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 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

ÍNDICE

Compromiso de la dirección de ANF AC

ANF AC, como prestador cualificado de servicios de confianza, y productor de elementos y servicios de seguridad, considera los sistemas TIC (Tecnologías de la Información y Comunicaciones) y la Seguridad de la Información que maneja en el desarrollo de su actividad un elemento clave para el cumplimiento de sus objetivos estratégicos.

La Dirección 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, apoya, con total firmeza y convencimiento, los requerimientos planteados en esta Política de Seguridad de la Información, y 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 para garantizar su idoneidad, adecuación y eficacia continuas.

Cualquier cambio que tenga un impacto en el nivel de seguridad brindado deberá ser aprobado por la Junta Rectora de la PKI.

Florencio Díaz Vilches

CEO de 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	1.5.		
OID	1.3.6.1.4.1.18332.101.80.1.		
Fecha de aprobación	01/02/2022	**Fecha de publicación**	01/02/2022

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
1.5.	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 objetivo 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 pautas de actuación en el caso de incidentes y define las responsabilidades.

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

El documento delimita qué se tiene que proteger, de quién y por qué. Debe explicar qué es lo que está permitido y qué no; determina los límites del comportamiento aceptable y cuál es la respuesta si estos se sobrepasan; e identificar los riesgos a los que está sometida la organización.

Con el fin de que esta Política de Seguridad sea un documento de utilidad en la organización y cumpla con lo establecido en la norma UNE-ISO/IEC 27001:2013 se han contemplado los siguientes requisitos:

- Está redactado de manera accesible para todo el personal de la organización. Por lo tanto, preciso y de fácil comprensión.
- Está aprobado por la Junta Rectora de la PKI a propuesta del Comité de Seguridad, y publicitado por el Responsable de Seguridad.
- Es de dominio público dentro de la organización, y está disponible para su consulta siempre que sea necesario.
- Debe ser la referencia para la resolución de conflictos y otras cuestiones relativas a la seguridad de la organización.

- Debe definir responsabilidades teniendo en cuenta que éstas van asociadas a lo que establezca en cada momento el Comité de Seguridad. El cual en función de las responsabilidades decidirá quién está autorizado a acceder a qué tipo de información.
- Se establece que los activos a proteger de la organización son:
    - el personal
    - la información, así como su
    - reputación y continuidad.
- Señala las normas y reglas que deben de ser adoptadas y las medidas de seguridad necesarias.

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:

- **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)***

La Infraestructura de Clave Pública (PKI) y los servicios prestados por ANF AC siguen las directrices del Reglamento [UE] 910/2014, de 23 de julio de 2014, del Parlamento Europeo y del Consejo (en adelante "eIDAS"), y la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

5. Misión

ANF AC en su calidad de Prestador Cualificado de Servicios de Confianza, administra una infraestructura de claves públicas con objeto de prestar los siguientes servicios cualificados:

- **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.

6. 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.

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

Normas dirigidas a: ALTA DIRECCION / Junta Rectora de la PKI

- La Alta Dirección del ANF AC debe estudiar y, en su caso, aprobar las propuestas normativas sobre el SGSI 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 a: Junta Rectora de la PKI y al CEO

- La Alta Dirección y CEO del ANF AC, deben asignar los recursos, la infraestructura física y el personal necesario para gestión de la seguridad de la información de la organización.
- El CEO asume la responsabilidad ejecutiva de llevar a cabo las decisiones adoptadas por la Junta Rectora de la PKI.

Normas dirigidas a: COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

- El Comité de Seguridad de la Información debe actualizar y presentar ante la Junta Directiva 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 al Responsable Tecnología 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

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.

6.2. 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.

6.3. 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 ANF AC.

7. 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.

8. Organización de la Seguridad

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

8.1. Organización de Seguridad: Funciones y Responsabilidades

Junta Rectora de la PKI	Es el grupo de alta dirección encargado de analizar y en su caso aprobar la estrategia de seguridad y continuidad de la información para la compañía, analizar y aprobar las políticas de seguridad de la información, establecer las prioridades para el desarrollo de proyectos de seguridad, y valorar los informes que le son sometidos a estudio sobre la implantación y la efectividad de las medidas adoptadas.
Equipo de Dirección	Es el grupo de Dirección encargado de gestionar y administrar los SGSI.
Comité de Seguridad	Es el grupo encargado de definir y proponer la estrategia de seguridad y continuidad de la información para la compañía, definir y proponer las políticas de seguridad de la información, elaborar y presentar los proyectos de seguridad, controlar su desarrollo, y revisar la implantación y la efectividad de las medidas adoptadas, emitiendo los informes correspondientes.
Responsables de Departamento	Es el grupo encargado de definir y proponer la estrategia de seguridad y continuidad de la información
Empleados	Personal adscrito a la plantilla de trabajadores de ANF AC que participa directamente en el sistema de gestión de seguridad de la información de ANF AC.
Empleados de terceros	Personal adscrito a la plantilla de trabajadores de las empresas contratadas por ANF AC, y que asumen el sistema de gestión de seguridad de la información de ANF AC.

8.2. 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” del cual forma parte este documento.

9. Datos de carácter personal

ANF AC trata datos de carácter personal. Los documentos que conforman el Sistema de Gestión de Seguridad de la Información, solo serán accesibles a las personas autorizadas. Todos los sistemas de información de ANF AC se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad.

ANF AC protege sus ficheros de datos de carácter personal de acuerdo con lo previsto en la Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, y 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)**.

10. 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:

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

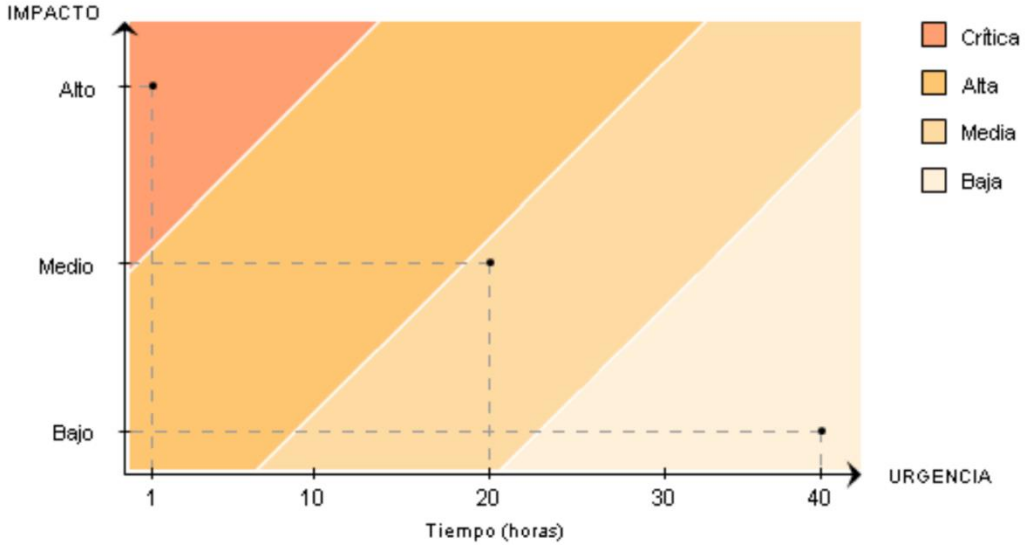
Posibles incidentes o eventos, que serán inexcusablemente registrados (esta lista no debe entenderse como Limitativa, sino que podrá ser ampliada con cualquier otro tipo de incidencias que hubiera quedado omitida, Y EN ESPECIAL primando la prudencia de notificar hasta la mera sospecha de anomalía en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