Manual de Calidad y SGSI

Sede corporativa: Paseo de la Castellana, 79 - 28046 – Madrid
Administración y Servicios jurídicos: G.V. Corts Catalanes, 996 -08018 - Barcelona
Teléfono: 902 902 172 (Llamadas desde España) - Internacional (+34) 933 935 946
Fax: (+34) 933 031 611 · Web: www.anf.es

Nivel de Seguridad

PÚBLICO

Aviso Importante

Control del documento

Versión	1.3
Autor	Moisés Amador
Fecha de Creación	15/04/13

Control de Modificaciones

Fecha	Modificado por	Razón
26/06/2013	Moisés Amador	Ampliación y actualización
10/07/2013	Moisés Amador	Actualización listado documentos y organigrama
03/09/2018	MariCarmen Mateo	Actualización

Control de Aprobación

Fecha	Responsable	Comentarios
26/06/2013	Florencio Díaz	Aprobado
10/07/2013	Florencio Díaz	Aprobado
03/09/2018	Florencio Díaz	Aprobado

Índice

1 Presentación de ANF AC 6

1.1 Entidad jurídica 7

1.2 Financiación 7

1.3 Subcontratación 7

1.4 Acreditaciones 8

2 Objetivo 10

2.1 Alcance y exclusiones 10

2.2 Referencias normativas 11

3 Procesos administrativos 12

4 Flujos del SGCSI ..... ¡Error! Marcador no definido.

5 Responsabilidad de la alta dirección de ANF AC 17

5.1 Requerimientos de documentación 18

5.1 Compromiso 18

5.2 Asignación de recursos 18

5.3 Formación 19

5.4 Declaración de imparcialidad 18

5.5 Compromiso de confidencialidad 19

6 Definición, implementación y operación 19

6.1 Política de calidad de ANF AC 19

6.2 Código de conducta 20

6.3 Política de privacidad 20

6.4 Garantía de productos y servicios 20

6.5 Política de seguridad de ANF 21

6.6 Organización de la seguridad de la información 21

6.7 Gestión de activos 22

6.8 Seguridad de los recursos humanos 22

6.9 Seguridad Física y Ambiental 22

6.10 Comunicaciones y Operaciones 24

6.11 Control de Acceso 24

6.12 Adquisición, desarrollo y mantenimiento de los sistemas de información 25

6.13 Gestión de incidentes 25

6.14 Continuidad del negocio 25

6.15 Cumplimiento 26

6.16 Análisis de riesgos 26

6.17 Declaración de aplicabilidad 26

7 Control y revisión 27
7.1 Satisfacción del cliente 27
7.2 Auditorías Internas..... 27
7.3 Seguimiento y medición de los procesos y del producto. Indicadores. 27
7.4 Control de las incidencias..... 27
7.5 Revisión por la alta direcció de ANF AC 27

8 Mantenimiento y mejora 29

1 Presentación de ANF AC

ANF Autoridad de Certificación (ANF AC - 1997), nace en el seno de la Asociación Nacional de Fabricantes de España (ANF – 1980). Inicialmente como División de I+D+i especializada en criptografía y seguridad informática, desarrolló toda la plataforma tecnológica que permite a ANF AC desarrollar su actividad como entidad de certificación.

En el año 2000, ANF AC adquirió entidad jurídica propia. Ese mismo año se notificó al Ministerio de Ciencia y Tecnología el inicio de actividad como emisor de certificados de firma electrónica**,** solicitando su inscripción en el registro oficial de autoridades de certificación de acuerdo con la legislación vigente en aquellas fechas.

ANF AC fue la **primera entidad en España** en emitir certificados electrónicos reconocidos. Actualmente ANF AC está oficialmente acreditada como Prestador de Cualificado de Servicios de Confianza, y homologada por toda la administración pública estatal, autonómica y municipal.

Nuestro éxito se debe a una sola causa: la continua inversión en **I+D+i** para dotar a los usuarios de tecnología innovadora. Igualmente, importante es nuestro compromiso con los clientes a la hora de atender sus necesidades, creando **productos y servicios escalables e interoperables** para cualquier sector.

ANF AC, en todas sus líneas de productos y servicios, asume el compromiso de utilizar la más avanzada tecnología y desarrollar todos los elementos necesarios para su puesta en explotación. ANF AC no utiliza software de terceros, garantiza total control y soporte desde origen.

ANF AC fue pionera en ofrecer de forma estándar en todos sus dispositivos homologados, firmas con **sello de tiempo** y **validación en origen**.

ANF AC dispone de filiales propias en Malta, Ecuador, Perú, Cuba, EE.UU. y Hong Kong.

ANF AC tiene asignado el código privado de empresa (SMI Network Management Private Enterprise Code) 18332 por la organización internacional IANA, (Internet Assigned Numbers Authority), bajo la rama iso.org.dod.internet.private.enterprise (1.3.6.1.4.1 -IANA –Registered Private Enterprise-).

ANF AC está comprometida con el Pacto Mundial de Naciones Unidas (Global Compact), forma parte de la organización de España desde el año 2013. La Junta Rectora de ANF AC está comprometida con los principios diez principios que engloban un compromiso social empresarial sobre Derechos Humanos, Ámbito Laboral, Medio Ambiente, Anti-Corrupción. Para su seguimiento y cumplimiento sigue las directrices de la ISO 26000.

ANF AC, declaramos en todas nuestras actuaciones como valores corporativos:

- Honestidad, integridad, transparencia, independencia, imparcialidad, confidencialidad, y profesionalidad.

- Confianza en los servicios de ANF AC, mediante mecanismos de certificación realizados por auditores independientes contra normas y estándares de reconocimiento internacional.

ANF AC, sigue y respeta la filosofía empresarial del Triple Balance, en el cual la rentabilidad es uno más de los objetivos que tiene que perseguir la actividad empresarial, junto con la sostenibilidad y el compromiso social. ANF AC solo interviene en áreas que puedan tener una relación con los servicios de certificación, que presupongan una mejora competitiva para la organización mediante la incorporación de elementos claramente diferenciales. Además, debe de aportar mejoras para la sociedad y presuponer una novedad en el mercado.

1.1 Entidad jurídica

ANF Autoridad de Certificación, (en adelante ANF AC), es una entidad jurídica, constituida al amparo de la Ley Orgánica 1/2002 de 22 de marzo e inscrita en el Ministerio del Interior con el número nacional 171.443 y CIF G-63287510.

1.2 Financiación

ANF AC, se financia con recursos propios generados por las actividades que desarrolla.

ANF AC, responde con todo su patrimonio para hacer frente a las posibles responsabilidades legales como indican las normas, dispone con Pólizas de RC que garantizan su responsabilidad de acuerdo con la legislación vigente:

- Aseguradora: CFC Underwriting Limited (Lloyd's de Londres).
- Ramo: Responsabilidad Civil Profesional.
- Cobertura asegurada: Cinco millones de euros (5.000.000 €).
- Número de Póliza: BA 059760 A.

ANF AC, es una organización con una experiencia empresarial de más de quince años. Durante todo este periodo de tiempo, ANF AC no ha tenido incidencia alguna. ANF AC garantiza una estabilidad financiera, cuenta con recursos financieros suficientes para hacer frente a sus compromisos a largo plazo. Sus presupuestos son coherentes y todo su desarrollo de negocio se basa en recursos propios.

ANF AC, dispone de diferentes filiales, todas ellas son entidades jurídicas independientes en las que ANF AC no asume compromisos financieros de relevancia.

La Junta Rectora de ANF AC es el órgano responsable de garantizar la estabilidad financiera de la entidad.

1.3 Subcontratación

ANF AC, no tiene contratistas en los términos definidos por la norma ISO 17024.

1.4 Acreditaciones

ANF Autoridad de Certificación esta oficialmente reconocido por el Ministerio de Industria, Comercio y Turismo como Prestador Cualificado de Servicios de Confianza en las áreas en la que presta sus servicios:

- Certificados Cualificados de Firma Electrónica
- Certificados Cualificados de Sello Electrónico
- Sellos Cualificados de Tiempo Electrónico
- Certificados de Web Segura SSL
- Dispositivos Cualificados de Firma Electrónica (*Resolución Ministerio y certificaciones de conformidad ISO 15408 Common Criteria EAL 4+ y 5+*)
- Servicio de Validación de Firma Electrónica (*en trámite, cuanta con auditoria conformidad*)
- Servicio de Validación de Sellos Electrónicos (*en trámite, cuanta con auditoria conformidad*)

Auditoria de Conformidad ISO 27001

Aplicada a la Prestación de Servicios de Certificación de Firma Electrónica.

Auditor: GUARDIAN

Auditoria de Conformidad ISO 9001

Auditor: Sistema de Gestión de la Calidad (SGC)

Auditoria Normas ETSI

Servicio	EN general	EN de alcance	Perfil/semántica
Creación, verificación y validación de firmas electrónicas.	EN 319 401	EN 319 411-1 EN 319 411-2	EN 319 412-1 EN 319 412-2 EN 319 412-3 EN 319 412-4 EN 319 412-5
La creación, verificación y validación de sellos electrónicos.	EN 319 401	EN 319 411-1 EN 319 411-2	EN 319 412-3
La creación, verificación y validación de sellos de tiempo electrónicos.	EN 319 401	EN 319 421	EN 319 422

Auditor: CSQA Italia

ISO 17024 - Esquema de Certificación AEPD-DPD

En trámite. Autorización provisional de la Agencia Española de Protección de Datos

1.5 Estructura organizativa

La Junta Rectora de ANF AC es el órgano de administración de la entidad en el sentido que establece la norma ISO 17024. Existe un Presidente de la Junta Rectora que es el factor mercantil de la organización, el cual a su vez asume las funciones de Director General, al frente de la Dirección Ejecutiva, con la responsabilidad máxima en la toma de decisiones de certificación.

También forma parte de la Dirección Ejecutiva, el Director Jurídico con funciones asesoras en la adopción de decisiones por parte del Director General.

Se ha creado un órgano consultivo denominado **"Comité de Expertos",** igualmente denominado Comité de imparcialidad, donde queda garantizada la participación de todas las partes implicadas en el proceso de certificación de personas. Su función es tutelar la independencia e imparcialidad del órgano de gobierno de ANF AC, en sus decisiones en relación con la certificación en todos los ámbitos de actuación. También realiza funciones de resolución de apelación, para el caso de que el candidato recurra la revisión de examen realizada por el Evaluador, u otras decisiones sobre la certificación.

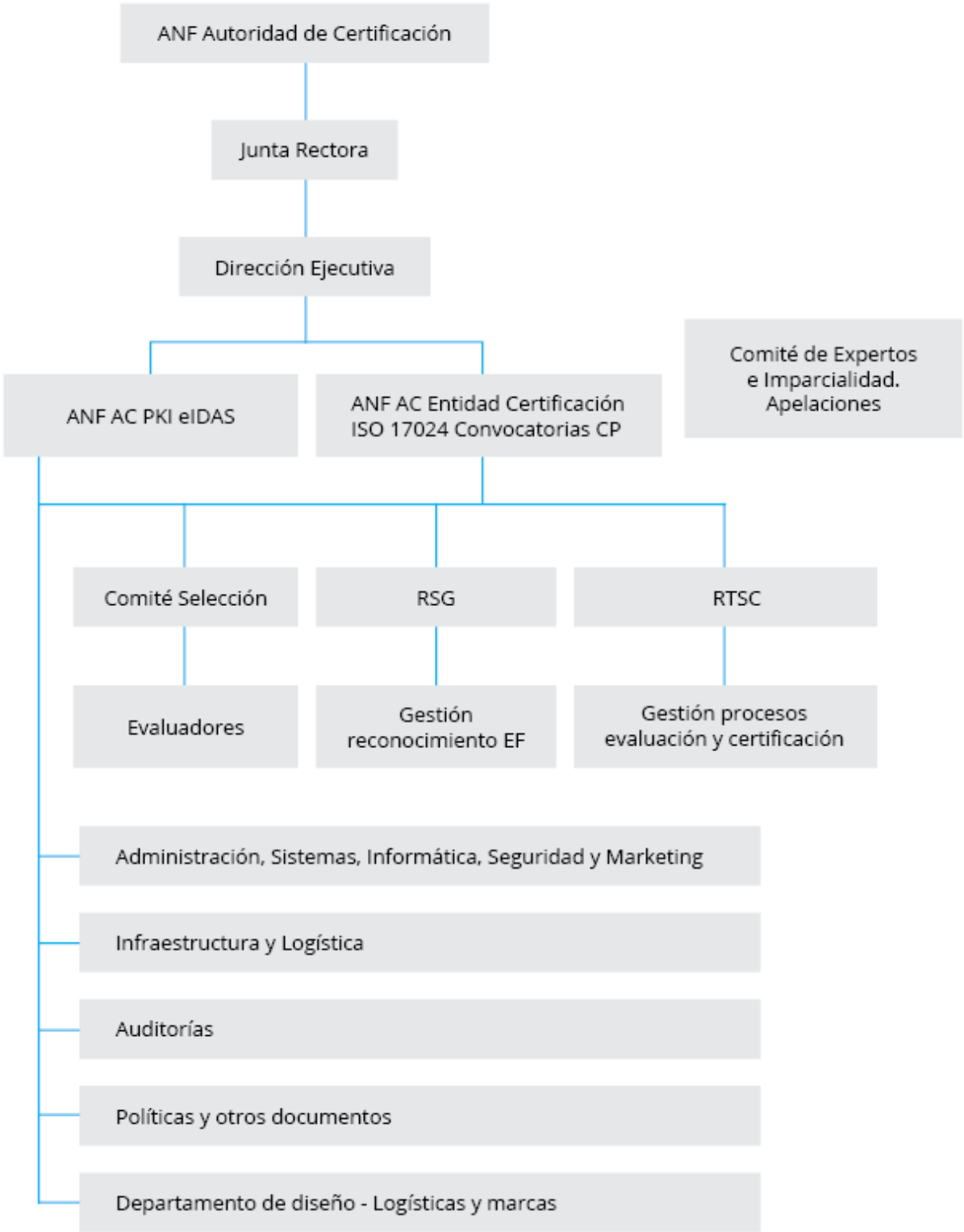
En los casos en los que pueda haber un conflicto de intereses, oído el Comité de Expertos, se decidirá, sobre si procede recusación.

Los requisitos de los puestos de trabajo, funciones y responsabilidades están definidos en un documento interno, que se complementa con las descritas en los procedimientos e instrucciones del sistema de certificación.

No existen Organismos Relacionados en los términos definidos en las norma ISO 17024 que puedan comprometer su independencia e imparcialidad.

Recae sobre la Dirección Jurídica de ANF AC la función de Delegado de Protección de Datos y, en coordinación con la Dirección General, la de *Compliance Officer*.

Seguidamente se refleja el organigrama de la estructura organizativa de ANF AC.


ANF Autoridad de Certificación
Junta Rectora
Dirección Ejecutiva
ANF AC PKI eIDAS
ANF AC Entidad Certificación ISO 17024 Convocatorias CP
Comité de Expertos e Imparcialidad. Apelaciones
Comité Selección
RSG
RTSC
Evaluadores
Gestión reconocimiento EF
Gestión procesos evaluación y certificación
Administración, Sistemas, Informática, Seguridad y Marketing
Infraestructura y Logística
Auditorías
Políticas y otros documentos
Departamento de diseño - Logísticas y marcas

2 Objetivo

ANF ha establecido un Sistema de Gestión de Calidad y de Seguridad de la Información (en adelante, SGCSI) basado en la norma ISO 9001 y en la norma ISO/IEC 27001 con el objetivo de establecer un proceso de mejora continua de la calidad y la seguridad de la información.

Este documento establece las medidas de seguridad de carácter general, dirigidas a asegurar la integridad, disponibilidad, control de accesos de personas autorizadas y conservación de la información. Además, establece la Política de Calidad de ANF AC.

Estados fundamentales de la información: transmisión, recepción, almacenamiento y publicación. La información debe de protegerse adecuadamente cualquiera que sea la forma que tome o los medios que se utilicen en dichos estados.

Asimismo, la información posee las siguientes características relacionadas con la seguridad:

- Confidencialidad: característica que previene contra la puesta a disposición, comunicación y divulgación de información a individuos, entidades o procesos no autorizados.

- Integridad: característica que asegura que la información no se ha transformado ni modificado de forma no autorizada durante su procesamiento, transporte o almacenamiento, detectando fácilmente posibles modificaciones que pudieran haberse producido.

- Disponibilidad: característica que asegura que los usuarios autorizados tienen acceso a la información cuando se requiera y previene contra intentos de denegar el uso autorizado a la misma.

- Autenticidad: característica por la que se garantiza la identidad del usuario que origina una información. Permite conocer con certeza quién envía o genera una información específica.

- Conservación de la información: en un sentido amplio, es el conjunto de procesos y operaciones que se conjugan para estabilizar y proteger los documentos del deterioro. A la hora de hablar de la gestión de recursos digitales, sea cual sea su forma o función, se debe tener en cuenta todas las etapas que componen el ciclo de vida de los documentos para aplicar las medidas de preservación los antes posible. Por lo tanto, más que a una característica intrínseca de la información se hace referencia a la gestión del ciclo de vida de la información.

- Trazabilidad: característica de la información que asegura el conocimiento de aspectos clave de las operaciones de creación, modificación y consulta, tales como: ¿quién realizó la operación?, ¿cuándo se realizó la operación?, ¿qué resultados tuvo la operación?

La seguridad de la información requiere un enfoque preventivo y adaptado a la dinámica de uso de la información generada. Sólo de esta manera se conseguirá preservar la información salvaguardando las garantías descritas, y cumpliendo las leyes que afectan al tratamiento de datos.

2.6 Alcance y exclusiones

El ámbito de aplicación del presente documento alcanza:

- Los productos y servicios comercializados por ANF AC, en todas sus áreas de actividad.

- Las aplicaciones, infraestructura y componentes tecnológicos (elementos de red, servicios, equipos de usuario, periféricos), necesarios para el desarrollo de la actividad.

- La información tratada, es decir, toda la información que recoge, custodia o crea el personal de ANF AC, en cualquier tipo de soporte o estado.

- Procesos organizativos referentes al uso de las aplicaciones.

2.7 Referencias normativas

El presente documento ha sido elaborado teniendo en cuenta el cumplimiento de las siguientes normas legales y técnicas aplicables a la actividad desarrollada por la organización:

NORMAS LEGALES

- **Reglamento (UE) 910/2014 de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.**

- **Ley 59/2003, de 19 de diciembre, de firma electrónica.**

- **Reglamento (UE) 679/2016 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.**

- **Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.**

- **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, de protección de datos de carácter personal.**

- **Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI).**

NORMAS TÉCNICAS

- **ISO/IEC 27001**

- **ISO 9001**

- **ISO 17024**

- **Normas ETSI – Servicios de Confianza**

3 Procesos administrativos

Procesos administrativos de ANF AC, requerimientos generales:

I. Proceso de solicitud y trámite del servicio o producto

1. Solo es posible realizar solicitudes de servicio en:
    a. Puntos oficialmente acreditados por ANF AC. Estos puntos cuentan con plafón acreditativo en lugar visible y están publicados en la Web corporativa de anf.es
    b. Servicio en linea en la Web corporativa de anf.es, con protocolo de comunicación SSL O TLS.
2. Los solicitantes tienen que identificarse mediante documento legal vigente. Con carácter general:
    a. De forma presencial mediante: DNI, pasaporte o tarjeta de residencia. Siempre con fotografía que permita reconocer al titular.
    b. De forma electrónica: mediante el empleo de certificado electrónico reconocido.

3. Los solicitantes tienen que determinar el servicio o producto, ANF AC asume la responsabilidad:
    a. Comprobar la adecuación del servicio o producto respecto al solicitante.
    b. Informar de forma clara y precisa el alcance y limitaciones del servicio o producto.
    c. Establecer el precio del servicio.
    d. Documentar las características del servicio o producto.
    e. Facilitar documento normalizado para formalizar la solicitud. La normalización de un documento como mínimo requiere:
        i. Estar personalizado con el membrete de ANF AC.
        ii. Disponer de un código OID que lo identifique de forma unívoca en la relación e documentos publicados por ANF AC.
        iii. Cuando el tipo de documento lo precise, además deberá:
            1. Contar con un control de versión.
            2. Establecer un rango de seguridad.
            3. Autor y fecha de aprobación.

4. Los solicitantes tienen que aceptar formalmente las solicitudes de servicio o producto. Este trámite pueden realizarlo:
    a. De forma presencial: firma manuscrita o poder notarial suficiente.
    b. De forma electrónica: firma electronica reconocida de acuerdo con la legislación vigente se requiere:
        i. La firma debe de haber sido elaborada con un certificado cualificado de firma electrónica.
        ii. La firma debe de haber sido generada con un dispositivo cualificado de creación de firma electrónica.
        iii. El emisor del certifciado debe de disponer y facilitar a los terceros que confían, de un dispositivo de validación de firmas electrónicas cualificadas que cumpla con lo establecido en el artículo 32 del Reglamento (UE) 910/2014.

iv. La firma electrónica debe permitir su conservación a largo plazo, para ello se requieren firmas AdES LTV de acuerdo con la norma de referencia ETSI según formato XAdES, CAdES o PAdES.

5. Los solicitantes tienen el derecho y ANF AC la obligación, de facilitar previa a la aceptación formal de documentos:
    a. Leer el contenido de los documentos a los que se requiere su adhesión.
    b. Recibir asesoramiento de cuantas consultas o dudas puedan tener, ya sean de índole técnico, legal o meramente funcional.
    c. Recibir copia de los documentos que han firmado.
    d. Recibir información de la garantía asociada al servicio o producto.
    e. Disponer de canales y procedimientos que le permitan presentar quejas, reclamaciones o denuncias.

6. ANF AC debe de cumplir con las obligaciones establecidas en la normativa legal, especialmente en materia de protección de datos.

7. ANF AC identifica de forma univoca cada solicitud, otorgando un identificador que permite localizar y auditar cada tramite de solicitud realizado.

8. Cuando la solicitud precise de material cifrado o con control de acceso mediante contraseñas secretas, en especial semillas de certificados electrónicos, ANF AC las comunicará de forma privada y segura, para ello podrá utilizar diferentes medios entre los buzones de confianza que ha comunicado el solicitante o incluso, combinación de ellos, p.ej. correo electrónico, SMS, notificaciones Push, carta, etc.

9. ANF AC no almacena contraseñas de sus clientes, empleando para ello algoritmo de digestión SHA56.

10. Los usuarios de los sistemas en linea de ANF AC, tienen la capacidad de administrar sus contraseñas de acceso, y configurar sus requerimientos de seguridad en credenciales basadas en certificados electrónicos.

11. ANF AC, no interviene en la generación de claves asimétricas RSA, dota de la tecnología necesaria para que cada usuario se genere su par de claves pública y privada.

II. Proceso de renovación de un servicio

1. El usuario, antes de la fecha de caducidad del servicio, es notificado por escrito por ANF AC.
2. ANF AC, facilita información y asesoramiento para realizar una renovación del servicio.
3. ANF AC, informa de forma clara y precisa del precio de renovación del servicio.

III. Proceso de revocación o cancelación de un servicio

1. El usuario dispone de diferentes canales de comunicación y procedimientos para la cancelación anticipada de un servicio.

2. ANF AC, facilita información y soporte que permita a todos los usuarios un cancelación de servicios sin demora injustificada.

3. ANF AC, registrará sin demora injustificada la cancelaciones de servicio que se produzcan, y facilitará a todos los usuarios que lo soliciten, comprobante de revocación o cancelación.

IV. Proceso de tratamiento de las incidencias de usuarios

1. Recepción de la incidencia:

    a. Si la incidencia es atendida telefónicamente la incidencia es grabada en un archivo mp3 que será adjuntado al ticket de la incidencia. Requerimientos:
        i. Se informará a todo usuario que se va a realizar una grabación por motivos de seguridad y calidad del servicio.
        ii. Cada incidencia es registrada con un identificador unívoco asociado a un ticket de incidencia.

    b. Si la incidencia es atendida por cualquier otro medio se genera directamente el ticket de la incidencia, que debe de disponer de un identificador unívoco.

    c. Cada identificador debe permitir la localización del ticket asociado.

2. Al ticket de la incidencia se le asigna:
   Una tipología, nivel de gravedad/urgencia, datos de contacto, archivo mp3 (si lo hubiera), cualquier otro archivo referente a la incidencia, explicación de la incidencia, y un agente que atenderá la incidencia.

3. La incidencia es tratada por la persona asignada.

4.- Resuelta la incidencia, se cierra la incidencia con información de la resolución aplicada.

5.- Siempre que sea posible, los usuarios tendrán acceso en linea a los expedientes de tramitación de incidencias.

.

V. Proceso de validación de un servicio

1. Cada solicitud de servicio es verificada por operador especializado en el servicio requerido.

2. Cada solicitud debe de recibir la confirmación formal de un operador responsable.

3. ANF AC, dispone de procediiento formal para aceptar, denegar, o solicitar ampliación documental a los usuarios. Las decisiones que se adoptan son comunicadas por escrito a los interesados.

4. Los interesados disponen de canales de comunicación y procedimientos para recurrir aquellas decisiones que consideran contrarias a la normativa.

5. Todos los procedimientos tienen establecidos plazos de tiempo, fijando claramente inicio y final.

VI. Proceso de suministro del servicio o producto

1. Cada servicio identifica de forma clara y precisa el momento en que se produce el suministro y la materialización de la prestación de servicio. Estableciendo un plazo que permita al usuario determinar la adecuación del servicio recibido con el servicio que contrató.

2. Cada producto suministrado es entregado de forma segura y estableciendo el momento en que se produce. A partir de ese momento se inicia el periodo de garantía.

3. En aquellos casos en los que el usuario debe de activar el servicio o recoger el producto, se establece como fecha de entrega, a las 24 h. en el que el usuario recibe el comunicado de su puesta a disposición.

4 Flujos del SGCSI

Se identifican los siguientes procedimientos del SGCSI. Cada uno de ellos está documentado con su diagrama de flojo, y dispone de su correspondiente operador.

- Operadores: Contratación, Formación y Control.
- Elaboración, aprobación y administración de la documentación.
- Auditorías internas.
- Nuevos tratamientos de datos**.**
- Proceso inscripción Convocatorias.
- Proceso ejecución Convocatorias.
- Proceso de evaluación.
- Revisiones y apelaciones
- Quejas y reclamaciones
- Proceso de Certificación DPD
- Auditoria AR y EF
- Elaboración, aprobación y administración de la documentación
- Mejora continua SGCSI

5 Responsabilidad de la alta dirección de ANF AC

5.1 Compromiso

La alta dirección de ANF AC ha adquirido el compromiso con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGCSI. Para ello, ha tomado las siguientes iniciativas:

- Establecer una política de calidad y de seguridad de la información.
- Asegurarse de que se establecen objetivos y planes del SGCSI.
- Establecer roles y responsabilidades de calidad y seguridad de la información, así como política de sanciones disciplinarias en caso de incumplimiento.
- Comunicar a la organización tanto la importancia de lograr los objetivos de calidad y de seguridad de la información y de cumplir con la política de calidad y de seguridad, como sus responsabilidades legales y la necesidad de mejora continua.
- Asignar suficientes recursos al SGCSI en todas sus fases.
- Decidir los criterios de aceptación de riesgos y sus correspondientes niveles.
- Asegurar que se realizan auditorías internas.
- Contratar y asegurar que se realizan auditorias por auditores independientes, de alto prestigio contra normas internacionalmente aceptadas.

5.2 Asignación de recursos

Para el correcto desarrollo de todas las actividades relacionadas con el SGCSI, es imprescindible la asignación de recursos. La alta dirección de ANF garantiza que se asignan los recursos suficientes para:

- Establecer, implementar, operar, monitorizar, revisar, mantener y mejorar el SGCSI.
- Garantizar que los procedimientos de calidad y de seguridad de la información apoyan los requerimientos de negocio.
- Identificar y tratar todos los requerimientos legales y normativos, así como las obligaciones contractuales de seguridad.
- Aplicar correctamente todos los controles implementados, manteniendo de esa forma la calidad y la seguridad adecuada.
- Realizar revisiones cuando sea necesario y actuar adecuadamente según los resultados de las mismas.
- Mejorar la eficacia del SGCSI donde sea necesario.

5.3 Formación

ANF AC asegura que todo el personal con responsabilidades en el SGCSI es competente para realizar las tareas requeridas.

Al personal se le proporciona la formación necesaria y se evalúa la efectividad de las acciones tomadas.

Se mantienen los registros de la educación, la formación, las capacidades, la experiencia y las calificaciones del personal de ANF AC implicado en el SGCSI.

Se asegura que cualquier persona que tenga acceso a los activos sepa y acepte sus responsabilidades en materia de seguridad de los sistemas de información y recursos con los que trabaja. La principal garantía a cubrir es la confidencialidad.

Además, también asegura que todo el personal relevante esté concienciado de la importancia de sus actividades de seguridad de la información (incluyendo requerimientos de seguridad y responsabilidades legales) y de cómo contribuye a la consecución de los objetivos del SGCSI.

5.4 Declaración de imparcialidad

La alta dirección, todos los responsables de área y operadores que intervienen en actuaciones de certificación, han suscrito Declaraciones de Imparcialidad.

5.5 Compromisos de confidencialidad

La alta dirección, todos los responsables de área y operadores que intervienen en actuaciones de certificación, han suscrito documentos de compromiso de confidencialidad.

6 Definición, implementación y operación

6.1 Requerimientos de documentación

ANF AC, ha establecido todos los registros y procedimientos documentados requeridos por las normas técnicas de referencia, así como todos los que ha considerado necesarios para evidenciar el cumplimiento de los requisitos de calidad y de seguridad de la información.

A través de su procedimiento de control de documentos y de control de registros define las acciones necesarias para la gestión de los documentos y de los registros. Para su gestión administra el documento denominado "Estructura de OID's de ANF AC" con OID 1.3.6.1.4.1.18332.45.4.1, el cual contiene la relación completa de los documentos publicados por la organización.

ANF AC, dispone de repositorios seguros de documentación.

6.2 Política de calidad de ANF AC

Publicada en la web corporativa de ANF AC, e identificada con el OID 1.3.6.1.4.1.18332.101.40.1

En ANF AC somos conscientes de que las necesidades de nuestros clientes son la medida exacta para la calidad de nuestra atención al público. La satisfacción es la llave para el éxito de nuestra empresa e intentamos lograr que el cliente vuelva a nosotros y no al producto que le suministramos.

Por ello, es nuestra meta primordial cumplir con las exigencias de nuestros clientes en lo que se refiere a la calidad de producto, el servicio diligente, la amabilidad en el trato, el asesoramiento honesto y el fiel cumplimiento del compromiso de suministro libre de errores. Es de mayor importancia para nosotros mejorar en todo a diario e introducir innovaciones como el mejor medio para mantener la fidelidad de nuestros clientes.

Los colaboradores AR Reconocidos y Entidades de Formación reconocida, son el capital más importante de nuestra empresa para lograr el éxito. Asumimos la responsabilidad de darles una formación adecuada, proporcionándoles todas las herramientas y medios de trabajo necesarios además de crear optimas relaciones profesionales con ellos. Cuidamos estos recursos dándoles el importante valor estratégico que tienen.

Tanto como persona individual o como miembro de un equipo somos responsables de nuestros actos y los resultados que provienen de los mismos. Es esencial el conocimiento pleno de las responsabilidades que el puesto implica y de las responsabilidades asumidas por la organización como Prestador Cualificado de Servicios de Certificación, o como Entidad de Certificación de Personas. Cada proceso en el que intervenimos está regulado por unas normas legales y unas normas técnicas que son necesarias conocer y respetar.

El ambiente laboral es un factor primordial para fomentar la comunicación positiva y la dedicación de los trabajadores. Es uno de nuestros objetivos vigilar por la salud y el bienestar de cada uno de ellos. El respeto al sentimiento de realización personal a través de una actividad profesional, es un objetivo prioritario para la Organización.

La suma de inteligencias da lugar a una mayor inteligencia y para lograrlo se hace necesaria la implicación de todas las personas que forman parte de la Organización.

Esto sólo es posible mediante la correcta valoración del esfuerzo, brindando oportunidades de forma equitativa, dotando de la suficiente autonomía para que cada uno pueda percibir el fruto de su trabajo, a la vez que la Organización incentiva prioritariamente el apoyo honesto y transparente entre compañeros, y una visión global de todos los procesos que conforman el servicio que reciben nuestros clientes.

Nuestro objetivo es la excelencia, para lograr este fin es necesario responder a todas las necesidades de nuestros clientes, y analizar y dar respuesta a sus insatisfacciones. Para ello, es necesario incrementar la eficiencia y calidad de nuestros servicios y productos a través de la mejora continua.

6.3 Código de conducta

Publicado en la web corporativa de ANF AC, e identificada con el OID 1.3.6.1.4.1.18332.105.12

6.4 Política de privacidad

Publicada en la web corporativa de ANF AC, e identificada con el OID 1.3.6.1.4.1.18332.101.20.1

6.5 Garantía de productos y servicios

Publicada declaración en la web corporativa de ANF AC,

DECLARACIÓN

ANF AC, así como los fabricantes que integran en sus productos dispositivos o componentes de ANF AC y otros proveedores que lo distribuyen, garantizan que:

El software funciona de forma sustancial de conformidad con lo establecido en los materiales escritos que lo acompañan, durante un período de noventa (90) días a contar desde la fecha de su recepción.

De forma general, el hardware asociado a las soluciones de ANF AC está libre de defectos en el material y en la confección, con un uso y servicio normales, durante un período de un (1) año a contar desde la fecha de su recepción.

El equipamiento entregado en cesión de uso cuenta con una garantía ilimitada. En aquellos equipamientos que incluyen una extensión de garantía, la cobertura atenderá a lo especificado en la misma.

Algunos países no permiten que se establezcan límites a la duración de una garantía tácita, por lo que es posible que la antedicha limitación no sea de aplicación, debiéndose adaptar como máximo a la legislación vigente en cada caso aplicable.

En caso de aplicación de la garantía, la responsabilidad total de ANF AC, la del fabricante de software, la del distribuidor o la de los integradores que lo instalan, y que en su caso ha suministrado los dispositivos de ANF AC, será a opción:

La devolución del precio pagado.

La reparación o sustitución del software o hardware que no se ajuste a la presente Garantía Limitada que le sea devuelto al Fabricante del Software o distribuidor o integrador con copia del recibo de compra.

La presente Garantía Limitada será nula si el software o el hardware fallan como resultado de accidente, abuso, manipulación no autorizada o mala aplicación.

Acreditación en el propio documento de firma del dispositivo seguro de firma empleado para generarla.

Equipamiento sustituido

El software y hardware sustituido estará garantizado durante el resto del período de garantía original o durante treinta (30) días, eligiendo de ambos períodos el que resulte mayor. Queda excluida de esta garantía limitada la devolución del producto por no idoneidad del mismo con las necesidades del usuario.

No hay responsabilidad por daños emergentes

En la máxima medida permitida por la legislación aplicable, ni ANF AC Autoridad de Certificación, ni el Fabricante del Software, ni sus proveedores, ni integradores se responsabilizarán de daños (incluyendo, entre otros, daños directos o indirectos por lesiones a las personas, lucro cesante, interrupción de actividad comercial, pérdida de información comercial o cualquier otra pérdida pecuniaria) que se deriven del uso o incapacidad de usar este producto, incluso si el Fabricante del Software, el proveedor o los integradores han sido informados de la posibilidad de tales daños.

En cualquier caso, toda la responsabilidad del Fabricante sus proveedores o integradores, en virtud de cualquier estipulación de este contrato se limitará a la cantidad efectivamente pagada por usuario por el software y/o el hardware de ANF AC.

Algunos países no permiten la exclusión o límite de responsabilidad respecto a daños emergentes o contingentes, por lo que puede ocurrir que la mencionada limitación no sea de aplicación en ellos.

6.6 Política de seguridad de ANF AC

La política de seguridad es la declaración de alto nivel de objetivos, directrices y compromisos de ANF AC, para acometer la gestión de seguridad de la información en los medios electrónicos, informáticos y telemáticos utilizados en la prestación del servicio. Este marco de seguridad se soportará en un conjunto de medidas, procedimientos y herramientas de seguridad para la protección de activos de información.

ANF AC, dispone de diferentes documentos específicos relativos a la seguridad de la información.

6.7 Organización de la seguridad de la información

ANF AC gestiona la seguridad de la información a través de la aprobación de la política de calidad y de seguridad de la información, asignando los roles de seguridad y coordinando y revisando la implementación de la calidad y seguridad en toda la organización.

También asegura el mantenimiento de la seguridad de los recursos y de los activos de información que son accesibles por externos a través del control de cualquier acceso a la información de ANF y del procesamiento de la información realizado por externos.

ANF AC proporciona unos medios organizativos que permiten iniciar, conseguir y mantener la implantación de los objetivos de calidad y seguridad de la información.

Se realizarán revisiones independientes de las vulnerabilidades existentes, riesgos asociados y controles establecidos.

Además, en el caso de prestación de servicios por parte de terceros, ANF analiza los riesgos existentes y asegura que existe una gestión eficaz de los mismos.

6.8 Gestión de activos

ANF AC asegura una protección adecuada de los activos (incluyendo mantenimiento, inventario y clasificación), identificando a los propietarios de estos activos, cuya responsabilidad es el mantenimiento de los controles adecuados sobre los mismos. Se tienen en cuenta todos los medios y soportes que transmiten, almacenan y procesan información y se realizará una clasificación de los mismos para asegurar que la información recibe un nivel de protección adecuado.

Esta clasificación permitirá indicar la necesidad, prioridades y grado de protección esperado para la información manejada. La gestión de activos tiene especial incidencia sobre la garantía de confidencialidad y es importante hacer constar el deber de los responsables de cumplir con las garantías de seguridad definidas en la introducción: confidencialidad, integridad, disponibilidad, autenticidad y conservación de la información.

ANF elaborará un inventario de los activos de información de las aplicaciones informáticas de que dispone, velando porque exista un responsable para cada uno de los activos.

6.9 Seguridad de los recursos humanos

Cualquier persona de ANF AC que tenga acceso a los activos inventariados dentro del alcance indicado (personal propio y subcontratado) conoce y acepta sus responsabilidades en materia de seguridad de los sistemas de información y recursos con los que trabaja (antes de la contratación, durante su vida laboral y una vez finalizada su relación laboral).

Se pretende cubrir, por tanto, la confidencialidad mediante el uso de cláusulas referentes a las obligaciones y responsabilidades de los empleados. Otro objetivo es cubrir el riesgo de robo, fraude y mal uso de las instalaciones.

Se informará a todo el personal para que sea consciente de la importancia de la seguridad y que sepan lo que se espera de ellos, cuáles son sus responsabilidades y que las acepten.

ANF AC establece un plan de comunicación que incluye sesiones de formación de seguridad para todos los empleados.

6.10 Seguridad Física y Ambiental

ANF AC asegura los activos tangibles descritos a través de controles de acceso. Las garantías que se cubren son la disponibilidad, la integridad y la confidencialidad de la información.

La infraestructura que sirve de soporte para el desarrollo de las actividades de la empresa, así como los soportes de almacenamiento que se usan, que residen en su edificio y en el de los proveedores de

servicio o terceros, están protegidos contra daño físico o hurto utilizando para ello mecanismos de control de acceso físico que aseguran que únicamente el personal autorizado tiene acceso a los mismos.

Por ello, dicha infraestructura estará ubicada en áreas de acceso restringido, con diferentes niveles de seguridad, a las cuales únicamente puede acceder personal debidamente autorizado. Los accesos a cada uno de los niveles son registrados por mecanismos de control de acceso, quedando disponibles para posteriores auditorías.

6.11 Comunicaciones y Operaciones

ANF AC asegura la operación correcta y segura de los medios de procesamiento de la información.

Se establecen responsabilidades y procedimientos para la gestión y operación de todos los medios de tratamiento de la información; así como para la gestión y control de servicios de terceros. Se han definido también procedimientos para la gestión de las relaciones con el cliente, el proceso de compras y el control de equipos.

Se implanta la segregación de tareas, cuando es adecuado, para reducir el riesgo de un mal uso deliberado o por negligencia.

Se introducirán controles y medidas adecuadas para prevenir y detectar la introducción de software dañino, y para evitar la infección de los sistemas de información.

Se establecen procedimientos para la realización de copias de seguridad y su recuperación.

Se establecen los procedimientos adecuados para proteger los documentos y soportes, cuando sea necesario; así como el almacenamiento, manipulación, transporte, destrucción y desecho accesible y recuperable solo por personal autorizado.

Se controlan los intercambios de información y software entre organizaciones, que cumplirán con toda la legislación vigente y con acuerdos formales previamente establecidos.

6.12 Control de Acceso

ANF AC ha desarrollado los procedimientos necesarios para el control de accesos que asegura el acceso del usuario autorizado y evita el acceso no autorizado a los servicios de red, a los servicios operativos, a la información mantenida en los sistemas de aplicación y a los sistemas de información por personal no autorizado.

Se tiene en cuenta:

- Inscripción y des-inscripción para otorgar acceso a los sistemas y servicios de información.
- Restricción y control de asignaciones y uso de privilegios.
- Buenas prácticas de seguridad en la selección y uso de claves.
- Protección adecuada al equipo desatendido.
- Métodos de autenticación para el control de acceso de usuarios remotos, cuando sea el caso.

- Procedimientos de registro seguro para el acceso a servicios operativos.
- Controles para tele-trabajo, cuando sea el caso.

6.13 Adquisición, desarrollo y mantenimiento de los sistemas de información

ANF AC es consciente de que la seguridad es una parte integral de sus sistemas de información.

Para ello realiza las tareas necesarias para la validación de data de Insumo, controles de procesamiento interno, integridad del mensaje y validación de data de output.

Para proteger la confidencialidad, autenticidad e integridad de la información se emplearán controles criptográficos.

Para garantizar la seguridad de los archivos del sistema se establecerán procedimientos para el control de software operacional, se controlarán los datos de prueba del sistema, y se creará control de acceso al código fuente del programa.

Para mantener la seguridad del software e información del sistema de aplicación se establecerán procedimientos de control de cambios, se realizará la revisión técnica de las aplicaciones después de cambios en el sistema operativo, se limitarán las modificaciones a los paquetes de software a los cambios necesarios y estos cambios serán controlados estrictamente.

Para reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas, se evaluará la exposición de la organización ante esas vulnerabilidades y se tomaran las medidas apropiadas para tratar el riesgo asociado.

6.14 Gestión de incidentes

ANF AC asegura que la información de los eventos y las debilidades en la seguridad de la información son comunicadas de manera que permiten tomar las acciones correctivas oportunas.

Se ha documentado un procedimiento para el control en el reporte de eventos y debilidades en la seguridad, que define responsabilidades y sistemáticas para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad.

6.15 Continuidad del negocio

ANF AC asegura la disponibilidad del servicio en caso de catástrofe y establece un plan de acción para minimizar sus efectos. Con esta acción se cubre la integridad, disponibilidad y la conservación de la información.

Se ha establecido un proceso de gestión de continuidad de actividad para garantizar la recuperación de los procesos críticos en caso de desastre, reduciendo el tiempo de no disponibilidad a niveles aceptables, mediante la adecuada combinación de controles de carácter organizativo, tecnológico y procedimentales, tanto preventivos como de recuperación.

6.16 Cumplimiento

ANF AC, mediante las políticas y estándares de seguridad definidos en el SGCSI trata de evitar incumplimientos de cualquier ley y de cualquier requerimiento de seguridad. También trata de maximiza la efectividad del proceso de auditoría de los sistemas de información.

ANF AC adquiere la responsabilidad de cumplir con la legislación vigente relativa a la seguridad de la información. ANF AC identifica los estatutos relevantes, regulaciones, leyes y requisitos contractuales relativos a seguridad de la información que afectan a la seguridad de sus activos de información.

Es responsabilidad de todos los departamentos implicados conocer y cumplir la legislación vigente que les es aplicable.

Todo el personal de ANF AC adquiere el compromiso de no divulgar ningún tipo de información.

Las aplicaciones informáticas se someterán periódicamente a una auditoria, encargada de verificar el cumplimiento de la normativa de seguridad y de los procedimientos del SGCSI.

6.17 Análisis de riesgos

ANF AC ha realizado una descripción de la metodología para la evaluación del riesgo, reporte de dicha evaluación y un plan de tratamiento del riesgo, según requerimientos normativos.

Se ha definido un criterio de riesgo para determinar la importancia de los riesgos. Las evaluaciones del riesgo identifican, cuantifican y priorizan los riesgos en comparación con el criterio para la aceptación del riesgo y los objetivos relevantes para ANF y sus clientes.

Los resultados guían y determinan la acción de gestión apropiada y las prioridades para manejar los riesgos de la seguridad de la información y para implementar las medidas de seguridad seleccionadas para protegerse contra estos riesgos.

6.18 Declaración de aplicabilidad

La declaración de aplicabilidad incluye:

1) Los objetivos de control y los controles seleccionados [para tratar los riesgos, en base a los criterios de aceptación de riesgos, además de los requisitos legales, reglamentarios y contractuales] y las justificaciones de su selección;

2) los objetivos de control y los controles actualmente implementados; y

3) la exclusión de cualquier objetivo de control y control del anexo A y la justificación de esta exclusión.

Nota: La declaración de aplicabilidad proporciona un resumen de las decisiones relativas al tratamiento de los riesgos. La justificación de las exclusiones facilita una comprobación cruzada de que no se ha omitido inadvertidamente ningún control.

7 Control y revisión

ANF AC establece diferentes procedimientos para el seguimiento y revisión del SGCSI.

7.1 Satisfacción del cliente

ANF AC ha definido una sistemática para medir la satisfacción de los clientes realizando periódicamente encuestas aleatorias.

7.2 Auditorías Internas

ANF AC realiza auditorías internas del SGCSI a intervalos planificados, según detalla en su procedimiento de Auditorías Internas.

7.3 Seguimiento y medición de los procesos y del producto.

ANF AC ha definido indicadores para sus procesos, asignando responsables para su seguimiento y objetivos a alcanzar.

Son revisados regularmente en una reunión que incluye también la revisión de los resultados de auditorías de seguridad, incidentes, revisión de las evaluaciones del riesgo, revisión del nivel de riesgo residual y del riesgo aceptable identificado, sugerencias y retroalimentación de todas las partes interesadas.

7.4 Control de las incidencias

ANF AC define en un procedimiento la sistemática para la gestión de las incidencias detectadas, incluyendo método de registro y evaluación con el objetivo de corregirlas y evitar su ocurrencia.

7.5 Revisión por la alta dirección de ANF

La alta dirección revisa los informes emitidos por las auditorías internas y externas realizada del SGCSI a intervalos periódicos para asegurar su continua idoneidad, conveniencia y efectividad. La revisión incluye evaluación para la mejora continua y la necesidad de cambios en el SGCSI, incluyendo las políticas de calidad y seguridad y los objetivos. Los resultados de las revisiones deben documentarse claramente.

Para ello, se recibe una serie de informaciones, que ayudan a tomar decisiones, entre las que se pueden enumerar:

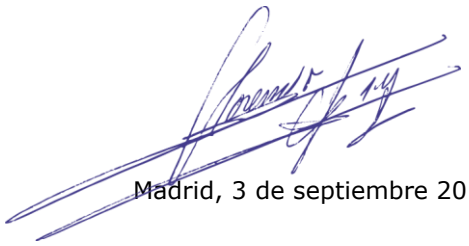
- Resultados de auditorías y revisiones del SGCSI.
- Observaciones de todas las partes interesadas.
- Técnicas, productos o procedimientos que pudieran ser útiles para mejorar el rendimiento y eficacia del SGCSI.
- Información sobre el estado de acciones preventivas y correctivas.
- Vulnerabilidades o amenazas que no fueran tratadas adecuadamente en evaluaciones de riesgos anteriores.
- Resultados de las mediciones de eficacia.
- Estado de las acciones iniciadas a raíz de revisiones anteriores de la Gerencia.
- Cualquier cambio que pueda afectar al SGCSI.
- Recomendaciones de mejora.

Basándose en todas estas informaciones, la Gerencia debe revisar el SGCSI y tomar decisiones y acciones relativas a:

- Mejora de la eficacia del SGCSI.
- Actualización de la evaluación de riesgos y del plan de tratamiento de riesgos.
- Modificación de los procedimientos y controles que afecten a la seguridad de la información, en respuesta a cambios internos o externos en los requisitos de negocio, requerimientos de seguridad, procesos de negocio, marco legal, obligaciones contractuales, niveles de riesgo y criterios de aceptación de riesgos.
- Necesidades de recursos.
- Mejora de la forma de medir la efectividad de los controles.

8 Mantenimiento y mejora del SGCSI

ANF AC, según indica en su procedimiento de acciones correctivas y preventivas, define las acciones correctivas necesarias para eliminar o minimizar las causas de las incidencias detectadas (internas o externas) o potenciales para poder evitar la recurrencia.



Madrid, 3 de septiembre 2018