Política de seguridad de la información (SGSI)

Sistema de gestión de la Seguridad de la Información

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 RESTRINGUIDO

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

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

ÍNDICE

ÍNDICE **3**
Liderazgo y compromiso de la dirección de ANF AC **5**
1. Control del documento **5**
1.1. Nombre del documento e identificación 6
1.2. Revisiones 6
2. Introducción **7**
3. Objetivo **9**
4. Alcance **11**
5. Términos y deficiniones **12**
6. Misión **13**
7. Marco normativo **14**
8. Organización de la seguridad **15**
8.1. Estructura de supervisión 15
8.1.1. Dirección General 15
8.1.2. Responsable de Seguridad 16
8.1.3. Director jurídico 17
8.2. Estructura de operación 17
8.2.1. Responsable de sistemas 17
8.2.2. Responsable de desarrollo informático y programación 18
8.2.3. Responsable de cumplimiento normativo 18
8.2.4. Responsable de criptografía 19
8.2.5. Usuarios de los sistemas 19
8.2.5.1. Funciones y obligaciones del personal 19
8.2.5.2. Funciones y obligaciones de terceras partes 20
8.3. Normas que rigen en la estructura organizacional de seguridad de la información 20
8.4. Incumplimientos 22
8.5. Sanciones 22
8.6. Resolución de conflictos 22
9. Los activos de la Seguridad de la Información **24**
9.1. Gestión de riesgos 25
9.2. Uso aceptable de los activos 26

9.3. Tratamiento de la información impresa después de su uso 26
9.4. Soportes de almacenamiento externo y equipos portables 26
9.5. Puesto de trabajo 27
9.6. Gestión de incidencias 29
9.7. Compromiso de confidencialidad para el personal 31
10. Herramientas para implementar la Política de Seguridad 32
11. Establecimiento, implantación, mantenimiento y mejora del SGSI / ENS 34
12. Concienciación del personal 36
12.1. Objetivo 36
12.2. Alcance 36
12.3. Responsabilidad 36
13. Planificación de la calificación 38
13.1. Responsabilidad 38
14. Datos de carácter personal 40
15. Organización de la Seguridad 42
15.1. Políticas y documentos publicados 42

Compromiso y liderazgo de la Dirección General

La Dirección General de ANF AC es consciente de la importancia de proteger la información y los activos desde los que se trata dicha información. Los procesos de negocio de la organización dependen, en su mayoría, de la existencia de dicha información, y en gran parte somos meros custodios de los datos.

Con el fin de asegurar dicha protección y mantener su compromiso con la seguridad de la información y con sus clientes, proveedores, colaboradores, trabajadores y demás partes interesadas, ANF AC ha llevado a cabo la implantación de un SGSI basándose en el estándar internacional ISO/IEC 27001:2013., que se ha visto reforzado con la implantación de las normas ENS en su nivel ALTO. Todo ello sin obviar las obligaciones establecidas por el Reglamento (UE) General de Protección de Datos, en las que el foco principal son preservar los derechos fundamentales de los titulares de los datos personales.

La Dirección General de ANF AC ha participado en la elaboración y aprueba este documento y toda la documentación asociada para el correcto desarrollo, implementación y mantenimiento del SGSI / ENS.

La ISO/IEC 27001:2013 y el ENS, establecen la necesidad de que la Dirección General sea consciente de los riesgos asociados al tratamiento y almacenamiento de la información que es tratada en la organización.

Por este motivo, toda exclusión de controles que se considere necesaria para cumplir los criterios de aceptación del riesgo necesita ser justificada mediante evidencia de que los riesgos asociados han sido aceptados por los responsables. La exclusión de controles no deberá afectar a la capacidad y/o responsabilidad de la organización para garantizar la seguridad de la información de acuerdo con los requisitos de seguridad derivados de la evaluación de riesgos y de los requisitos legales o reglamentarios aplicables.

La Dirección General de ANF AC declara su total compromiso con todos los objetivos establecidos en esta Política de Seguridad de la Información, y del conjunto de documentos publicados en el marco de los Sistemas de Gestión de la Seguridad de la Información.

Asimismo, se compromete a impulsar y aprobar las medidas necesarias para su implantación efectiva en la organización.

La excelencia requiere asumir un esfuerzo de mejora continua y, en base a ello, la Dirección de ANF AC realiza anualmente una revisión de su SGSI / ENS para garantizar su idoneidad, adecuación y eficacia continuas.

Firmado,

FLORENCIO DIAZ VILCHES - 37271387W

Firmado digitalmente por FLORENCIO DIAZ VILCHES - 37271387W
Fecha: 2023.07.21 16:02:48 +02'00'

Florencio Díaz Vilches

Director General

ANF Autoridad de Certificación

1. Control del documento

1.1. Nombre del documento e identificación

Nombre del documento	Política de seguridad de la información		
Versión	1.6.		
OID	1.3.6.1.4.1.18332.101.80.1.		
Fecha de aprobación	10/07/2023	**Fecha de publicación**	10/07/2023

1.2. Revisiones

Con el fin de asegurar la vigencia de este marco normativo, este documento será revisado al menos una vez al año y, de forma inmediata, cuando se produzcan cambios relevantes en la organización, en el marco legal o normas técnicas.

En su revisión se deberá tener en cuenta las novedades afecten a la estrategia de futuro del negocio, condiciones legales, novedades técnicas, e incidencias que se hayan producido.

La responsabilidad de la aprobación de medidas que presupongan una modificación de la Política de Seguridad de la Información, es de la Junta Rectora de la PKI a propuesta del Comité de Seguridad

Versión	Cambios	Autor	Aprobación
1.6	Revisión y adaptación al ENS	Pablo Díaz	10/07/2023
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

Esta Política de Seguridad de la Información de ANF Autoridad de Certificación (en adelante, ANF AC) forma parte del cuerpo normativo del Sistema de Gestión de Seguridad de la Información (en adelante SGSI) de ANF AC.

ANF AC, para su prestación de servicios de confianza depende de sus recursos humanos, de la información que almacena y custodia, su base documental, la tecnología desarrollada por su departamento de I+D+i, activos inmateriales y activos materiales, entre los que destacan los sistemas TIC (Tecnologías de Información y Comunicaciones), así como su reputación.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes y en definitiva, garantizando la continuidad de la organización.

Los sistemas TIC deben estar protegidos contra todo tipo de amenazas, ya sean fortuitas o intencionadas. Nuestro sector acredita una rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que todos los departamentos de la organización deben aplicar las medidas mínimas de seguridad exigidas por el Sistema de Gestión de la Seguridad de la Información implantado por ANF AC, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados. Este documento define las directrices de Seguridad de la Información conforme a los intereses de ANF AC y sus partes interesadas.

De especial incidencia para nuestra organización es el marco legal y técnico. ANF AC está regulada por leyes y normas específicas que nos comprometemos seguir y respetar.

Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes. Concretamente:

1. La seguridad del sistema debe contemplar los aspectos de prevención, detección y corrección, para conseguir que las amenazas sobre el mismo no se materialicen, no afecten gravemente a la información que maneja, o los servicios que se prestan.
2. Las medidas de prevención deben eliminar o, al menos reducir, la posibilidad de que las amenazas lleguen a materializarse con perjuicio para el sistema. Estas medidas de prevención contemplarán, entre otras, la disuasión y la reducción de la exposición.

3. Las medidas de detección estarán acompañadas de medidas de reacción, de forma que los incidentes de seguridad se atajen a tiempo.
4. Las medidas de recuperación permitirán la restauración de la información y los servicios, de forma que se pueda hacer frente a las situaciones en las que un incidente de seguridad inhabilite los medios habituales.
5. Sin merma de los demás principios básicos y requisitos mínimos establecidos, el sistema garantizará la conservación de los datos e informaciones en soporte electrónico.
6. De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

3. Objetivo

Este documento tiene por objeto recoger las directrices que debe seguir la seguridad de la información de acuerdo a las necesidades de ANF AC y a la legislación vigente. Además, establece las directrices y principios que ANF AC gestionará y protegerá su información y sus servicios, a través de la implantación, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información (en adelante, SGSI) aplicando los requisitos de la Norma UNE ISO/IEC 27001:2017 y de sus partes interesadas, dentro del marco regulatorio legal y vigente como el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Se definen los siguientes objetivos:

- Definir los principios básicos de Seguridad de la Información.
- Detallar todos los aspectos relacionados con la política de Seguridad de la Información de ANF AC (objeto, alcance, aprobación, entrada en vigor y aplicación, incumplimientos y sanciones, revisión y mejora).
- Indicar la documentación que desarrolla la política de Seguridad de la Información de ANF AC.
- Detallar la organización de la Seguridad de la Información en ANF AC.
- Describir la actuación de ANF AC respecto a datos de carácter personal.
- Promover la mejora continua de la eficacia de nuestro sistema, y procesos, como objetivo permanente de ANF AC, así como sostener e incrementar la seguridad de la información y la satisfacción del cliente.

Los objetivos de seguridad de la información deben:

- ser coherentes con la política de seguridad de la información
- ser medibles (si aplica)
- tener en cuenta requisitos de seguridad aplicables y los resultados de valoraciones y de tratamiento de riesgos
- ser comunicados
- ser actualizados

De forma general ANF AC articulará mecanismos de prevención, reacción y recuperación con objeto de minimizar el impacto de los incidentes de seguridad.

En cuanto a la **prevención**, se debe evitar que los servicios y la información resulten afectados por un incidente de seguridad. Para ello, se implementará las medidas de seguridad establecidas en el Anexo II del ENS, así como aquellas medidas adicionales que pudieran ser identificadas en el proceso de análisis de riesgos.

En cuanto a la **reacción**, se establecerán mecanismos de detección, comunicación y gestión de incidentes de seguridad, de forma que cualquier incidente pueda ser tratado en el menor plazo posible. Siempre que sea posible, se detectarán de forma automática los incidentes de seguridad, utilizando elementos de monitorización de los servicios o de detección de anomalías y poniendo en marcha los procedimientos de respuesta al incidente en el menor plazo posible. Para los incidentes detectados por los usuarios, ya sean internos o externos, se establecerán los pertinentes canales de comunicación de incidentes.

En cuanto a la **recuperación**, para aquellos servicios que se consideren críticos, en base a la valoración que de los mismos realicen sus responsables, se deberán desarrollar planes que permitan la continuidad de dichos servicios en el caso de que, a raíz de un incidente de seguridad, quedaran indisponibles.

Esta Política de Seguridad,

- Esta firmada por el Director General de la Organización.
- Está aprobado por la Alta Dirección a propuesta del Comité de Seguridad, y publicitado por el Responsable de Seguridad.
- Es de dominio público dentro de la organización y colaboradores externos que prestan sus servicios en ANF AC. Se facilita una copia del documento durante el procedimiento de Bienvenida.
- Debe ser la referencia para la resolución de conflictos y otras cuestiones relativas a la seguridad de la organización.

4. Alcance

El presente documento, así como los aquellos que lo complementen, implementen o desarrollen, serán de aplicación a todos los sistemas de información de ANF AC y aquella infraestructura y sistemas que le proporcionen soporte.

ANF Autoridad de Certificación (ANF AC) dispone de acreditación y presta los siguientes servicios de confianza cualificados:

- **Solución de firma electrónica centralizada, con emisión, custodia, puesta a disposición y control de uso en Cloud. Sign to Sign.**
- **Solución de video identificación para autenticación de transacciones y expedición de certificados. Mi eID eSIGN.**
- **Sistema interno de información – Canal de denuncias en Cloud. Grattil.**
- **Emisión de certificados cualificados de firma electrónica**
- **Emisión de certificados cualificados de sello electrónica *(QSealC)***
- **Emisión de certificados cualificados de autenticación de sitio web *(QWAC)***
- **Servicio de sellado de tiempo electrónico cualificado *(QTimeStamping)***
- **Servicio de validación cualificada de firmas y sellos electrónicos**
- **Servicio cualificado de preservación de firmas y sellos electrónicos**
- **Servicio de entrega electrónica certificada cualificada *(eDelivery)***

5. Términos y deficiniones

- **SGSI**: Son las siglas del Sistema de Gestión de la Seguridad de la Información (regulado por la Norma UNE-ISO/IEC 27001), que es un conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.
- **ENS**: Son las siglas del Esquema Nacional de Seguridad, regulado por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, siendo su aplicación en el ámbito de la administración electrónica del sector público. Su objeto es establecer la política de seguridad y crear las condiciones necesarias para la confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permita el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.
- **Parte interesada**: Persona o grupo que tiene un interés en el desempeño o éxito de la organización.
- **Autenticidad**: Propiedad de que una persona y o empresa que ha accedido y utilizado la información es lo que afirma ser.
- **Confidencialidad**: Propiedad de la información de no ponerse a disposición o ser reveladas a personas y o empresas no autorizadas.
- **Integridad**: Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
- **Trazabilidad**: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a una persona y o empresa.
- **Disponibilidad**: Propiedad de la información de estar accesible y utilizable en el momento que se requiera por la persona y o empresa autorizada.
- **Activo**: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización.
- **Riesgo**: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
- **Amenaza**: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
- **Análisis de riesgos**: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
- **Tratamiento de riesgos**: Proceso de modificar el riesgo, mediante la implementación de controles.
- **Datos personales**: Cualquier información relacionada con una persona que permita identificarla o pueda servir para identificarla.

6. Misión

ANF AC es un Prestador Cualificado de Servicios de Confianza en conformidad con el Reglamento eIDAS. ANF AC administra una infraestructura de claves públicas (PKI) y esta oficialmente acreditada para la prestación, entre otros servicios cualificados:

- **Servicio centralizado de autenticación firma electrónica, emisión, custodia, puesta a disposición y control de acceso**.
- **Servicio de video identificación a distancia, para autenticación y emisión de certificados electrónicos**.
- **Servicio de emisión, revocación y renovación de certificados cualificados de firma electrónica**, en conformidad con el Reglamento eIDAS.
- **Servicio de emisión, revocación y renovación de certificados cualificados de sello electrónico**, en conformidad con el Reglamento eIDAS.
- **Servicio de emisión, revocación y renovación de certificados cualificados de servidor seguro SSL**, en conformidad con el Reglamento eIDAS.
- **Servicio de Validación cualificada de firmas y sellos electrónicos.**
- **Servicio de sellos de tiempo electrónico**, que permite a sus usuarios obtener una garantía que determina con plena certeza que la información existía en un momento concreto del tiempo.
- **Servicio de conservación de firmas electrónicas**, que tiene como objetivo ampliar la fiabilidad de los datos de la firma electrónica más allá del periodo de validez tecnológico.
- **Servicio de entrega electrónica certificada**, que permite transmitir datos entre partes terceras por medios electrónicos.

Además, ANF AC pone a disposición de sus clientes y del mercado en general,

- Sistema interno de información – Canal de denuncias en conformidad con la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

ANF AC esta acrecitada oficialmente por,

Agencia Española de Protección de Datos, como Entidad de Certificación conforme al Esquema DPD – AEPD

Agencia Estatal de Administración Tributaria, servicio de Digitalización Certificada de documentos fiscales.

7. Marco normativo

El marco legal y técnico que debe de ser respetado por ANF AC, esta detallado en el documento OID: 1.3.6.1.4.1.18332.101.80.8 Anexo 12_Normas y Estándares ANF AC.
ANF ha sido auditado y certificado en conformidad contra normas y estándares de de reconocimento internacional, entre otros:

- Conjunto de normas ETSI relativas a los servicios cualificados eIDAS.
- ISO 9001
- ISO 27001
- ISO 27024
- ISO 14001

Las normas legales de referencia son,

- Reglamento [UE] 910/2014, de 23 de julio de 2014, del Parlamento Europeo y del Consejo (en adelante "eIDAS"),
- la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza,
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos - RGPD).
- Ley 3/2018, de 5 de diciembre, Organica de Protección de Datos y Garantia de Derechos Digitales.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

GUIAS DE REFERENCIA
El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones por parte del Centro Criptológico Nacional (CCN), para facilitar un mejor cumplimiento de dichos requisitos mínimos. La serie de documentos CN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad.

1. CCN-STIC-402: Organización y Gestión para la Seguridad de los Sistemas TIC. 2006.
2. CCN-STIC-801: ENS - Responsabilidades y funciones. 2019.
3. CCN-STIC-805: ENS - Política de Seguridad de la Información. 2011
4. CCN-STIC-830: ENS - Ámbito de aplicación del Esquema Nacional de Seguridad. 2016 Informes y resoluciones de la Agencia Española de Protección de Datos (AEPD)

8. Organización de la seguridad

La organización de la seguridad está basada en la Guía CCN-STIC-402: Organización y Gestión para la Seguridad de los Sistemas TIC del Centro Criptológico Nacional.

Se establecerán las siguientes estructuras:

- **Estructura de supervisión**, que es la que se encarga de verificar el cumplimiento de los requisitos de seguridad y el alineamiento continuo con los objetivos de la organización.

- **Estructura de operación**, que se encarga de implantar las medidas de seguridad identificadas

ANF AC dispone de una política específica "Política de Roles y Responsabilidades" OID 1.3.6.1.4.1.18332.38.1.

8.1. Estructura de supervisión

La estructura de supervisión de la seguridad se encarga de verificar la correcta implantación y operación de los requisitos de seguridad que se hayan establecido, de cara a mantener la alineación con los objetivos y de cumplir con las normas y legislación aplicable.

Forman parte de esta estructura de ALTA DIRECCIÓN de ANF AC:

- La Dirección General. D. Florencio Díaz Vilches
- Responsable de Seguridad. D. Alvaro Díaz Baño
- Director Jurídico. Dª Maria del Carmen Mateo Torena

Las funciones y responsabilidades de cada una de las figuras se describen en los siguientes apartados

8.1.1. Dirección General

La Dirección General manifiesta su compromiso formal con el apoyo a los planes de seguridad que se deriven de la aplicación de esta Política. Dicho apoyo se concretará en:

- proporcionar los recursos humanos y económicos necesarios, dentro de las posibilidades presupuestarias;
- asignar roles y responsabilidades a las personas asociadas a los planes de seguridad;
- apoyar la formación de los recursos humanos implicados en los planes de seguridad para que adquieran el nivel de concienciación y las competencias necesarias;
- velar por el cumplimiento con el Esquema Nacional de Seguridad;
- facilitar las comunicaciones con otras organizaciones en materia de Seguridad de la Información;

- promover la mejora continua en el ámbito de Seguridad de la Información.

El compromiso con el apoyo a los planes se manifiesta con la aprobación formal del presente documento.

8.1.2. Responsable de Seguridad

Es responsable de la definición, coordinación, difusión y verificación de los requisitos de Seguridad de la información en la Organización.

Este Responsable forma parte del Comité de Seguridad, tomando el papel de Presidente del Comité y, por tanto, es el encargado de elevar a dicho Comité los asuntos de interés relacionados con la seguridad de la información, su coordinación y nombramiento.

Sus responsabilidades incluyen:

- Determina en cada momentos los miembros que forman el Comité de Seguridad.
- Convoca y coordina las reuniones del Comité de Seguridad, en el que participará como Secretario.
- Establecer las medidas de seguridad, conforme a las necesidades establecidas por los Responsables de los Servicios y de la Información, del análisis y gestión de riesgos, de la información fruto del análisis de los indicadores implementados, y de las pautas del Anexo II del Esquema Nacional de Seguridad.
- Supervisar el cumplimiento de la Política de Seguridad de la información, así como de sus normas y procedimientos derivados.
- Planificación de los objetivos estratégicos en materia de ciberseguridad. Propondrá a Recursos Humanos los objetivos en materia de ciberseguridad valorables para la promoción y/o retribuciones especiales del personal.
- Coordinar y controlar las medidas de Seguridad de la Información. Junto al Responsable de Sistemas diseñará e implantará los indicadores necesarios para medir la eficacia y eficiencia de las medidas implantadas.
- Mantener un registro de incidentes de seguridad. Investigar y analizar los incidentes de seguridad y verificar el cumplimiento de los protocolos de seguimiento de los mismos, y de la ejecución de las actuaciones que se establezcan a raíz de estos.
- Supervisar y coordinar las crisis (situaciones excepcionales) de ciberseguridad.
- Promover, coordinar y dar soporte a los análisis periódicos de riesgos de seguridad de los Responsables de los Servicios y de la Información. Presentar el resultado de estos análisis al Comité de Seguridad, dentro del plan de Gestión de Riesgos.
- Planificará y coordinará las auditorías internas y externas necesarias para la certificación en el ENS, el SGSI, y otras de interés de la organización. Colaborará con las mismas, y supervisará la implantación de las correcciones que se deriven de las mismas.

- Mantendrá organizada, actualizada y revisada periodicamente la documentación de seguridad, asegurando el acceso a la misma al personal de la organización.

El Responsable de Seguridad de la Información será nombrado por la Dirección General

8.1.3. Director jurídico

Es responsable de la definición, coordinación, verificación y en su caso aprobación de los requisitos legales en la Organización.

Este Responsable forma parte del Comité de Seguridad, tomando el papel de Secretario del Comité y, por tanto, es el encargado de elaborar las actas, someterlas a firma, su archivo y custodia.

Asume la función de Delegado de Protección de Datos (DPD). En su calidad de DPD garantizará que los datos personales se tratan y se protegen conforme al Reglamento General de Protección de Datos (RGPD UE 2016/679) / Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, por lo que trabajará en coordinación con el resto de componentes de la ALTA DIRECCIÓN y Comité de Seguridad.

8.2. Estructura de operación

La estructura de operación de la seguridad debe asumir la administración operativa de la seguridad de los sistemas de información, implantando en dichos sistemas las medidas necesarias para satisfacer los requisitos de seguridad establecidos por la estructura de especificación.

Forman parte de esta estructura:

- Responsable de desarrollo informático y programación. Aramis Rodríguez Blanco
- Responsable de cumplimiento normativo. Pablo Díaz Baño
- Responsable de criptografía. Yulier Nuñez Musa
- Responsable de sistemas. D. Jordi Cabrera Clarissó
- Los usuarios de los sistemas.

Se describen a continuación las funciones y responsabilidades de las figuras asociadas a la estructura de operación.

8.2.1. Responsable de sistemas

Será el Director de Sistemas.

Sus funciones y responsabilidades son:

- Definir, en coordinación con el Responsable de Seguridad de la Información, las especificaciones funcionales de seguridad de los Sistemas de Información de la Organización.
- Garantizar que en el diseño de sistemas de información y redes de comunicaciones se contemplen desde el principio los aspectos necesarios de seguridad de la información en cuanto a disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.
- Revisar que la configuración de seguridad tras la instalación de un sistema nuevo es la adecuada.
- Revisar que la configuración de seguridad tras los cambios en un sistema sigue siendo la adecuada.
- Implantar y verificar el funcionamiento de las medidas de seguridad que resulten de los planes de tratamiento de riesgos o planes de acciones correctivas a raíz de las auditorías de seguridad de la información.
- Verificar el correcto funcionamiento de los indicadores de seguridad de la información.
- Realizar auditorías técnicas periódicas para verificar el funcionamiento de las medidas y cumplimiento de los requisitos de seguridad establecidos. Estas auditorías pueden ser llevadas a cabo por personal interno o externo

8.2.2. Responsable de desarrollo informático y programación

Será el Encargado del Área informatica y de programación.

Sus funciones y responsabilidades son:

- Definir, en coordinación con el Responsable de Seguridad de la Información, las especificaciones funcionales de seguridad de las aplicaciones que se diseñen y desarrollen por el equipo técnico de ANF AC.
- Garantizar que en el diseño de los programasa se contemplen desde el principio los aspectos necesarios de seguridad de la información en cuanto a disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.
- Analizar y decidir las tecnologías y lenguajes de programación en los que se desarrollaran los proyectos.
- Coordinar al equipo técnico de desarrollo.

8.2.3. Responsable de cumplimiento normativo

Desempeña de forma unificada las resposabilidades del Responsable del Servicio y del Responsable de la Seguridad de la Información del ENS.

Sus funciones y responsabilidades son:

- Determinar los requisitos y niveles de seguridad de los servicios prestados y de la información. Con el apoyo, si lo requiere, del Responsable de la Seguridad y del Responsable del Sistema.

- Incluir las especificaciones de seguridad en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.
- Valorar las consecuencias de un impacto negativo sobre la seguridad de los servicios, atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos. Para el desarrollo de esta función contará con el apoyo de la Dirección Jurídica.
- Asistirá a todas las reuniones que se lleven a cabo para el diseño y elaboración de las plataformas tecnológicas de ANF AC.
- Acompañará a los auditores externos para atender sus requerimientos.
- Dirigirá las auditorias internas.

8.2.4. Responsable de criptografía

Será el Encargado de supervisar el estado de la técnica en cuanto a seguridad critográfica, y determinar los algoritmos y modo de utilización en los productos y servicios de ANF AC.

8.2.5. Usuarios de los sistemas

Todo el personal y usuarios de los sistemas de información de ANF AC

8.2.5.1. Funciones y obligaciones del personal

Todo el personal de ANF AC que tenga algún tipo de relación con el uso, la gestión, mantenimiento y explotación de la información y de los servicios prestados sobre ella, tiene la obligación de conocer la Política de Seguridad de la Información y cumplirla.

El Comité de Seguridad dispondrá los medios para que esta Política llegue a los interesados y esté permanentemente a su disposición.

Todo este personal deberá asistir a sesiones de concienciación en materia de seguridad, las cuales se establecerán en el plan de formación y concienciación anual.

Las personas con responsabilidad en el uso, la gestión, mantenimiento o explotación de los servicios soportados en las TIC recibirán formación para el manejo seguro de los sistemas, en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

8.2.5.2. Funciones y obligaciones de terceras partes

Las terceras partes que estén relacionadas con la gestión, mantenimiento o explotación de los servicios prestados por ANF AC serán hechos partícipes de esta Política de Seguridad de la Información. Las terceras partes quedarán obligadas al cumplimiento de esta Política y a las normativas que se puedan derivar de ella.

Las terceras partes podrán desarrollar sus propios procedimientos operativos para satisfacer la Política.
Se deberán establecer procedimientos específicos de comunicación de incidencias para que los terceros afectados puedan reportarlas.

El personal de las terceras partes deberá recibir sesiones de concienciación, tal como se exige para el personal propio.

Cuando algún aspecto de esta Política no pueda ser satisfecho por una tercera parte, el Responsable de Seguridad deberá realizar un informe del riesgo en que se incurre. Ese riesgo deberá ser aceptado por el Comité de Seguridad

8.3. Normas que rigen en la estructura organizacional de seguridad de la información

Normas dirigidas a la Dirección General y al conjunto de miembros de la estructura de supervisión:

- La Alta Dirección del ANF AC debe estudiar y, en su caso, aprobar las propuestas normativas que le proponga el Comité de Seguridad.
- La Alta Dirección, en caso de aprobar un nuevo documento del SGSI, dará instrucciones para que el mismo se ponga en conocimiento de todas las partes que tienen autorización de acceso al mismo.
- La Alta Dirección, en caso de aprobar la modificación o supresión de un documento de SGSI, dará instrucciones de informar de la nueva versión a todas las partes que tienen autorización de acceso al mismo.
- La Alta Dirección debe promover activamente una cultura de seguridad de la información en ANF AC, apoyando de forma preferente la elaboración y participación de cursos sobre SGSI.
- La Alta Dirección informará al Comité de Seguridad de:
    - Aspectos relativos la estrategia de negocio de la entidad.
    - Aspectos relativos sobre el conocimiento de mercado, en especial, la competencia.
- La Alta Dirección realizará una estimación de los recursos económicos disponibles para el SGSI.

Normas dirigidas al Director General

- Asume la responsabilidad de asignar los recursos, la infraestructura física y el personal necesario para gestión de la seguridad de la información de la organización.

- Asume la responsabilidad de controlar que se llevan a cabo las decisiones adoptadas por la ALTA DIRECCIÓN.

Normas dirigidas a: COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

- El Comité de Seguridad de la Información debe actualizar y presentar ante la ALTA DIRECCIÓN las Políticas de Seguridad de la Información, la metodología para el análisis de riesgos de seguridad y la metodología para la clasificación de la información, según lo considere pertinente.
- El Comité de Seguridad de la Información debe analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario.
- El Comité de Seguridad asume la responsabilidad de gestionar el desarrollo, revisión y evaluación de la política de seguridad de la información.
- Esta Política se revisará al menos una vez al año, y siempre que se produzca alguna nueva circunstancia que lo aconseje. En su revisión deberá tener en cuenta cuantas novedades afecten a la estrategia de futuro del negocio, condiciones legales, novedades técnicas, e incidencias que se hayan producido.
- En las revisiones que realicé el Comité de Seguridad deberá tener en cuenta lo establecido en el marco legal vigente, las normas técnicas de referencia y recomendaciones publicadas por las organizaciones de referencia de las que es miembro ANF AC, y sobre las que se ha asumido un compromiso de respetar.
- El Comité de Seguridad de la Información debe verificar el cumplimiento de las políticas de seguridad de la información aquí mencionadas.

Normas dirigidas al Responsable de Seguridad

- El Responsable de Seguridad debe liderar la generación de lineamientos para gestionar la seguridad de la información de ANF AC y el establecimiento de controles técnicos, físicos y administrativos derivados de análisis de riesgos de seguridad.
- El Responsable de Seguridad debe validar y monitorear de manera periódica la implantación de los controles de seguridad establecidos.

Normas dirigidas al Responsable de Auditorías internas

- El Responsable de Auditorías Internas debe planear y ejecutar las auditorías internas al Sistema de Gestión de Seguridad de la Información de la entidad a fin de determinar si las políticas, procesos, procedimientos y controles establecidos están conformes con los requerimientos institucionales, requerimientos de seguridad y regulaciones aplicables.
- El Responsable de Auditorias debe ejecutar revisiones totales o parciales de los procesos o áreas que hacen parte del alcance del Sistema de Gestión de Seguridad de la Información, con el fin de verificar la eficacia de las acciones correctivas cuando sean identificadas no conformidades.
- El Responsable de Auditorias debe informar los responsables de las áreas y al Comité de Seguridad los hallazgos de las auditorías.

Normas dirigidas a los Responsables de Desarrollo Informátco y de Sistemas

- El Responsable Tecnología debe asignar las funciones, roles y responsabilidades, a sus empleados para la operación y administración de la plataforma tecnológica la organización. Dichas funciones, roles y responsabilidades deben encontrarse documentadas y apropiadamente segregadas.

Normas dirigidas a: TODOS LOS EMPLEADOS DE LA ORGANIZACIÓN Y TERCEROS COLABORADORES

Los empleados de ANF AC, y las terceras partes que realicen labores en o para la organización, tienen la responsabilidad de cumplir con las políticas, normas, procedimientos y estándares referentes a la seguridad de la información.

8.4. Incumplimientos

El incumplimiento de cualquier obligación o norma reseñada en alguno de estos documentos es calificada por defecto como OBJETIVA. No obstante, será el Comité de Seguridad, en relación a las circunstancias específicas de cada caso, el que determine en última instancia la calificación definitiva.

8.5. Sanciones

Cualquier acción encaminada a reducir o eliminar la eficacia de los controles implementados para garantizar la Seguridad de la Información, para alterar las propiedades de Seguridad de la Información, o para dificultar o impedir la investigación de cualquier violación de la política de Seguridad de la Información y su normativa de desarrollo, será considerada una violación de confianza y podría ser causa de investigación y, en su caso, de las correspondientes acciones disciplinarias o legales contra los responsables.

Las sanciones se clasificarán según establece la Normativa interna de Política de Sanciones Disciplinarias

OID 1.3.6.1.4.1.18332.101.45.34”

8.6. Resolución de conflictos

En caso de conflicto entre los diferentes responsables de información o de servicio que componen la estructura organizativa de la Política de Seguridad de la Información, éste será resuelto por el superior jerárquico de los mismos con la mediación del Responsable de Seguridad de la Información, elevándose para su resolución al Comité de Seguridad de la Información en caso de no llegar a un acuerdo.

En la resolución de estas controversias se tendrán siempre en cuenta las exigencias derivadas de la protección de datos de carácter personal.

8.7 Personal autorizado para transporte de soportes de información

Lista de personal autorizado a transportar de forma recurrente determinados soportes de información:

- Responsable de Seguridad
- Responsable de Sistemas

El Responsable de Seguridad puede otorgar autorizaciones puntuales a otro personal de la organización para transportar soportes de información.

9. Los activos de la Seguridad de la Información

ANF AC posee información que debe ser protegida frente a riesgos y amenazas para asegurar el correcto funcionamiento de su negocio. Este tipo de información es imprescindible para el objetivo de la empresa, es lo que se denomina activo de Seguridad de la Información. Su protección es el objetivo de todo Sistema de Gestión de Seguridad de la Información.

Los activos pueden dividirse en diferentes grupos según su naturaleza. Si seguimos la metodología de Magerit para agrupar activos (utilizada por las AA. PP.), estos son los tipos que encontramos.

1. **Los servicios**, es decir, los procesos de negocio que la organización ofrece al exterior como es la emisión de certificados, time-stamp, respuestas OCSP, etc, o que ofrece con carácter interno, como es el caso de la gestión de nóminas, facturación, etc.
2. **Los datos e información que se manipula dentro de la organización**. Suelen ser el núcleo del sistema, mientras que el resto de activos suelen darle soporte de almacenamiento, manipulación, etcétera.
3. **Aplicaciones de software.**
4. **Equipos informáticos.**
5. **Personal**. Este es el activo principal. Incluye personal interno, subcontratado, de los clientes, etcétera.
6. **Redes de comunicaciones** que dan soporte a la organización para el movimiento de la información. Pueden ser redes propias o subcontratadas a terceros.
7. **Soportes de información**. Los soportes físicos que permiten el almacenamiento de la información durante un largo período de tiempo.
8. **Equipamiento auxiliar** que da soporte a los sistemas de información y que son activos que no se han incluido en ninguno de los otros grupos. Por ejemplo, los equipos de destrucción de documentación o los equipos de climatización.
9. **Instalaciones donde se alojan los sistemas de información**, como oficinas, edificios o vehículos.

Junto a estos activos, hay que tener en cuenta aquellos intangibles como la imagen y la reputación de una empresa. Para proteger los activos de información es necesario conocerlos e identificar cuáles son dentro de la organización. Para ello se ha elaborado un inventario que los identifica y clasifica. Cada activo del inventario incluye, al menos, su descripción, localización y responsable de uso.Análisis y gestión de riesgos de seguridad de la Información

El Sistema de Gestión de Seguridad de la Información ha realizado un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- regularmente, al menos una vez al año,
- cuando cambie la información manejada,
- cuando cambien los servicios prestados,
- cuando ocurra un incidente grave de seguridad,
- cuando se reporten vulnerabilidades graves.

La organización detalla todos los aspectos relativos a este apartado en el documento publicado “Evaluación de Riesgos”.

De forma general cabe destacar:

9.1. Gestión de riesgos

Los servicios e infraestructuras bajo el alcance de la presente Política deberán estar sometidos a un análisis de riesgos para orientar las medidas de protección a minimizar los mismos.

Como metodología base para la realización de los análisis de riesgos se utilizará Magerit.

Se utilizarán, como punto de partida, el catálogo de amenazas de seguridad previsto en la metodología.

El análisis se realizará:

- regularmente, una vez al año.
- cuando haya cambios significativos en la información manejada.
- cuando haya cambios en los servicios esenciales prestados o cambios significativos en las infraestructuras que los soportan.
- cuando ocurra un incidente de seguridad grave.
- cuando se identifiquen amenazas severas que no hubieran sido tenidas en cuenta o vulnerabilidades graves que no estén contrarrestadas por las medidas de protección implantadas.

De acuerdo con la escala de riesgos de la metodología Magerit, el nivel de riesgo deberá situarse por debajo de nivel ALTO para considerarse de forma automática como aceptable (el riesgo residual máximo debe ser MEDIO). Valores de riesgo residual mayores a MEDIO deberán ser aceptados explícitamente por el Comité de Seguridad, previa justificación de la conveniencia de su aceptación.

Para los valores de riesgo residual que no sean aceptables se deberá elaborar el correspondiente Plan de Tratamiento que permita llevar los valores de riesgo a valores aceptables.

9.2. 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)

9.3. 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)

9.4. 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)

9.5. 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 deben 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)

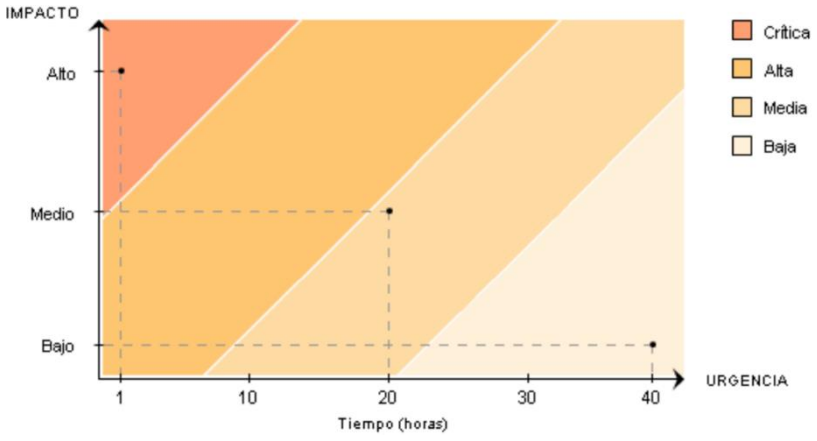
9.6. Gestión de incidencias

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)

DENEGACIÓN DE SERVICIO

Se establecerán medidas preventivas frente a ataques de denegación de servicio y denegación de servicio distribuido (Denial of Service, DoS y Distributed Denial of Service, DDoS). Para ello:

- Se planificará y dotará al sistema de capacidad suficiente para atender con holgura a la carga prevista.
- Se desplegarán tecnologías para prevenir los ataques conocidos.

Detección y reacción.

- Se establecerá un sistema de detección y tratamiento de ataques de denegación de servicio (DoS y DDoS).
- Se establecerán procedimientos de reacción a los ataques, incluyendo la comunicación con el proveedor de comunicaciones.

Ataques propios.

- Se detectará y se evitará el lanzamiento de ataques desde las propias instalaciones perjudicando a terceros.

9.7. 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)

10. 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.

11. Establecimiento, implantación, mantenimiento y mejora del SGSI / ENS

El despliegue del SGSI/ENS se inicia a partir del Análisis de Riesgos, que permitirá determinar el nivel de riesgo de seguridad de la información en que se encuentra la entidad e identificar los controles de seguridad necesarios y oportunidades de mejora para el tratamiento del riesgo y llevarlo a un nivel aceptable, tomando en cuenta el Contexto de la Organización.

Los controles de seguridad deberán implantarse, mantenerse y mejorarse continuamente, y estar disponibles como información documentada que deberá ser revisada y aprobada por el Comité de Seguridad de la Información.

En cumplimiento del Real Decreto del ENS, la presente Política de Seguridad se desarrollará aplicando los siguientes requisitos mínimos para incluirse en la documentación del sistema:

- Organización e implantación del proceso de seguridad.
- Análisis y gestión de los riesgos.
- Gestión de personal.
- Profesionalidad.
- Autorización y control de los accesos.
- Protección de las instalaciones.
- Adquisición de productos.
- Seguridad por defecto.
- Integridad y actualización del sistema.
- Protección de la información almacenada y en tránsito.
- Prevención ante otros sistemas de información interconectados.
- Registro de actividad.
- Incidentes de seguridad.
- Continuidad de la actividad.
- Mejora continua del proceso de seguridad

Además de aplicar los requisitos de la Norma UNE ISO/IEC 27001 y del propio Real Decreto 311/2022 como tal, se deberán utilizar las Guías CCN-STIC de Seguridad que son las normas, instrucciones, guías y recomendaciones desarrolladas por el Centro Criptológico Nacional con el fin de mejorar el grado de seguridad de las organizaciones, especialmente la Serie CCN-STIC-800 que establece las políticas y procedimientos adecuados para la implementación de las medidas contempladas en el ENS, así como el Código de Prácticas para los Controles de Seguridad de la Información UNE ISO/IEC 27002 en el SGSI.

Se deberá comunicar la información documentada de los controles de seguridad al personal que trabaja en la entidad (personal interno y externo), que tendrá la obligación de aplicarla en la realización de sus actividades laborales, comprometiéndose de este modo, al cumplimiento de los requisitos del SGSI/ENS.

La información documentada será clasificada en: pública, interna y confidencial, dando el uso adecuado de acuerdo con dicha clasificación y según el criterio que se establezca en el Procedimiento de Clasificación, Etiquetado y Protección de la Información.

Se realizarán auditorías que revisen y verifiquen el cumplimiento del SGSI/ENS con los requisitos de la Norma UNE ISO/IEC 27001 para el SGSI y con el Real Decreto 311/2022, de 3 de mayo por el que se regula el Esquema

Nacional de Seguridad, por lo que el personal afectado por el alcance de dichas auditorías deberá ser colaborativo para la eficacia de las mismas, así como en la aplicación de las acciones correctivas que se deriven para el mejoramiento continuo.

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

Dimensionamiento / gestión de la capacidad

Para cada proyecto y para atender la infraestructura básica de la organización, se deben tener en cuenta:

- Necesidades de procesamiento.
- Necesidades de almacenamiento de información: durante su procesamiento y durante el periodo que deba retenerse.
- Necesidades de comunicación.
- Necesidades de personal: cantidad y cualificación profesional.
- Necesidades de instalaciones y medios auxiliares.
- Mejora continua de la gestión de la capacidad.

En nuevos proyectos, con carácter previo a la puesta en explotación, se realizará un estudio que determine las necesidades en cada uno de los parámeros anteriormente reseñados.

Se realizará una previsión de la capacidad y se mantendrá actualizada durante todo el ciclo de vida del sistema

13.1 Responsabilidad

El Responsable de Desarrollo y Tecnología, debe efectuar el monitoreo del lenguaje de desarrollo, previsiòn de consumo de memoria RAN, disco duro, y procesamiento. Así como las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas, a fin de garantizar un procesamiento y almacenamiento adecuados

El Responsable de Sistemas determinará 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)

Los Responsables de de Desarrollo 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.

13.2 Responsabilidad Criptográfica

Aquellas áreas que utilizan criptografía, se contará con la supervisión del Responsable de Cumplimiento Normativo.

14. Datos de carácter personal

ANF AC aplicará los principios incluidos en el RGPD cuando realice tratamientos datos de carácter personal: ANF AC cuenta con una Política de Privacidad y recomendamos encarecidamente su lectura, https://anf.es/politica-de-privacidad/

De forma resumida informamos a continuación sobre los principales elementos de su interés,

- Principio de "licitud, transparencia y lealtad": los datos deberán ser tratados de manera lícita, leal y transparente para el interesado.
- Principio de "limitación de la finalidad": implica, por una parte, la obligación de que los datos sean tratados con una o varias finalidades determinadas, explícitas y legítimas y, por otra, que se prohíbe que los datos recogidos con unos fines determinados, explícitos y legítimos sean tratados posteriormente de una manera incompatible con esos fines.
- Principio de "minimización de datos": solo se recogerá datos de carácter personal cuando sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
- Principio de "exactitud": los datos deben ser exactos y, si fuera preciso, actualizados, debiendo adoptarse por parte de ANF AC, todas las medidas razonables para que se rectifiquen o supriman los datos inexactos en relación a los fines que se persiguen.
- Principio de "limitación del plazo de conservación": solo pueden tratarse los datos adecuados, pertinentes y necesarios para una finalidad, la conservación de esos datos debe limitarse en el tiempo al logro de los fines que el tratamiento persigue. Una vez que esas finalidades se han alcanzado, los datos deben ser borrados o, al menos, desprovistos de todo elemento que permita identificar a los interesados.
- Principio de "integridad y confidencialidad": obligación de actuar proactivamente con el objetivo de proteger los datos que manejan frente a cualquier riesgo que amenace su seguridad.
- Principio de "responsabilidad proactiva": implica aplicar por parte de ANF AC las medidas técnicas y organizativas apropiadas para garantizar y estar en condiciones de demostrar que el tratamiento de datos personales se lleva a cabo de conformidad con el RGPD.

ANF AC aplicará medidas de seguridad para garantizar el derecho fundamental a la protección de datos garantizando la confidencialidad, la integridad y la disponibilidad de los datos personales. Para garantizar estos tres factores de la seguridad se aplicarán las medidas de seguridad necesarias adecuadas al nivel de los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas conforme al artículo 32 del RGPD.

En relación con las medidas de seguridad en el ámbito del sector público, ANF AC cumplirá con la disposición adicional primera de la LOPDyGDD, que se señala que los responsables enumerados en el artículo 77.1 de la citada ley orgánica, entre los que se encuentran las fundaciones del sector público como ANF AC, deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado.

ANF AC dispone de un Registro de Actividades del Tratamiento de datos de carácter personal que incluirá los contenidos regulados en el artículo 30 del RGPD.

15. Organización de la Seguridad

15.1. Políticas y documentos publicados

El detalle de todos los documentos publicados y aprobados por la organización, explicación resumida del objetivo de cada uno de ellos y referencias normativas, se detalla en el documento "Alcance y estructura documental del Sistema de Gestión de Seguridad de la Información" OID 1.3.6.1.4.1.18332.101.79.1 del cual forma parte este documento.

Esta Política de Seguridad de la Información se desarrollará mediante la elaboración de otras políticas o normativas de seguridad que aborden aspectos específicos. A raíz de dichas políticas y normativas se podrán desarrollar procedimientos que describan la forma de llevarlas a cabo.L a Política de Seguridad de la Información es de obligado cumplimiento y se estructura en los siguientes niveles relacionados jerárquicamente:

Primer nivel:	Política de Seguridad de la Información.
Segundo nivel:	Normativas de Seguridad de la Información.
Tercer nivel:	Procedimientos e Instrucciones Técnicas de Seguridad de la Información.
Cuarto nivel:	Informes, registros y evidencias electrónicas.

Otra documentación

Se podrá seguir en todo momento los procedimientos, normas e instrucciones técnicas STIC, así como las guías CCN-STIC Revisión y aprobación

Revisión y aprobación

Este documento y el conjunto de documentos elaborados y aprobados por ANF AC, son revisados al menos cada dos años, o cuando los acontecimientos determinen la conveniencia de revisión.

La presente Política de Seguridad de la Información fue aprobada por la Dirección General de las series 400, 500, 600 y 800.