Information Security Policy

Information security management (ISM)

Paseo de la Castellana,79 -28046- Madrid (España)

Telefono: 932 661 614 (Llamadas desde España)

Internacional +34 933 935 946

Web: www.anf.es

Nivel de Seguridad

Documento CONFIDENCIAL

Acceso restringido a miembros de la Junta Rectora de la PKI, Comité de Seguridad, Auditores, empleados y organismo regulador.

INTEGRIDAD NIVEL 1 – DISPONIBILIDAD NIVEL 1

Aviso Importante

Dirección: Paseo de la Castellana, 79 - 28046 - Madrid (España)

Teléfono: 932 661 614 (llamadas desde España) Internacional (+34) 933 935 946

Web: www.anf.es

INDEX

ANF AC Management Commitment

The Management of ANF AC declares its total commitment with all the objectives established in this Information Security Plan, and of the set of documents published in the framework of Information Security Management Systems.

ANF AC, as a qualified trust services provider, and producer of security elements and services, considers the ICT systems (Information and Communications Technologies) and the Information Security that it manages in the development of its activity a key element for the fulfillment of its strategic objectives.

The Management of ANF AC supports, with total firmness and conviction, the requirements set forth in this Information Security Plan, and undertakes to promote and approve the necessary measures for its effective implementation in the organization.

Excellence requires assuming an effort of continuous improvement and, based on this, the Management of ANF AC carries out an annual review of its ISMS to guarantee its suitability, adaptation and continuous effectiveness.

Any changes that have an impact on the level of security provided must be approved by the PKI Governing Board.

Florencio Díaz Vilches

CEO of ANF Autoridad de Certificación

1. Document control

1.1. Name and identification of the document

Document name	Information Security Policy		
Version	1.5.		
OID	1.3.6.1.4.1.18332.101.80.1.		
Approval date	01/02/2022	**Publication date**	01/02/2022

1.2. Reviews

In order to ensure the validity of this regulatory framework, this document will be reviewed at least once a year and, immediately, when relevant changes occur in the organization, in the legal framework or technical standards.

In its review will have to take into account the new developments affecting the future strategy of the business, legal conditions, technical developments, and incidents that have occurred.

The responsibility for the approval of measures that presuppose a modification of the Information Security Policy, is of the PKI Governing Board at the proposal of the Security Committee.

Version	Changes	Author	Approval
1.5.	Revisión y actualización	Pablo Díaz	01/02/2022
1.4.	Revisión y actualización	F. Díaz	10/01/2019
1.3.	Revisión y actualización	Álvaro Díaz	01/02/2016
1.2.	Revisión y actualización	Laura Villas	27/04/2015
1.1.	Ampliación y actualización	Moisés Amador	02/04/2014
1.0.	Versión inicial de la Política de seguridad de la información	Isabel Fábregas	24/01/2011

2. Introducción

This Information Security Policy of ANF Autoridad de Certificación (hereinafter, ANF AC) is part of the regulatory body of the Information Security Management System (hereinafter ISMS) of ANF AC.

ANF Certification Authority (hereinafter, ANF AC), for its provision of trustworthy services depends on its human resources, the information it stores and custody, its documentary base, the technology developed by its R & D department, intangible assets and tangible assets, including ICT systems (Information and Communication Technologies), as well as its reputation.

The objective of information security is to guarantee the quality of information and the continuous provision of services, acting preventively, supervising daily activity and reacting quickly to incidents and ultimately, ensuring the continuity of the organization.

ICT systems must be protected against all types of threats, whether fortuitous or intentional. Our sector has a rapid evolution with the potential to influence the confidentiality, integrity, availability, intended use and value of information and services. To defend against these threats, a strategy is required that adapts to changes in the conditions of the environment to ensure the continuous provision of services. This implies that all departments of the organization must apply the minimum-security measures required by the Information Security Management System implemented by ANF AC, as well as continuously monitor levels of service delivery, follow and analyze the reported vulnerabilities, and prepare an effective response to the incidents to ensure the continuity of the services provided. This document defines the Information Security guidelines in accordance with the interests of ANF AC and its interested parties.

Of special incidence for our organization is the legal and technical framework. ANF AC is regulated by specific laws and regulations that we are committed to follow and respect.

The different departments must ensure that ICT security is an integral part of every stage of the system's life cycle, from its conception to its withdrawal from service, through development or acquisition decisions and exploitation activities. Security requirements and funding needs should be identified and included in planning, offers request, and bidding documents for ICT projects.

Departments should be prepared to prevent, detect, react and recover from incidents. Specifically:

1. The system security must include aspects of prevention, detection and correction, to procure threats on the system do not materialize, do not affect seriously the information handled, or the services provided.
2. Preventive measures should eliminate or at least reduce the possibility that threats get to materialize endangering the system. These prevention measures will include, among others, deterrence and reduction of exposure.
3. The detection measures will be accompanied by measures of reaction, so that security incidents be addressed on time.
4. The recovery measures will allow the restoration of information and services, so that they can cope with situations in which a security incident disable the usual means.
5. Without detracting from the other basic principles and minimum requirements established, the system will ensure the preservation of data and information in electronic form.

6. Similarly, the system services remain available throughout the life cycle of digital information, through a conception and procedures that are the basis for the preservation of digital heritage.

3. Purpose

Its main objective of this document is to collect the guidelines that must follow the security of the information according to the needs of ANF AC and the current legislation. In addition, it establishes guidelines for action in the case of incidents and defines responsibilities.

The following objectives are defined:

- Define the basic principles of Information Security.
- Detail all aspects related to the Information Security policy of ANF AC (object, scope, approval, entry into force and application, breaches and sanctions, review and improvement).
- Indicate the documentation that develops the Information Security policy of ANF AC.
- Detail the organization of Information Security in ANF AC.
- Describe the actions of ANF AC regarding personal data.
- Promote the continuous improvement of the effectiveness of our system and processes, as a permanent objective of ANF AC, as well as sustain and increase information security and customer satisfaction.

Information security objectives should:

- be consistent with the information security policy
- be measurable (if applicable)
- take into account applicable safety requirements and the results of valuations and risk treatment
- be communicated
- be updated

The document delimits what has to be protected, whose and why. It should explain what is allowed and what is not allowed; determines the limits of acceptable behavior and what the response is if these are exceeded; and identify the risks to which the organization is subject.

In order for this Security Policy to be a useful document in the organization and comply with the provisions of the UNE-ISO / IEC 27001: 2013 standard, the following requirements have been contemplated:

- It is drafted in a way accessible to all staff of the organization. Therefore, accurate and easy to understand.
- It is approved by the Governing Board at the proposal of the PKI Security Committee, and publicized by the Safety Manager.
- It is common knowledge within the organization, and is available for consultation whenever necessary.
- It must be the reference for conflicts resolution and other issues relating to the security of the organization.
- It must define responsibilities given that they are associated with what is established at all times by Safety Committee. Which, depending on the responsibilities, will decide who is authorized to access what kind of information.
- It is established that the organization assets to protect are:
    - staff

  - information, as well as its
  - reputation and continuity.
- It points out the rules and regulations that must be taken and the necessary security measures.

4. Scope

This document, as well as those that complement, implement or develop it, will be applicable to all information systems of ANF AC and that infrastructure and systems that provide support.

ANF Certification Authority (ANF AC) is accredited and provides the following qualified trust services:

- **Issuance of qualified electronic signature certificates**
- **Issuance of qualified electronic seal certificates *(QSealC)***
- **Issuance of Qualified Website Authentication Certificates *(QWACs)***
- **Qualified electronic time stamping service *(QTimeStamping)***
- **Qualified validation service of electronic signatures and seals**
- **Qualified preservation service for electronic signatures and seals**
- **Qualified certified electronic delivery service *(eDelivery)***

The Public Key Infrastructure (PKI) and the services provided by ANF AC follow the guidelines of Reglamento [UE] 910/2014, de 23 de julio de 2014, del Parlamento Europeo y del Consejo (hereinafter "eIDAS"), and the Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

5. Mission

ANF AC, as a Qualified Trusted Services Provider, manages a public key infrastructure in order to provide the following qualified services:

- **Service of issuance, revocation and renewal of qualified certificates of electronic signature**, in accordance with the eIDAS Regulation.
- **Service of emission, revocation and renewal of qualified certificates of electronic seal**, in accordance with the eIDAS Regulation.
- **Service of issuance, revocation and renewal of qualified SSL secure server certificates**, in accordance with the eIDAS Regulation.
- **Qualified Validation service of electronic signatures and seals**.
- **Electronic time stamp servic**e, which allows its users to obtain a guarantee that determines with total certainty that the information existed at a specific moment in time.
- **Service of electronic signature preservation**, which aims to extend the reliability of electronic signature data beyond the period of technological validity.
- **Certified electronic delivery service**, which allows data to be transmitted between third parties by electronic means.

6. Regulatory Framework

The legal and technical framework that must be respected by ANF AC, is detailed in the document OID: 1.3.6.1.4.1.18332.101.80.8 Annex 12_Normas y Estándares ANF AC.

6.1. Rules governing for the organizational structure of information security

Rules for: TOP MANAGEMENT / PKI Governing Board

- The top management of ANF AC should study and, where appropriate, approve the proposed regulations on the ISMS as proposed by the Security Committee.
- The top management, in case of approving a new document of ISMS, will give instructions so that it is brought to the attention of all parties that are authorized to access.
- The top management, in case of approving the modification or deletion of a document of ISMS will give instructions to report the new version to all parties who are authorized to access.
- The top management should actively promote a culture of information security in ANF AC, preferentially supporting the development and participation of ISMS courses.
- The top management shall inform the Security Committee about:
    - Aspects regarding the business strategy of the organization.
    - Aspects relating to market knowledge, especially competition.
- The top management will make an estimate of the financial resources available for the ISMS.

Rules for: PKI Governing Board and CEO

- The top management and CEO of ANF AC must allocate resources, physical infrastructure and personnel needed to manage the information security of the organization.
- The CEO assumes executive responsibility for carrying out the decisions adopted by the PKI Governing Board.

Rules addressed to: INFORMATION SECURITY COMMITTEE

- The Information Security Committee must update and submit to the Governing Board the Information Security Policies, the methodology for security risk analysis and methodology for classification of information as it deems appropriate.
- The Information Security Committee should analyze security incidents that are scaled and activate the process of contact with the authorities, when necessary.
- The Security Committee is responsible for managing the development, review and evaluation of information security policy.
- This policy will be reviewed at least once a year, and whenever any new circumstances advises it. In its review, it should be taken into account how many new developments affect the future strategy of the business, legal conditions, technical developments, and incidents that have occurred.
- In the revisions made by the Security Committee shall take into account the provisions of the existing legal framework, technical reference standards and recommendations issued by the reference organizations of which ANF AC is a member, and on which it has taken a commitment to respect.

- The Security Information Committee must verify compliance with security policies of the information mentioned in here.

Rules addressed to the Security Officer

- The Security Officer should lead the generation of guidelines for managing security information of ANF AC and the establishment of technical, physical and administrative controls resulting of security risk analysis.
- The Security Officer should validate and regularly monitor the implementation of the established security controls.

Rules addressed to the Internal Audit Manager

- The Internal Audit Manager should plan and perform internal audits to the Information Security Management System of the entity in order to determine whether policies, processes, procedures and controls in place are consistent with institutional requirements, security requirements and applicable regulations.
- The Audit Manager must execute full or partial reviews of processes or areas that are part of the scope of the Information Security Management System in order to verify the effectiveness of corrective actions when nonconformities are identified. The Office of Internal Control
- The Audit Manager should report the audit findings to those responsible of the areas and to the Security Committee.

Rules addressed to the Technology and Systems Manager

- Technology Manager must assign the functions, roles and responsibilities, to their employees for the operation and administration of the organization's technology platform. Such functions, roles, and responsibilities must be documented and appropriately segregated.

Rules addressed to: ALL EMPLOYEES OF THE ORGANIZATION AND THIRD PARTIES

- ANF AC employees, and third parties working in or for the organization, are responsible for complying with policies, rules, procedures and standards regarding information security.

6.2. Infractions

The failure to comply with any obligation or rule outlined in any of these documents is rated by default as OBJECTIVE. However, it will be the Security Committee, in relation to the specific circumstances of each case, who ultimately determines the final qualification.

6.3. Sanctions

Any action aimed at reducing or eliminating the effectiveness of the controls implemented to guarantee Information Security, to alter the properties of Information Security, or to hinder or prevent the investigation of any violation of the Information Security policy and its development regulations, will be considered a

violation of trust and could be cause for investigation and, where appropriate, the corresponding disciplinary or legal actions against those responsible.

Sanctions are classified as established by the Internal Regulation of ANF AC.

7. The Assets of the Information Security

ANF AC has information that must be protected against risks and threats to ensure the proper operation of your business. This type of information is essential for the company, is what is called Information Security asset. Its protection is the objective of any Information Security Management System.

Assets can be divided into different groups per their nature. If we follow Magerit's methodology for grouping assets (used by AA.PP.), these are the types we find.

1. **Services**, that is, the business processes that the organization offers abroad such as the issuance of certificates, time-stamp, OCSP responses, etc., or that it offers internally, as is the case with payroll management, billing, etc.
2. **Data and information that is manipulated within the organization.** They are usually the core of the system, while the rest of assets usually give storage support, manipulation, and so on.
3. **Software applications.**
4. **Computer equipment.**
5. **The staff.** This is the main asset. Includes internal staff, subcontractors, customers, and so on.
6. **Communications networks** that support the organization for the movement of information. They can be owned or subcontracted networks to third parties.
7. **Information media**. The physical supports that allow the storage of information over a long period.
8. **Auxiliary equipment** that supports information systems and which are assets that have not been included in any of the other groups. For example, documentation destruction equipment or air conditioning equipment.
9. **Facilities where information systems**, such as offices, buildings or vehicles **are housed.**

Along with these assets, you must consider those intangibles such as the image and reputation of a company. To protect the information assets, it is necessary to know them and to identify what they are within the organization. For this purpose, an inventory has been drawn up that identifies and classifies them. Each asset in the inventory includes, at least, its description, location and responsible for use.

8. Organization Security

ANF AC has a specific policy "Policy of Roles and Responsibilities" OID 1.3.6.1.4.1.18332.38.1.

8.1. Organization Security: Roles and Responsibilities

PKI Governing Board	It is the top management group responsible for analyzing and, where appropriate, approving the company's security and information continuity strategy, analyzing and approving information security policies, setting priorities for the development of security projects, and assess the reports submitted to it for study on the implementation and effectiveness of the measures adopted.
Managemen team	It is the management group in charge of managing and administering ISMS.
Security Committee	It is the group in charge of defining and proposing the security strategy and information continuity for the company, defining and proposing information security policies, developing and presenting security projects, controlling their development, and reviewing the implementation and Effectiveness of the measures adopted, issuing the corresponding reports.
Department Responsible	It is the group in charge of defining and proposing the strategy of security and continuity of the information.
Employees	Personnel assigned to the ANF AC workforce who are directly involved in ANF AC's information security management system.
Third-party Employees	Personnel assigned to the workforce of the companies contracted by ANF AC, and that assume the information security management system of ANF AC.

8.2. Policies and published documents

The details of all the documents published and approved by the organization, a summary explanation of the objective of each of them and normative references, are detailed in the document “Scope and documentary structure of the Information Security Management System" of which this document is part of.

9. Personal Data

ANF AC treats personal data. The documents that make up the Information Security Management System will only be accessible to authorized persons. All information systems of ANF AC will conform to the levels of security required by the regulations for the nature and purpose of the personal data collected in the aforementioned Security Document.

ANF AC protects personal data files in accordance with the provisions of Spanish Law 15/1999 of December 13, Protection of Personal Data (Act), in the Spanish Royal Decree 1720/2007 of 21 December , by which it is approved the Regulation of development of the Organic Law 15/1999, of December 13, and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

10. Information Security Risk Analysis and Management

The Information Security Management System has performed a risk analysis, evaluating the threats and risks to which they are exposed. This analysis will be repeated:

- Regularly, at least once a year,
- When changing the managed information,
- When changing services provided,
- When a serious security incident occurs,
- When severe vulnerabilities are reported.

The organization detailing all aspects relating to this paragraph in the document published "Methodology Risk Analysis".

In general, it is worth mentioning:

10.1. Uso aceptable de los activos

De forma general:
Los activos deben de estar clasificados según su valor, los requisitos legales, su sensibilidad y criticidad para la organización.

La información, junto a los procesos y sistemas que hacen uso de ella, son activos esenciales para cumplir los objetivos de ANF AC. Es esencial la seguridad de la información cualquiera que sea su forma y medio de comunicación y/o conservación (información de los sistemas, documentos impresos, etc.). Toda información definida como activo debe ser clasificada para garantizar un nivel de seguridad y privacidad, y que garantice su adecuada conservación a lo largo del tiempo.

De forma específica:

- Política de gestión de activos de información (Ver Anexo 18 Cap. 10)

10.2. Tratamiento de la información impresa después de su uso

De forma general:

- **Destrucción**
  - **-Soporte papel**:
    Debe depositarse en papeleras dispuestas a tal efecto para posteriormente ser destruidos bajo control.
  - **Soporte electrónico**:
    Antes de ser desechados o reutilizados, deben ser procesados para su borrado lógico o hacer ilegible la información contenida lógico o hacer ilegible la información contenida.
- **Etiquetado**

Toda información, sea en soporte electrónico o papel, que disponga de la imagen corporativa de la entidad o sus formatos será automáticamente clasificada como de *Uso interno*. Solo el Responsable de Seguridad tendrá la facultad de definir otra clasificación como: *Pública o Confidencial.*

De forma específica según lo establecido en:

- Política de clasificación, etiquetado y manejo de la información (Ver Anexo 18, Cap.11)

10.3. Soportes de almacenamiento externo y equipos portables

De forma general:

- Está absolutamente prohibido el empleo de dispositivos de almacenamiento externo –HD, PenDrive, Soportes ópticos, etc- de ámbito privado en equipos informáticos de la organización.
- Está totalmente prohibido, salvo autorización expresa del Responsable de Seguridad, emplear equipos informáticos portables personales, en las instalaciones de ANF AC.
- Está totalmente prohibido, salvo autorización expresa del Responsable de Seguridad, la conexión de Smartphones, tablets, etc., a la red de comunicaciones de ANF AC.

De forma específica según lo establecido en:

- Política de Periféricos y medios de almacenamiento (Ver Cap 13 Anexo 18)

10.4. Puesto de trabajo

De forma general:

Equipos informáticos de la organización

- Cada persona al incorporarse en la organización, recibe los instrumentos de trabajo necesarios, firmando la recepción de los mismos en un proceso denominado "*Bienvenida*", y el compromiso de su devolución en un proceso denominado "*Despedida*"
- El acceso a estos equipos debe de ser personal y empleando los recursos que la organización a puesto a su disposición.
- Debe de verificar que se activa el protector de pantalla de manera automática y que la reanudación del puesto de trabajo implica la desactivación de la pantalla protectora con la introducción del sistema de protección correspondiente.
- ANF AC sigue la Política de "mesa limpia", - Guardarlos en cajones con llave y/o en archivadores-. Está completamente prohibido
    - Deje documentos a la vista.
    - Dejar información a la vista como:
        - Nombre de Usuario y Passwords
        - Direcciones IP
        - Contratos
        - Facturas

        - Números de Cuenta
        - Listas de Clientes
        - Propiedad Intelectual
- ANF AC dispone de almacén cerrado y acceso restringido a personal autorizado, que debe de ser utilizado para custodia de:
        - Datos de Empleados/ Currículums
        - Datos de terceras personas ajenas a la organización.
- ANF AC dispone de Caja de Seguridad que deben de ser utilizadas para el almacenamiento de información de alto valor.
- ANF AC tiene contratadas diversas cajas de seguridad bancaria que deben de ser utilizadas para el guarda y custodia de información crítica.
- El identificador de usuario tendrá unos privilegios asociados, en función del cargo y las funciones que desempeñe. Los privilegios asociados a cada usuario le permitirán, en función de cada caso, acceder a un determinado tipo de información.
- El uso de un identificador único hace posible el seguimiento de las actividades realizadas por los usuarios, otorgando así responsabilidad individual sobre las acciones.
- Las modificaciones de hardware y software se realizarán exclusivamente por personal técnico de la organización. O por empresas o autónomos expresamente autorizados por el Responsable de Seguridad.
- Está prohibido el empleo del equipamiento informático de la empresa para actividades personales.
- Está prohibido el acceso a páginas de Internet que no tengan como único y exclusivo fin, desarrollar actividades necesarias para los objetivos de la organización.

Impresoras, escáner y fotocopiadoras

- No se debe de dejar funciones y equipos de soporte desatendidos, sobre todo si se va a imprimir o se está imprimiendo información confidencial de la organización.

Correo electrónico y otros canales de comunicación

- Los usuarios que utilicen el correo electrónico dentro de la organización serán responsables de evitar prácticas que puedan comprometer la seguridad de la información.
    - Los servicios de email corporativos se suministran para servir a propósitos operacionales y administrativos relacionados con el negocio.
    - Todos los emails procesados por los Sistemas de Información corporativos y redes son considerados propiedad de la organización, por lo tanto, y dado que los mismos no gozan de privacidad, no se pueden utilizar las cuentas corporativas de la empresa, para asuntos personales.
      AVISO IMPORTANTE: ANF AC con el fin de mejorar sus procesos de calidad de gestión y controles de seguridad, monitoriza periódicamente los correos recibidos y enviados. Y la organización dispone de un sistema de recuperación de correos borrados.
- Está prohibido usar el correo electrónico para:

- Para enviar información confidencial/sensible, particularmente a través de Internet, a menos que ésta sea primero cifrada por un sistema de cifrado aprobado por el Responsable de Seguridad.
- Para crear, enviar, reenviar o almacenar emails con mensajes o adjuntos que podrían ser ilegales o considerados ofensivos, p.ej. sexualmente explícitos, racistas, difamatorios, abusivos, obscenos, discriminatorios u otros ofensivos. Para enviar un mensaje desde la cuenta de alguien o en su nombre (incluyendo el uso de una dirección falsa en el campo 'De').
- SOLO si se autoriza por Dirección, una secretaria puede enviar emails en nombre de Dirección de la organización, pero deberá firmar el email en su propio nombre.
- Sea razonable sobre el número y tamaños de email enviados y guardados.
- Periódicamente elimine definitivamente del buzón correos borrados o spam.
- Clasifique los mensajes que necesite para mantenerlos bajo las carpetas apropiadas.

- No se pueden utilizar los medios de comunicación de ANF AC para conversaciones privadas y personales.
- AVISO IMPORTATNE: ANF AC con el fin de mejorar sus procesos de calidad de gestión y controles de seguridad, realiza grabación de las conversaciones. ANF AC habilita una línea de comunicación privada para llamadas personales urgentes.

De forma específica según lo establecido en:

- Política de uso de tokens de seguridad (Ver Anexo 18 Cap. 12)
- Política de seguridad física y medioambiental (Ver Anexo 18 Cap. 15)
- Política para uso de dispositivos móviles (Ver Anexo 18 Cap. 5)
- Política para uso de conexiones remotas (Ver Anexo 18 Cap. 6)
- Política de gestión de activos de la organización (Ver Anexo 18 Cap. 10)
- Política de seguridad para los equipos corporativos (Ver Anexo 18 Cap. 16)
- Política de uso del correo electrónico (Ver Anexo 18 Cap. 23)
- Política de adecuación de uso de Internet (Ver Anexo 18 Cap. 24)

10.5. Gestión de incidencias

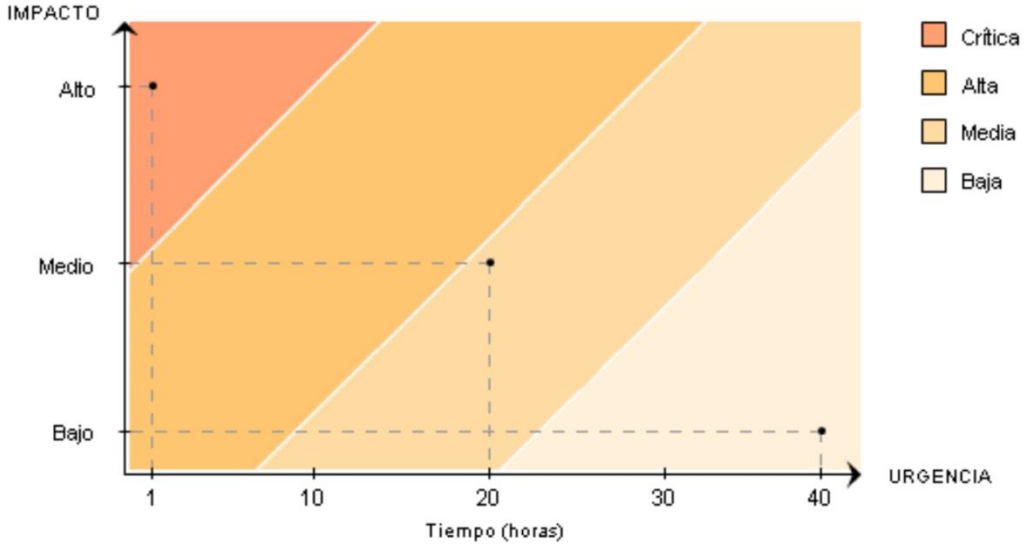
Posibles incidentes o eventos, que serán inexcusablemente registrados (esta lista no debe entenderse como Limitativa, sino que podrá ser ampliada con cualquier otro tipo de incidencias que hubiera quedado omitida, Y EN ESPECIAL primando la prudencia de notificar hasta la mera sospecha de anomalía en la rutina habitual de la organización) pueden ser los siguientes:

De forma general:

- Pérdida de servicio, equipos o instalaciones
- fallos o sobrecargas del sistema
- errores humanos
- incumplimiento de políticas o directrices

- incumplimientos de los acuerdos de seguridad física
- cambios del sistema no controlados
- fallos del software o del hardware
- violaciones de acceso
- eventos que afecten a la identificación y autenticación de los usuarios
- eventos que afecten a los derechos de acceso a los datos
- incidencias que afecten a la gestión de soportes incidencias que afecten a la gestión de soportes
- eventos que afecten a los procedimientos de copias de seguridad y recuperación.

Prioridad según impacto de la incidencia



Crítica: Es una emergencia, es un incidente cuya resolución no admite demora.
Los incidentes de este tipo se procesarán en paralelo de haber varios, y en su resolución se emplearán todos los recursos disponibles disponibles. Ejemplo: todos los que supongan peligro para vidas humanas, para la infraestructura de Internet, sistema de emisión de certificados servicios de CRL-OCSs-TSU-AR.
Hasta ahora también se han considerado todos aquellos incidentes que requerían acción inmediata debido a su rapidez y ámbito de difusión.

Alta: Un incidente de alta prioridad es aquél cuyas características requieren que sea atendido antes que otros, aunque sea detectado posteriormente. Para esto se mantiene una cola independiente de incidentes de alta prioridad, y no se procesarán los de prioridad inferior mientras queden de éstos. Los incidentes de alta prioridad se procesan en serie. Ejemplo: se consideran incidentes de alta prioridad todos aquellos en que exista infiltración de una cuenta privilegiada o denegación de servicio.

Media: Por defecto, los incidentes se atienden en serie por orden de llegada, mientras no requiera atención uno de prioridad superior. Un incidente de prioridad normal puede adquirir la categoría de alta prioridad si no recibe atención por un tiempo prolongado. Ejemplo: todos los incidentes no clasificados no clasificados como alta prioridad o emergencia, donde el atacante haya ganado acceso a un sistema informático ajeno. También se incluyen escáneres insistentes de redes, o ataques de denegación de servicio.

Baja: Los incidentes de baja prioridad se atienden en en serie por orden de llegada, mientras no requiera atención uno de prioridad superior. Un incidente de baja prioridad será cerrado automáticamente si no recibe atención por un tiempo prolongado.

De forma específica según lo establecido en:

- Política de registro de eventos y monitoreo de los recursos tecnológicos y los sistemas de la organización (Ver Anexo 18 Cap. 19)
- Política para el reporte y tratamiento de incidentes de seguridad (Ver Anexo 18 Cap. 31)

10.6. Compromiso de confidencialidad para el personal

De forma general:

Todo el personal al incorporarse a ANF AC, y dentro del procedimiento de BIENVENIDA, suscribe un compromiso de confidencialidad.

Este COMPROMISO DEBE MANTENERSE, incluso después de extinguida la relación laboral con organización.

De forma específica según lo establecido en:

- Política de seguridad del personal (Ver anexo 18 Cap. 7)
- Política aplicable durante la vinculación de empleados y personal provisto por terceros (Ver anexo 18 Cap. 8)

11. Herramientas para implementar la Política de Seguridad

Dado que la Política de Seguridad está escrita a un nivel muy amplio, se requiere complementarla con documentos más precisos que ayuden a llevar a cabo lo propuesto:

- **Normas de seguridad** *(security standards)*
  Las normas uniformizan el uso de aspectos concretos del sistema. Indican el uso correcto y las responsabilidades de los usuarios. Son de carácter obligatorio.

- **Guías de seguridad** *(security guides)*
  Las guías tienen un carácter formativo y buscan ayudar a los usuarios a aplicar correctamente las medidas de seguridad proporcionando razonamientos donde no existen procedimientos precisos. Las guías ayudan a prevenir que se pasen por alto aspectos importantes de seguridad que pueden materializarse de varias formas. ANF AC cuenta con diversos cursos formativos específicos para cada área de la organización.

- **Procedimientos de seguridad** *(security procedures)*
  Los procedimientos de seguridad afrontan tareas concretas, indicando lo que hay que hacer, paso a paso. Son útiles en tareas repetitivas.

Por motivos funcionales estos elementos no siempre se separan nítidamente, sino que a veces se generan manuales, cursos formativos y reglamentos de seguridad, que tienen un poco de todos los elementos anteriormente mencionados, buscando siempre una mayor efectividad en la concienciación y formación de los usuarios del sistema.

Si bien los manuales y reglamentos de carácter mixto pueden servir como herramientas importantes, a menudo es útil distinguir claramente entre lo que es política (abstracta) y su aplicación concreta. De esta forma se es más flexible y se consigue una cierta uniformidad de resultados incluso cuando cambia la tecnología o los mecanismos empleados. Por lo tanto, en la medida de lo posible, siempre se establecerán diferencias entre unos y otros.

Todos y cada uno de los documentos publicados por ANF AC en el marco de su Política de Seguridad, están detallados en el documento “Alcance y Estructura Documental del SGSI”.

En el marco de los Sistemas de Gestión de la Seguridad de la Información, y en conformidad con el apartado 12.6.1 GESTIÓN DE VULNERABILIDADES TÉCNICAS. Se realiza,

- Mantener actualizada la información de fabricantes y proveedores

Las actualizaciones, ya sean de seguridad o de funcionalidad, de los sistemas de control deben estar guiadas por un proceso de gestión de parches que identifique adecuadamente el ciclo de vida e indique su periodicidad. Una buena gestión de parches en los sistemas de control se ha de enfrentar con la cultura de este entorno, que se opone a todo cambio en un sistema que funciona; y a la cultura de los fabricantes, no

muy dados a publicar parches para solucionar problemas de seguridad. Afortunadamente, ambas limitaciones son ya casi cosas del pasado.

12. Concienciación del personal

La seguridad de la información se basa en la capacidad para preservar su integridad, confidencialidad, disponibilidad y accesibilidad por parte de los elementos involucrados en su tratamiento: equipamiento, software, procedimientos, así como de los recursos humanos que utilizan dichos componentes.

En este sentido, es fundamental educar e informar al personal desde su ingreso y en forma continua, cualquiera sea su situación laboral con la entidad, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad. De la misma forma, es necesario definir las sanciones que se aplicarán en caso de incumplimiento.

La implementación del SGSI, tiene como meta minimizar la probabilidad de ocurrencia de incidentes. Es por ello, que resulta necesario implementar un mecanismo que permita reportar las debilidades y los incidentes tan pronto como sea posible, a fin de subsanarlos y evitar eventuales replicaciones. Por lo tanto, es importante analizar las causas del incidente producido y aprender del mismo, a fin de corregir las prácticas existentes, que no pudieron prevenirlo, y evitarlo en el futuro.

12.1. Objetivo

Reducir los riesgos de error humano, comisión de ilícitos, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información.

Ser explicito con las responsabilidades en materia de seguridad en la etapa del ingreso de personal e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado.

Garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren capacitados para cumplir los requerimientos del SGSI en el transcurso de sus tareas normales.

Establecer Compromisos de Confidencialidad con todo el personal y usuarios externos de las instalaciones relacionados con el manejo de la información de la organización. Establecer las herramientas y mecanismos necesarios para promover la comunicación de debilidades existentes en materia de seguridad, así como de los incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir su reincidencia.

12.2. Alcance

Se aplica a todo el personal de ANF AC y al personal provisto por terceros, cualquiera sea su situación laboral, y al personal externo que efectúe tareas para la entidad.

12.3. Responsabilidad

El Responsable Legal y de Recursos Humanos incluirá las funciones relativas a la seguridad de la información en las descripciones de puestos de los funcionarios, informará a todo el personal que ingresa, sus obligaciones respecto al cumplimiento de la Política de Seguridad de la Información, gestionará los Compromisos de Confidencialidad con el personal y coordinará las tareas de capacitación de usuarios respecto a la Política.

El Responsable de Seguridad tendrá a cargo el seguimiento, documentación y análisis de los incidentes de seguridad reportados, así como su comunicación al Comité de Seguridad de la Información, a los responsables en el tratamiento de la información.

El Comité de Seguridad de la Información debe ser responsable de implementar los medios y canales necesarios para que el Responsable de Seguridad maneje los reportes de incidentes y anomalías de los sistemas. Asimismo, dicho Comité, tomará conocimiento, efectuará el seguimiento de la investigación, controlará la evolución e impulsará la resolución de los incidentes relativos a la seguridad.

El Responsable Legal y RRHH participará en la construcción del Compromiso de Confidencialidad a firmar por los empleados, contratistas y terceros que desarrollen funciones en la entidad, en el asesoramiento sobre las sanciones a ser aplicadas por incumplimiento de los requerimientos del SGSI, y en el tratamiento de incidentes de seguridad que requieran de su intervención. Todo el personal de ANF AC debe ser responsable del reporte de debilidades e incidentes de seguridad que oportunamente se detecten.

13. Planificación de la calificación

El Responsable de Tecnología, debe efectuar el monitoreo de las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas, a fin de garantizar un procesamiento y almacenamiento adecuados. Para ello, tomará en cuenta además los nuevos requerimientos de los sistemas, así como las tendencias actuales y proyectadas en el procesamiento de la información de la organización para el período estipulado de vida útil de cada componente. Asimismo, informará las necesidades detectadas que puedan identificar y evitar potenciales cuellos de botella, que podrían plantear una amenaza a la seguridad o a la continuidad del procesamiento y puedan planificar una adecuada acción correctiva.

Todo ello queda recogido en los documentos:

- Documentación técnica del sistema de supervisión permanente de servidores (18332.36.1.1)
- Documentación técnica del sistema de protección de servidores (18332.37.1.1)
- Normativa sobre medidas de seguridad en las comunicaciones (1.3.6.1.4.1.18332.7.4.1)
- Sistema de detección de ataques e intrusiones (18332.35.1.1)

13.1. Responsabilidad

Los Responsables de Tecnología y de Seguridad, deben sugerir criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, solicitando la realización de las pruebas necesarias antes de su aprobación definitiva. Se deben considerar los siguientes puntos:

- Verificar el impacto en el desempeño y los requerimientos de capacidad de las computadoras.
- Garantizar la recuperación ante errores.
- Preparar y poner a prueba los procedimientos operativos de rutina según normas definidas.
- Garantizar la implementación de controles de seguridad.
- Diseñar planes de continuidad para las actividades de la Secretaría Distrital de Gobierno.
- Asegurar que la instalación del nuevo sistema, no afecte negativamente los sistemas existentes, especialmente en los períodos pico de procesamiento.
- Considerar el efecto que tiene el nuevo sistema en la seguridad global de la infraestructura tecnológica de ANF AC.
- Realizar el plan de entrenamiento en la operación y/o uso de los nuevos sistemas.