the provision of the service.

NH sets minimum safety requirements that must be contractually regulated in all agreements with service providers. These requirements are as follows:

- Acceptance and compliance by the provider of the NH Safety Policy and the guidelines included in the Security Regulatory Framework that apply to it. In cases where there is a conflict between the safety measures established by NH and the provider's own safety measures, those that are more restrictive will be established.
- Confidentiality agreement: all contracts regulating the relationship between a provider and NH will include a clause in which the provider undertakes to guarantee the confidentiality of NH information that may become known as a result of the provision of the service. This obligation will not only be in force during the period of the collaboration, but will be extended indefinitely after the end of the collaboration.

Likewise, the confidentiality clause will include a strict prohibition for the provider of access to all information that is not strictly necessary for the provision of the service.

- Clause associated with the protection of personal data: for suppliers that provide a service that involves the processing of personal data or the provision of this services implies a potential access to them, the contract includes the commitment to comply with applicable legislation and regulations by the provider.
  Likewise, it shall be established that non-compliance on the part of the supplier may be ground for termination of the contract by NH and/or a claim for damages caused to NH by non-compliance.
- Clause associated with the protection of means of payment: for suppliers that provide a service that involves the processing of actual data from means of payment (account numbers, bank card numbers, names of cardholders, service codes, expiration dates, etc.) or the provision of this services implies a potential access to them, the contract includes the commitment of compliance with the PCI-DSS in force on the part of the provider.
- Subcontracting: the supplier is obliged to notify NH of cases in which it will subcontract all or part of the service it provides to NH, if the contract specification does not explicitly prohibit the subcontracting of the service. The safety obligations contained in the contract shall apply equally to all subcontractors involved in the provision of the service.
- Notification of security incidents: the supplier shall have the obligation to communicate, as soon as possible, the occurrence of any security incident that affects or may have affected information owned by NH and that the service provider treats as a consequence of providing the service.
- Physical security: Suppliers working in NH facilities must comply with the physical security measures established by NH. Specifically, they will undertake to ensure that all their personnel use the security measures provided by NH to identify external personnel who use their facilities.
  In addition, the supplier must ensure that, at the end of the contract, the accreditations allowing its personnel access to NH facilities are returned for cancellation.
- Compliance Review: The service contract will expressly establish the provider's obligation to comply with the NH Security Policy and applicable legal regulations, and NH may supervise such compliance at the time and in the manner it deems appropriate.
- Return of information: the obligation on the part of the provider to destroy and/or return all NH information to which he may have had access as a result of providing the service will be reflected in the contract.
- User management for access to NH information systems: Providers requiring access to NH information systems must comply with the following guidelines:
  - Provide identification data of the work team for the proper management of user accounts in NH information systems.
  - Communicate any modification in the composition of the work team, so that NH can properly manage registrations and cancellations in its information systems.

The contractual regulation of the above safety requirements applies to all contracts and is the minimum required by NH.

Therefore, and without prejudice to the foregoing, Information Security may establish additional requirements based on the risk analysis described above.

Administration and monitoring

The daily management of the relationship with suppliers will be carried out, fundamentally, by the person responsible for the contract.

Thus, in order to ensure that the provision of the service complies with the information security requirements established by the NH, the person responsible for contracting out outsourced services should carry out the following tasks:

- Ensure that suppliers are aware of and comply with the NH Security Policy and the security measures applicable to it.
- Notify registrations, cancellations and modifications of user accounts used by the supplier's personnel and define access privileges, in order to guarantee that access privileges to information systems are kept up to date and are based on the principle of minimum privilege.

It is responsibility of Information Security to ensure compliance with the security requirements when contracting the service. This monitoring function will be based on the periodic review of compliance with the security requirements established in the contracting of the service, which may be articulated differently for each of them: validition of certifications, third party audit reports, ad-hoc reviews, etc.

The person responsible for hiring must approve the execution of any change in the provision of the service. Thus, the security impact of any changes made to the service provided must be jointly assessed by Information Security and the service provider before the change is made.

It is responsibility of Information Security to keep an up-to-date record of IT service providers, including their risk categorization and the result of the risk analysis performed.

Termination

The last stage defined in the management of the relationship with a service provider is the termination of the relationship between the service provider and NH. In order to manage the risks associated with the termination of the relationship, the following requirements are defined:

- All access privileges granted to the provider's staff should be revoked, taking into account:
  - Physical access: Through the return and cancellation of access cards, access codes, keys, etc.
  - Logical access: Through the revocation of user accounts used by the provider for access to different information systems, including permissions for remote access to NH systems.
- The destruction and/or return of information assets by the provider to NH, as well as physical assets (laptops, tokens for remote access, telephones, etc.) owned by NH, must be guaranteed.

The hiring manager must notify Information Security of the termination date of the contracts. Together, they must ensure compliance with the requirements provided above.

5.11. INFORMATION SECURITY INCIDENT MANAGEMENT

5.11.1. Information security incident management and improvements

Procedures and responsibilities

NH must define the procedures and responsibilities necessary for the proper management of information security incidents. To this end, there are the following types:

- NH internal and external employees and collaborators: should report any type of security incident or indication to Information Security as soon as possible.
- Resolution team: are responsible for executing the necessary actions to contain and resolve incidents. They must periodically report the status of treated incidents and collect the necessary evidence for further expert investigations.
- Legal Affairs & Compliance: should assess whether legal action is necessary.
- Information Security:
  - Analyse reported incidents and discard false positives.
  - Supervise the containment and incident resolution phase.
  - Escalate and report incidents to third parties.
  - Notify interested parties of all incidents involving a serious information security incident, such as those affecting personal data or the payment card data environment.

The NH information security incident management process covers all phases of the life cycle of a security incident, from detection to closure.

Detection

Types of incidents

The typology of security incidents is variable in nature, including, but not limited to, the following cases: denial of service; information leakage; internal logical attack; external logical attack; malware; illegal or illicit activity; loss of equipment; violations of NH Group internal policies; etc.

Incident identification

The identification of information security incidents can occur in two ways:

- External to Information Security: through employees, internal or external collaborators, clients, State Security Forces or third party organizations with which NH may maintain any type of relationship. Regardless of the origin of the incident, it is obligation of all employees and internal and external collaborators to notify Information Security of any security incident they detect as soon as possible. Information Security is responsible for:
  - Define and disseminate formal security incident reporting channels.
  - Train and make NH employees and internal and external collaborators aware of how to identify and report a safety incident.
- Internal to Information Security: based on the proactive surveillance of threats that can be carried out using security-monitoring tools. It is responsibility of Information Security to define the requirements regarding the generation of security logs to be generated in NH information systems and the tools necessary to manage these logs.

Incident evaluation

Once an incidence has been reported, the team responsible for the incidence should carry out a preliminary analysis of the incidence. In order to carry out this analysis, the team must gather as much information about the incidence as necessary. At least the following information should be collected:

- The exact date and time the incident was detected.
- Person who has detected the incident.
- People, systems, locations or information that have been compromised.
- Logs and other evidence needed to assess the nature of the incident.
- Team responsible for resolving the incident.

Based on this information, Information Security performs the following actions:

- Assess whether it is really an incident or if it is a false positive.
- Evaluate the potential impact of the incident, classify it as an incident and register it.
- Communicate incidents involving a serious information security incident to all affected parties. Likewise, the necessary mechanisms must be established to communicate to the corresponding authorities those incidents that affect the payment card data environment or personal information, among others.

Incident recording

All identified information security incidents should be recorded in a unique information repository, which allows:

- Keep a historical record of security incidents managed by the NH Group.
- Generate a minimum level of information on the actions carried out by NH during the management of each one of the incidents.

Resolution

Incident containment

The first step of incident management should be the containment of the incident, with the purpose of minimizing the potential impact that the incident may generate. The objective of this step is not to identify the root cause of the problem but to minimize its impact and prevent the incident from spreading and affecting new assets that were not initially affected.

Evidence collection

In order to enable the possibility of taking legal action, both criminal and civil, against a person or organization that has caused a security incident or, in the event that as a result of the incident payment data or personal data have been compromised, throughout the incident management process the collection of evidence showing the occurrence of the incident must be ensured. This compilation process must guarantee the validity of the evidence, by means of:

- The establishment of controls to guarantee the quality and integrity of evidence.
- Compliance with regulations or codes of best practices for the preparation of tests.

The following guidelines are established to guarantee the quality and integrity of the evidence collected and that, therefore, may be admitted as evidence in a judicial process:

- In the case of paper documents: a copy of the original document should be kept with a record of who found the document, where and when it was found, and who witnessed the discovery. It must be ensured that the original document has not been altered.
- In the case of information on computer media: exact images or copies of any removable media and information on hard disks or memory must be made to ensure its availability.
- A record must be kept of all actions taken during the copying process and must be witnessed by another person. The original media and the log should be stored in a secure place to prevent unauthorized access to them.

Incident resolution

Containment of the incident does not always imply resolution of the cause for which the incident materialized. Once the incident is contained, the resolution team must take the following steps:

- Identify the root cause of the incident.
- Proceed with the resolution of the root cause by introducing the appropriate countermeasures and verifying their effectiveness.

The resolution team should keep Information Security informed on a regular basis and document all actions taken during incident management. Members of the resolution team may not provide information related to incident management to third parties outside of the resolution team itself or Information Security.

If the assigned resolution team is unable to resolve the issue, it should escalate the issue to more experienced resolution teams according to established procedures and channels.

During the incident management process, Information Security must monitor the degree of progress achieved and assume sole responsibility for reporting to third parties any information related to the incident.

Closing

Report

At the end of any security incident, the incident resolution team shall generate a formalised report containing at least the following information:

- Origin of the incident.
- Impact caused.
- Actions taken during case management, both during containment and in case resolution.
- Proposal of foreseen actions to minimize the probability of occurrence of new similar incidents.

Legal actions

Based on the conclusions drawn from the incident closure report, Information Security with Legal Affairs, and if applicable Compliance, will assess the need to make the results of investigations available to People or to NH Internal Committees empowered to take appropriate legal action that may result from the incident.

Continuous improvement

In order to contribute to the continuous improvement of the security incident management process, Information Security will, periodically or on request, produce executive reports related to the security incident management process.

The content of such reports shall include aspects such as:

- Volume and nature of security incidents managed in the process.
- Analysis of root causes of recurrent incidents and proposal of action plans to correct them.
- Monitoring of the action plans proposed as a consequence of the security incidents managed during the period.

5.12. INFORMATION SECURITY CONSIDERATIONS FOR BUSINESS CONTINUITY MANAGEMENT

5.12.1. Continuity of information security

Continuity of information security is taken into account by NH within the business continuity management process.

Planning

With regard to information security continuity planning, the department Information Security is responsible for:

- Defining the information security requirements that must be taken into account when planning the business continuity management process.
- Supervising that the information security requirements considered in the planning phase are actually implemented in the backup information systems.
- Analyzing new aspects related to information security within the business continuity management process, aiming to identify new information security requirements applicable under adverse situations.

Implementation

NH must establish, document and implement processes, procedures and controls to ensure the required level of information security during adverse situations.

Information Security must ensure that there are:

- Personnel with authority and competence to respond to security incidents.
- Recovery procedures detailing specific security requirements.

In accordance with information security continuity requirements, the following must be established, documented, implemented and maintained:

- Information security controls within the processes, procedures, support systems and tools used for business continuity management.
- Support controls aimed at mitigating those information security controls that cannot be employed during an adverse situation.

Review and update

NH must verify periodically, or after a significant modification, that security controls in relation to business continuity are implemented correctly, in order to ensure that these controls are effective in adverse situations.

In order to benefit from potential synergies, these checks are carried out during business continuity plan tests.

5.12.2. Technological contingency

The NH Group has designed and implemented a technological contingency architecture that enables the Group to meet the availability requirements defined by the business representatives.

In addition, the following formal, documented procedures are available:

- Organizational procedures used to declare a contingency situation, manage the situation and, once completed, return to normal operation.
- Technical procedures, used as guidance to recover a specific system and/or specific technological architecture. These procedures are comprehensive in order to make the person responsible for their execution independent.

The correct operation of the technological contingency architecture and its associated procedures is periodically tested. This process is documented and formalized, it is carried out by the providers responsible for managing the IT infrastructure, and it is supervised by Information Security.

5.13. COMPLIANCE

In order to comply with legal and contractual requirements, the following aspects must be taken into account:

- Identify existing legislation related to information security.
- Adapt information systems, processes and responsibilities according to the identified legislation.
- Respect intellectual property rights.

- Provide appropriate protection for legally relevant or essential information records.
- Ensure compliance with personal data protection laws.

5.13.1. Compliance with legal and contractual requirements

Identification of applicable law and contractual requirements

The identification of new legal and contractual requirements related to information security is carried out in NH through Legal Affairs, Compliance and Information Security.

Any legislation involving any of the following aspects should be considered:

- Protection of private information and personal data.
- Intellectual property rights.
- Legal actions due to negligence or breach of contract.
- Collection of evidence in case of security incidents.
- Export of data to other countries.
- Security requirements in systems or communications.
- Monitoring of information and user rights.
- Protection of records.
- Security requirements in supplier contracts.
- Prevention of money laundering.
- Specific legislation for electronic financial transactions.

The identification of new regulatory requirements allows NH to:

- Define plans to adapt to the new regulatory requirements identified, either in the form of a project led by Legal Affairs & Compliance or Information Security, or including its execution within initiatives in other areas.
- Updating the NH Security Policy and the regulatory standards that derive from it. In this regard, it should be taken into account that, in its content, the NH Security Policy aims at all times to comply with the regulatory frameworks that apply to information systems.
- Define the security requirements to be taken into account during the development of new projects.
- Defining the security requirements to be taken into account in supplier relationships.
- Update the inventory of risks, threats and vulnerabilities, so that they are taken into account in the planning and execution of risk analysis exercises.

Finally, the areas and departments involved in the process are responsible for direct dialogue with external auditors, regulatory agencies, law enforcement agencies, and third parties in general, regarding certification of NH's level of compliance with the corresponding, applicable regulation.

Intellectual property rights

All activities related to information, or material, subject to intellectual property rights must consider the applicable legal restrictions in this regard.

Agreements should be established with manufacturers and/or owners of software and hardware products or protected material (e.g., documents, reports, etc.) in order to comply with intellectual property rights. Non-licensed software may only be used when it has been developed by the NH Group itself or has been specifically delivered by the developers.

NH employees and internal and external collaborators are aware of intellectual property rights and are aware of the prohibition on copying protected (copyrighted) applications and the prohibition on the use of unlicensed applications.

Protection of the company's records

Records of legally relevant or essential information (e.g., financial, accounting or any regulatory relevant data) must be protected in order to prevent leakage, loss or illicit alteration.

To this end, security measures are in place to ensure the confidentiality, integrity and availability of such records.

Protection and privacy of personal data

The protection of any personal data that is processed automatically or manually must guarantee the privacy of individuals, as well as the possibility to fully exercise their rights.

The technical and organizational security measures, as well as the responsibilities assigned to comply with current data protection legislation, are detailed in the NH "Security Document" and its annexes.

5.13.2. Information security reviews

Security policy compliance

NH understands information security as a process of continuous improvement. To this end, periodic reviews are performed with the following objectives:

- To verify compliance with NH's Security Policy, as well as the regulatory standards that derive from it, by employees and internal and external collaborators of the NH Group.
- To improve the NH Security Policy and, consequently, the NH security model. Performing compliance reviews contributes to:
    - o Identify deviations in the operational efficiency of the controls and/or in their design.
    - o Identify new security needs.
    - o Keep updated the regulatory standards deriving from the NH Security Policy.

Independent review of information security

An Information Security Review Plan must be drawn up annually, detailing the security reviews and analyses to be carried out in the next year. This Plan is included in the Information Security Tactical Plan for each year.

Similarly, external reviews, analyses and evaluations affecting IT & Systems will be coordinated by Information Security.

The following factors, among others, must be taken into account when drawing up the Plan:

- The NH Information Security Risk Map.
- The security incidents that occurred during the last year.
- Regulatory requirements affecting information systems.

The execution of each one of the review tasks included in the Plan will have to be detailed:

- The key stakeholders of both IT & Systems and the collaborators included in the scope of the evaluation will be identified.
- The IT & Systems managers, as well as the collaborators included in the scope, must provide all the information requested by Information Security for the development of the review.
- The scope of the review, the execution deadlines and how to access the information necessary to perform the audit will be agreed with the stakeholders that were previously identified.

The person designated as responsible for the information security review, evaluation or analysis shall in no case report hierarchically to the head of the Area or Department audited, thus ensuring the independence of the results.

Similarly, in the case of technical reviews to be carried out on NH production systems, the execution of the audit work must comply with the following considerations:

- All tests that may affect the availability of NH systems should be performed during low activity periods (e.g. outside working hours).
- Tests on production systems shall not modify or delete data. Tests that need to modify or delete data to prove the existence of a vulnerability should always be run in an isolated test environment.
- All checks and tests performed on systems should be recorded and evidenced.
- Tools used to test production systems must be licensed, supported, and approved prior to their use.

The results of security reviews, assessments and analyses conducted and/or coordinated by Information Security will be reported to the Security Committee and associated action plans will be planned to correct identified weaknesses. In those of a technical nature in which very serious vulnerabilities are detected, it will not be necessary to report all the results. Instead, results may be reported independently in order to anticipate the approval of the corresponding action plans.

The results of the security reviews, evaluations and analyses carried out or coordinated by Information Security will also serve for the development of the NH Group Security Plan.

6. COMPLIANCE

The present regulations provide coverage for aspects covered by the following internationally recognised security standards:

- Information technology. Security techniques. Information security management systems. Requirements. (ISO/IEC 27001)
- Information technology. Security techniques. Code of practice for information security controls. (ISO/IEC 27002)
- Payment Card Industry Data Security Standard (PCI DSS)

For the development of this policy, the legal requirements included in the applicable legislation corresponding to the main countries where the NH Group operates, such as the GDPR, the LOPD, the LPI or the LSSI, have been taken into account.

7. RELATED DOCUMENTS

- ALLNH-POL100-EN - Security Policy
- ALLNH-NOR201-EN - Glossary of terms and definitions