Sistema de gestión de la Seguridad de la Información

Política de seguridad de la información

ÍNDICE

CONTROL DE DOCUMENTO

Título	Política de Seguridad de la Información
Versión	2.1
Fecha	15-01-2009
Revisión Anterior	31-10-2023

Control de Cambios y Versiones

Fecha	Versión	Motivo del Cambio
15-01-2019	1.0	Primera versión.
22-01-2019	1.1	Se elimina el alcance y se hace referencia a los objetivos del SGSI
08-04-2019	1.2	Adaptación a eIDAS
20-09-2019	1.3	Se incluye apartado en referencia a TSA
09-03-2021	2.0	Adaptación al Esquema Nacional de Seguridad
31-10-2023	2.1	Adaptación al nuevo RD 311/2022 del 3 de mayo

1. INTRODUCCIÓN

VIAFIRMA, como muestra de compromiso con la seguridad de la información de sus sistemas ha desarrollado la presente Política de Seguridad de la Información, en adelante Política de Seguridad, de conformidad con lo establecido en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y con la normativa UNE-EN ISO/IEC 27001:2017.

La Política de Seguridad es una declaración ética, responsable y de estricto cumplimiento en toda la Organización, la cual es desplegada a través de las diferentes Normativas y Procedimientos con los que se procura que los riesgos sean tratados adecuadamente.

El uso de los Activos de información debe estar en consonancia con las buenas prácticas y procedimientos de trabajo profesionales, así como con los requisitos legales, reglamentarios y contractuales, que deben garantizar la Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad de la información y los servicios.

1.1. Objetivo y ámbito de aplicación

Este documento constituye el establecimiento de un marco organizativo y tecnológico en la Organización.

Se entenderá la Seguridad, como un proceso integral constituido por todos los elementos técnicos, humanos y materiales y organizativos relacionados con los sistemas de información, quedando excluidas cualquier tipo de actuaciones puntuales o de tratamiento coyuntural.

Debe ser conocida y cumplida por todo el personal de la Organización, independientemente del puesto, cargo y responsabilidad dentro del mismo.

1.2. Destinatarios de la política de seguridad

Todas las personas pertenecientes a VIAFIRMA y las personas externas a ella que realicen trabajos o servicios para VIAFIRMA son destinatarios de la Política de Seguridad.

2. LEGISLACIÓN Y NORMATIVA DE REFERENCIA

El marco normativo de las actividades de VIAFIRMA en el ámbito de esta Política de Seguridad está integrado por las siguientes normas:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- 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)
- UNE-EN ISO/IEC 27001:2017
- Reglamento Europeo de Firma Electrónica (eIDAS). Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE).
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público
- Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
- Ley 2/2019, de 1 de marzo, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual
- Real Decreto-Ley 14/2019 de 31 de octubre medidas en materia de administración digital, contratación del sector público y telecomunicaciones
- Ley 6/2020, de 11 de noviembre reguladora de determinados aspectos de los servicios electrónicos de confianza.

- Guías de la serie 400, 500 y 800 del CCN

3. MISIÓN, FINES, FUNCIONES Y ACTUACIONES

3.1. Misión

Viafirma nace con la idea de poder **automatizar procesos de firma complejos difícilmente realizables mediante las fórmulas tradicionales en papel**. Actualmente la firma electrónica es más eficiente que su equivalente manuscrito, por lo que una correcta optimización de los documentos hará que los equipos de trabajo sean más productivos y puedan dedicarles más tiempo a otras actividades de mayor importancia para la empresa.

Ofrecemos diferentes **soluciones de firma orientadas a entornos presenciales y remotos**, permitiendo la firma de contratos desde cualquier dispositivo y lugar.

3.2. Fines

Dar respuesta a una extensa lista de desafíos en la transformación digital de las empresas e instituciones, en un amplísimo número de sectores. Después de haber concursado en diversas licitaciones nacionales en los últimos años, compitiendo con las principales empresas del sector, podemos asegurar por los resultados que ofrecemos la suite de soluciones de firma electrónica más completa y avanzada del mercado español.

3.3. Funciones

La empresa se dedica al desarrollo y comercialización de productos relacionados con las firmas electrónicas y digitales.

La **suite Viafirma** es el conjunto de soluciones de la firma que dan respuesta a una extensa lista de desafíos en la transformación digital de las empresas e instituciones, en un amplísimo número de sectores. Después de haber concursado en diversas licitaciones nacionales en los últimos años, compitiendo con las principales empresas del sector, podemos asegurar por los resultados que ofrecemos la suite de soluciones de firma electrónica más completa y avanzada del mercado español.

3.4. Actuaciones

Ante el imparable avance tecnológico actual, desde Viafirma apostamos fuerte por la movilidad. Tareas y trámites que antes requerían disponibilidad y presencia en el centro de trabajo hoy en día pueden realizarse sobre la marcha con nuestras soluciones. Nuestros productos ayudan a las empresas a reducir su huella de carbono. Eliminar el papel en la oficina trae consigo un beneficio directo para el medio ambiente. Un trabajador de oficina puede usar hasta 10.000 hojas de papel al año, de las que se desperdician más del 50%. La innovación constante siempre va detrás de nuestros productos, alineándose en todo momento con las necesidades y tendencias del mercado actual.

4. OBJETIVOS DE LA POLÍTICA DE SEGURIDAD

Son objetivos de la política de seguridad TIC:

- Garantizar a todos los clientes y usuarios de los servicios ofrecidos por Viafirma que sus datos serán gestionados de acuerdo con los estándares y buenas prácticas en seguridad TIC.
- Garantizar la seguridad de la información, proteger los activos o recursos de información.
- Aumentar el nivel de concienciación en materia de seguridad TIC en VIAFIRMA, garantizando que el personal a su servicio es consciente de sus obligaciones y responsabilidades.
- Establecer las bases de un modelo integral de gestión de la seguridad TIC en VIAFIRMA, que cubra en un ciclo continuo de mejora los aspectos técnicos, organizativos y procedimentales.
- Garantizar el cumplimiento de la legislación vigente en materia de seguridad TIC.
- Crear la estructura de seguridad de VIAFIRMA.
- Marcar las directrices, los objetivos y los principios básicos de seguridad de la información de la organización.
- Orientar la organización para la prestación de servicios basados en la gestión de riesgos.
- Servir de base para el desarrollo de las normas, procedimientos y procesos de gestión de la seguridad de la información.
- Realizar el tratamiento de datos de carácter personal siempre de acuerdo con la legislación aplicable en todo momento, siendo especialmente importantes la RGPD y el LOPDgdd.

5. PRINCIPIOS Y DIRECTRICES DE LA SEGURIDAD TIC

5.1. Principios

Principio de confidencialidad: los activos TIC deberán ser accesibles únicamente para aquellas personas usuarias, órganos y entidades o procesos expresamente autorizados para ello, con respeto a las obligaciones de secreto y sigilo profesional.

Principio de integridad y calidad: se deberá garantizar el mantenimiento de la integridad y calidad de la información, así como de los procesos de tratamiento de la misma, estableciéndose los mecanismos para asegurar que los procesos de creación, tratamiento, almacenamiento y distribución de la información contribuyen a preservar su exactitud y corrección.

Principio de disponibilidad y continuidad: se garantizará un alto nivel de disponibilidad en los activos TIC y se dotarán de los planes y medidas necesarias para asegurar la continuidad de los servicios y la recuperación ante posibles contingencias graves.

Principio de gestión del riesgo: se deberá articular un proceso continuo de análisis y tratamiento de riesgos como mecanismo básico sobre el que debe descansar la gestión de la seguridad de los activos TIC.

Principio de proporcionalidad en coste: la implantación de medidas que mitiguen los riesgos de seguridad de los activos TIC deberá hacerse bajo un enfoque de proporcionalidad en los costes económicos y operativos.

Principio de concienciación y formación: se articulará iniciativas que permitan a las personas usuarias conocer sus deberes y obligaciones en cuanto al tratamiento seguro de la información se refiere. De igual forma, se fomentará la formación específica en materia de seguridad TIC de todas aquellas personas que gestionan y administran sistemas de información y telecomunicaciones.

Principio de prevención: se desarrollarán planes y líneas de trabajo específicas orientadas a prevenir fraudes, incumplimientos o incidentes relacionados con la seguridad TIC.

Principio de mejora continua: se revisará el grado de eficacia de los controles de seguridad TIC implantados, al objeto de adecuarlos a la constante evolución de los riesgos y del entorno tecnológico de la organización.

Principio de seguridad TIC en el ciclo de vida de los activos TIC: las especificaciones de seguridad se incluirán en todas las fases del ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.

Principio de función diferenciada: la responsabilidad de la seguridad de los sistemas de tecnologías de la información y comunicaciones estará diferenciada de la responsabilidad sobre la prestación de los servicios.

5.2. Contexto y obligaciones generales

VIAFIRMA depende de los sistemas TIC para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

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.

Los sistemas TIC deben estar protegidos contra amenazas de 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 los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, 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.

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 departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el Artículo 8 del Esquema Nacional de Seguridad, regulado por RD 311/2022.

5.3. Prevención

Se debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello deberán implementarse las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los departamentos (o servicios externos contratados) deben:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

5.4. Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple ralentización hasta su detención, se debe monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 11 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 10 del ENS.

Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

5.5. Respuesta

Se deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos u otras organizaciones externas.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT de INCIBE)

5.6. Recuperación

Para garantizar la disponibilidad de los servicios críticos, se deben desarrollar planes de continuidad de los sistemas TIC y actividades de recuperación.

5.7 Otros principios generales

- El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.
- La información debe ser protegida contra accesos y alteraciones no autorizados, manteniéndola confidencial e íntegra.
- La información debe estar disponible, permitiendo su acceso autorizado, siempre que sea necesario.

- La Seguridad de la Información es responsabilidad de todos. Todas las personas que tiene acceso a la información de la Organización deben protegerla, por lo que deben estar adecuadamente formadas y concienciadas.
- La Seguridad de la Información no es algo estático, debe ser constantemente controlada y periódicamente revisada.
- Todos aquellos activos (infraestructura, soportes, sistemas, comunicaciones, etc.) donde reside la información, viaja o es procesada, deben estar adecuadamente protegidos.
- El sistema ha de proteger el perímetro, en particular, si se conecta a redes públicas, según lo establecido en el artículo 24 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Las medidas de seguridad que se implanten deben estar en proporción a la criticidad de la información que proteja y a los daños o pérdidas que se puedan producir en ella. En todo momento se seguirá como mínimo las medidas de seguridad impuestas por el Esquema Nacional de Seguridad, así como las guías CCN-STIC elaboradas por el Centro Criptológico Nacional del Centro Nacional de Inteligencia.
- La seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida. Además, VIAFIRMA exigirá, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.
- Los sistemas se instalarán en áreas separadas, dotadas de un procedimiento de control de acceso. Como mínimo, las salas deben estar cerradas y disponer de un control de llaves.
- En la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones que vayan a ser empleados por las Administraciones públicas se estará a lo dispuesto en el artículo 19 del Real Decreto 311/2022, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Los sistemas deben diseñarse y configurarse de forma que se garantice la seguridad por defecto tal y como se exige en el artículo 19 del Real Decreto 3/2010, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- El tratamiento de datos de carácter personal debe estar siempre de acuerdo con las leyes aplicables en cada momento, siendo especialmente importantes el Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La estructura organizativa de la gestión de la seguridad de la información en el ámbito de la seguridad de la información de VIAFIRMA está compuesta por los siguientes agentes:

- CEO de VIAFIRMA
- Comité de Seguridad de la Información.
- Responsable de Seguridad.
- Responsables de la Información y de los Servicios.
- Responsables del Sistema de Información.
- Delegado de Protección de Datos.
- Responsable del Tratamiento.
- Encargado de Tratamiento.

6.1. CEO de VIAFIRMA

Es el responsable de aprobar la política de seguridad.

6.2. Comité de Seguridad de la Información

Para la gestión de la seguridad de la información, se crea el Comité de Seguridad de la Información, en adelante comité de seguridad, dentro del ámbito de la presente Política de Seguridad formado por un equipo multidisciplinar que coordinará las actividades y controles de seguridad establecidos en la organización y que vela por el cumplimiento de la normativa vigente, interna y externa, en materia de protección de datos de carácter personal y seguridad.

Son funciones del Comité de Seguridad las siguientes:

- Identificar los objetivos de la Organización en el ámbito de la Seguridad de la Información.

- Elaborar la Política de Seguridad, establecer los criterios de revisión de la misma, revisar, distribuirla y velar por su cumplimiento.

- Promover y respaldar los planes de acción e iniciativas que garanticen la implantación de la Política de Seguridad en la Organización.

- Establecer los requisitos de seguridad que deben cumplir a nivel organizativo, técnicos y de control, los sistemas y servicios de la Organización.

- Garantizar que la seguridad forma parte del proceso de planificación de la gestión de la información y como proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información.

- Comunicar a los terceros que colaboren en la explotación de los sistemas de información la realización de la misma conforme a los exigidos en el ENS y en la UNE-EN ISO/IEC 27001:20017

- Aprobar los nombramientos de responsables y responsabilidades en materia de seguridad de la información.

- Valorar el grado de conformidad de los procedimientos implantados en la Organización con las normas definidas en la política, estableciendo planes de mejora para aquellos que requieran de una modificación para su conformidad.

- Supervisar las normativas y procedimientos de seguridad que se definan para dar cumplimiento y desarrollo a la Política de Seguridad.

- Acordar y aprobar metodologías y procesos específicos relativos a la Seguridad de la Información.

- Verificar que todas las acciones llevadas a cabo en materia de Seguridad sean compatibles o se encuentren respaldadas por la Política de Seguridad.

- Promover la realización de auditorías periódicas que permitan verificar el cumplimiento de las obligaciones de las Administraciones en materia de Seguridad.

- Promover la formación y concienciación en materia de Seguridad de la Información a todo el personal.

- Mantener contactos periódicos con grupos, otras entidades, organismos, foros, etc. que resulten de interés en el ámbito de la Seguridad de la Información, compartiendo experiencias y conocimiento que ayuden a mejorar y mantener la seguridad de los sistemas de la Organización.

- Valorar y evaluar los recursos necesarios para dar soporte al proceso de planificación e implantación de la seguridad en la Organización.

El Comité de Seguridad estará compuesto por los siguientes miembros:

Presidencia: Antonio Cabrera Jiménez.

Vocalías:

- Benito Galán Algora.
- Fran Gómez González.
- Diego Gil Serrano.

Secretaría: Mamen Maya Fernández.

El Comité de Seguridad podrá convocar a sus reuniones a las personas que en cada caso autorice la Presidencia, por propia iniciativa o a propuesta de alguno de sus miembros. Asimismo, podrá recabar de personal técnico especializado, propio o externo, la información pertinente para la toma de decisiones.

En caso de vacante, ausencia, enfermedad u otras causas legales, la persona titular de la Presidencia será sustituida por la persona titular de la Secretaría del Comité de Seguridad. Las Vocalías podrán designar una persona que las sustituya en estas circunstancias entre personal de VIAFIRMA.

Con objeto de ejercer un seguimiento periódico, el Comité de Seguridad se reunirá, al menos, dos veces al año con carácter ordinario.

Por razones de urgencia, el Comité de Seguridad se reunirá de forma extraordinaria cuando el presidente lo estime oportuno o a petición de uno o más vocales del Comité de Seguridad, y siempre que:

- Aparezcan incidencias de seguridad graves que afecten a cualquier área de su competencia.
- Surjan nuevas necesidades de seguridad que requiera la participación de los componentes del Comité.

Para la celebración de las reuniones del Comité de Seguridad será preciso la presencia de, al menos, el 51% de los miembros permanentes.

6.3. Responsable de Seguridad

Es la persona responsable de supervisar que los servicios y sistemas de información de la Organización se mantengan con el mayor grado de seguridad atendiendo a los principios de:

Confidencialidad: la información asociada a los servicios electrónicos al ciudadano solo debe poder ser conocida por las personas autorizadas para ello.
Integridad: la información asociada a los servicios electrónicos al ciudadano no debe ser alterada por personas no autorizadas.
Disponibilidad: garantía de que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma siempre que lo requieran, así como garantía de que los servicios electrónicos permanecerán disponibles.

Son funciones del Responsable de Seguridad:

- Supervisar el cumplimiento de la presente Política, de sus normas y procedimientos derivados.
- Asesorar en materia de seguridad a los integrantes de VIAFIRMA que así lo requieran.
- Coordinar la interacción con otros organismos especializados.

- Tomar conocimiento y supervisar la investigación y monitorización de los incidentes de seguridad.
- Coordinar el establecimiento de las medidas de seguridad, adecuadas y eficaces para cumplir los requisitos de seguridad establecidos por las personas Responsables de los Servicios y de la Información, siguiendo en todo momento lo exigido en el Anexo II del ENS y en el Anexo A de la UNE-EN ISO/IEC 27001:2017.
- Asesorar, en colaboración con la persona Responsable del Sistema, las personas Responsables de los Servicios y de la Información en la realización de los análisis y gestión de riesgos, elevando el informe resultado al Comité de Seguridad.
- Promover las actividades de concienciación y formación en materia de seguridad en su ámbito de responsabilidad, siguiendo las directrices del Comité de Seguridad.
- Preparar los temas a tratar en las reuniones del Comité de Seguridad, aportando información puntual para la toma de decisiones.

Respecto a la documentación, son funciones de la persona Responsable de Seguridad:

- Aprobar y proponer al Comité de Seguridad la documentación de seguridad de segundo nivel (Normativas y Procedimientos de Seguridad) de obligado cumplimiento.
- Supervisar la documentación de tercer nivel (Procedimientos de Seguridad) de obligado cumplimiento.
- Mantener la documentación organizada y actualizada, gestionando los mecanismos de acceso a la misma.

En aquellos sistemas de información que, por su complejidad, distribución, separación física de elementos o números de usuarios, se necesitara de personal adicional para llevar a cabo las funciones del Responsable de Seguridad, el Responsable de Seguridad podrá designar cuantos Responsables de Seguridad Delegados considere necesarios. Los Responsables de Seguridad Delegados se harán cargo, en su ámbito, de todas aquellas acciones que delegue el Responsable de Seguridad teniendo dependencias funcionales directas con él.

La persona Responsable de Seguridad es la figura que determina las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos. Deberá ser una persona física, jerárquicamente superior e independiente de la persona responsable del Sistema de Información.

La persona Responsable de Seguridad será nombrada y cesada por el Comité de Seguridad.

6.4. Responsable de la Información y de los Servicios

Esta responsabilidad recaerá en los titulares del departamento de desarrollo de productos/servicios. El responsable de información será quién determine los requisitos de la información tratada mientras que el responsable de servicio determinará los requisitos de los servicios prestados.

Son las personas responsables de clasificar la información conforme a los criterios y categorías establecidas en el ENS y en cada una de las dimensiones de seguridad conocidas y aplicables, dentro del marco establecido en el Anexo I del ENS y del Anexo A de la normativa UNE-EN ISO/IEC 27001:2017.

Son los responsables de determinar los niveles de seguridad de los servicios en cada dimensión de seguridad dentro del marco establecido en el Anexo I del ENS y en cada una de las dimensiones de seguridad conocidas y aplicables (disponibilidad, autenticidad, trazabilidad, confidencialidad e integridad) y del Anexo A de la normativa UNE-EN ISO/IEC 27001:2017.

Son los encargados, contando con la participación y asesoramiento de la persona Responsable de Seguridad y de la persona Responsable del Sistema de Información, de realizar los preceptivos análisis de riesgos, y de seleccionar las salvaguardas a implantar.

Son los responsables de aceptar los riesgos residuales calculados en el análisis de riesgos, y de realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

Las personas responsables de información y de los servicios son nombrados y cesados por el Comité de Seguridad.

6.5. Responsable del Sistema de Información

Las personas Responsables de los Sistemas de Información serán designadas al efecto por el departamento de sistemas y figurarán en la documentación de seguridad de los sistemas de información. Para cada sistema de información deberá existir una persona Responsable de Sistema, siendo posible que una misma persona sea responsable de varios sistemas.

Sus principales responsabilidades serán:

- Supervisar el desarrollo, operación y mantenimiento de los sistemas de información durante todo su ciclo de vida, así como las especificaciones de los mismos, la instalación y verificación de su correcto funcionamiento.
- Ser el primer responsable de la seguridad de los sistemas de información que dirija, velando porque la seguridad de la información esté presente en todas y cada una de las partes de sus ciclos de vida. Especialmente deberá velar porque el desarrollo de los sistemas siga las directrices de seguridad establecidas en el ENS y en el Anexo A de la UNE-EN ISO/IEC 27001:2017. Para todo ello podrá contar con el asesoramiento de la persona Responsable de Seguridad.
- Creación, mantenimiento y actualización continua de la documentación de seguridad de los sistemas de información, con el asesoramiento de la persona Responsable de la Seguridad.
- Asesorar en la definición de la topología y sistema de gestión de los sistemas de información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Asesorar en colaboración con la persona Responsable de la Seguridad, a las personas Responsables de la Información y a las personas Responsables de los Servicios, en el proceso de la gestión de riesgos.
- Suspender el manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y con la persona Responsable de la Seguridad, antes de ser ejecutada.

6.6. Delegado de Protección de Datos

La persona Delegada de Protección de Datos será única para toda la Organización, se informará de su nombramiento y cese a VIAFIRMA Española de Protección de Datos.

Son funciones de la persona Delegada de Protección de Datos:

- Informar y asesorar a la Organización y a todos los empleados que se ocupen del tratamiento de datos personales, de las obligaciones que se deriven del Reglamento General de Protección de Datos y de otras disposiciones relacionadas con la protección de datos.
- Supervisar el cumplimiento del Reglamento General de Protección de Datos en la Organización.
- Asesorar acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.
- Cooperar con la Autoridad de control
- Actuar como punto de contacto de la Autoridad de Control

Además, asesorará y supervisará en las siguientes áreas:

- Cumplimiento de principios relativos al tratamiento, como los de limitación en la finalidad, minimización o exactitud de los datos
- Identificación de las bases jurídicas de los tratamientos.
- Valoración de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.
- Existencia de normativa sectorial que pueda determinar condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos.
- Diseño e implantación de medidas de información a los afectados por los tratamientos de datos.
- Establecimiento de mecanismos de recepción y gestión de solicitudes de ejercicio de derechos por parte de los interesados.
- Valoración de las solicitudes de ejercicio de derechos por parte de los interesados.
- Contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación Organización – encargado de tratamiento.
- Identificación de los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia.
- Diseño e implantación de políticas de protección de datos.
- Auditorías de protección de datos.
- Establecimiento y gestión de los registros de actividades de tratamiento

- Análisis de riesgo de los tratamientos realizados
- Implantación de las medidas de protección de datos desde el diseño y protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos
- Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos
- Establecimiento de procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación a las autoridades de supervisión y a los afectados
- Determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos
- Realización de evaluaciones de impacto sobre la protección de datos
- Relaciones con las autoridades de supervisión
- Implantación de programas de formación y sensibilización del personal de la Organización en materia de protección de datos.

La persona Delegada de Protección de Datos es nombrada y cesada por el Comité de Seguridad.

6.7. Responsable de Tratamiento

La persona Responsable del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determina los fines y medios del tratamiento, es decir, VIAFIRMA.

VIAFIRMA debe, entre otras cosas:

- Garantizar la observancia de los principios relativos al tratamiento y aprobar la política, normativa y procedimientos concernientes a la protección de datos personales.
- Designar a quien ejerza como persona Responsable de Seguridad, quien deberá coordinar y controlar las medidas de seguridad definidas.
- Designar a la persona Delegada de Protección de Datos, cuando corresponda.
- Adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos personales y evitar su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos

almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural. En particular, difundirá entre el personal las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pudieran incurrir en caso de incumplimiento.

- Garantizar el cumplimiento de las políticas y normativas aprobadas e implementadas en VIAFIRMA.
- Asegurar que la realización de tratamientos por cuenta de terceras partes esté regulada en un contrato, que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que la persona encargada del tratamiento únicamente tratará los datos conforme a las instrucciones de la persona responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará (ni siquiera para su conservación) a otras personas.
- Adoptar las medidas correctoras adecuadas.

6.8. Encargado de tratamiento

Si las personas Responsables de los Tratamientos designarán a una persona Encargada del Tratamiento lo harán únicamente por cada tratamiento a una persona Encargada de Tratamiento que ofrezca garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas para que el tratamiento sea conforme al Reglamento General de Protección de Datos y garantice la protección de los derechos de las personas interesadas, de conformidad con el artículo 28 del Reglamento General de Protección de Datos.

Las principales funciones y responsabilidades, dentro de su ámbito de actuación, son las establecidas en el artículo 28 del Reglamento General de Protección de Datos y demás normativa de aplicación.

- Tratará los datos personales únicamente siguiendo instrucciones documentadas de la persona responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará a la persona responsable de esa

exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público.

- Garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria.
- Tomará todas las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos personales y evitar su alteración, pérdida, tratamiento o acceso no autorizado.
- Asistirá a la persona responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos para los derechos del interesado.
- Ayudará a la persona responsable a garantizar el cumplimiento de las obligaciones establecidas para la seguridad del tratamiento, notificación de violaciones de seguridad, evaluación de impacto y consulta previa a la AEPD, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado;
- A elección de la persona responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros;
- Pondrá a disposición de la persona responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte de la persona responsable o de otro auditor autorizado por dicho responsable.

Tanto la persona Responsable como la persona Encargada del Tratamiento deberá determinar claramente cuándo el tratamiento se realiza bajo su autoridad, conforme a lo establecido en el artículo 29 del Reglamento General de Protección de Datos y cuándo se realiza mediante una persona Encargada de Tratamiento sujeto a lo establecido en el artículo 28 de dicho Reglamento General de Protección de Datos.

6.9. Resolución de conflictos

En el caso de conflicto y, de acuerdo con el principio de jerarquía que rige en VIAFIRMA, éste será resuelto por el superior jerárquico. En defecto de lo anterior, siempre prevalecerá la decisión del Comité de Seguridad.

En caso de que exista conflicto entre los responsables que componen la estructura organizativa de la presente Política y lo estipulado en la normativa de protección de datos personales vigente, prevalecerá la decisión que presente un mayor nivel de exigencia respecto a la protección de datos de carácter personal.

7. OBLIGACIONES DEL PERSONAL

Todo el personal, interno y externo, de VIAFIRMA tiene la obligación de conocer y cumplir la presente Política de Seguridad, las normativas y procedimientos derivados de la misma, tales como las relativas a la protección de datos de carácter personal, siendo responsabilidad del Comité de Seguridad disponer de los mecanismos necesarios para que la información llegue a todo el personal indicado.

El incumplimiento manifiesto de la Política de Seguridad de la Información o las normativas y procedimientos derivados de ésta podrá acarrear el inicio de medidas disciplinarias oportunas y, en su caso, las responsabilidades legales correspondientes.

Todo el personal relacionado con la información y los sistemas deberá regirse según las estipulaciones del art. 15 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, relativo a la gestión del personal.

8. ASESORAMIENTO ESPECIALIZADO EN MATERIA DE LA SEGURIDAD DE LA INFORMACIÓN

La persona Responsable de Seguridad será la encargada de coordinar los conocimientos y las experiencias disponibles en VIAFIRMA con el fin de proporcionar ayuda en la toma de decisiones en materia de seguridad, pudiendo obtener asesoramiento de otras organizaciones y entidades de carácter público o privado.

8.1. Cooperación con otras organizaciones

La persona Responsable de Seguridad será la encargada a efectos de coordinación o intercambiar experiencias y obtener asesoramiento para el mejoramiento de las prácticas y controles de seguridad, se mantendrán contactos con los siguientes organismos y entidades especializadas en temas relativos a la seguridad de la información:

- Agencia Española de Protección de Datos (AEPD): velando por el cumplimiento de la legislación sobre protección de datos de carácter personal y controlando su aplicación.
- Instituto Nacional de Ciberseguridad (INCIBE) – CERT Centro de Respuesta a Incidentes de Seguridad: ofreciendo soluciones reactivas a incidentes informáticos, servicios de prevención frente a posibles amenazas y servicios de información, concienciación y formación en materia de seguridad (www.incibe.es).
- Grupo de Delitos Informativos Informáticos y Telemáticos de la Guardia Civil y Brigada de Investigación Tecnológica (BIT) del Cuerpo Nacional de Policía: investigando acciones relacionadas con la delincuencia informática y los fraudes en el sector de las telecomunicaciones que le encomienden las Autoridades Judiciales o que conozca por comunicaciones y denuncias de los ciudadanos y que por su importancia o relevancia social, dificultad técnica o número de afectados, aconseje la dedicación de este grupo.

Adicionalmente, se mantendrán contactos con otras organizaciones y entidades de carácter público y privado para compartir experiencias en esta materia.

8.2. Revisión independiente de la seguridad de la información

El Comité de Seguridad TIC propondrá la realización de revisiones independientes sobre la vigencia e implementación de la Política de Seguridad TIC con el objetivo de garantizar que las prácticas en VIAFIRMA reflejan adecuadamente sus disposiciones, sin perjuicio de que otros órganos internos o externos puedan llevar a cabo revisiones sobre la Política de Seguridad TIC y las medidas de seguridad implantadas.

9. TRATAMIENTO DE CARACTER PERSONAL

Para el tratamiento de datos de carácter personal en los sistemas de información se seguirá en todo momento lo desarrollado en el documento de seguridad y su documentación asociada conforme a lo exigido en el 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), así como a lo establecido en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

10. FORMACIÓN Y CONCIENCIACIÓN

El objetivo es lograr la plena conciencia respecto a que la Seguridad de la Información afecta a todos los miembros de VIAFIRMA y a todas las actividades de acuerdo con el principio de Seguridad Integral recogido en el art. 6 del ENS. A estos efectos, VIAFIRMA, propondrá y organizará sesiones formativas y de concienciación para que todas las personas que intervienen en el proceso y sus responsables jerárquicos tengan una sensibilidad hacia los riesgos que se corren incluyéndose estas actividades en el Plan de Formación anual del organismo.

Toda la plantilla de VIAFIRMA tiene la obligación de conocer y cumplir esta Política de Seguridad TIC y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a todas las personas afectadas.

Toda la plantilla de VIAFIRMA recibirá las acciones de concienciación en materia de seguridad de la Información, de forma periódica con el fin de al menos, una vez al año. Se establecerá un programa de concienciación continua para atender a todo el personal de VIAFIRMA, en particular a las personas de nueva incorporación.

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

El Comité de Seguridad y la persona Responsable de Seguridad se encargará de promover las actividades de formación y concienciación en materia de seguridad.

11. ANÁLISIS Y GESTIÓN DE RIESGOS

VIAFIRMA realizará una gestión de la seguridad basada en los riesgos, propiciando que tanto el análisis como la gestión de riesgos sean parte esencial del proceso de seguridad, que deberá ser lo más transversal posible al resto de procesos de la organización.

La gestión de riesgos permitirá mantener un entorno controlado, minimizando los riesgos hasta niveles aceptables, reduciendo estos niveles mediante el despliegue de medidas de seguridad, proceso para el que se establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad.

VIAFIRMA asume el compromiso de controlar los riesgos de seguridad, así como dar cumplimiento a la legislación y normas internas vigente bajo un proceso de mejora continua conforme a los marcos y metodologías existentes en la actualidad, utilizando MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) y la herramienta PILAR para su implantación.

Para ello, con el objetivo de conocer el nivel de exposición de los activos de información a los riesgos y amenazas en materia de seguridad, las personas Responsables de los Sistemas de Información realizarán, con periodicidad al menos anual, análisis de riesgos cuyas consecuencias se plasmarán en actuaciones para tratar y mitigar el riesgo, o incluso replantear la seguridad de los sistemas en caso necesario.

Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos de carácter personal, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, así como la comunicación o acceso no autorizados a dichos datos.

Se realizará un análisis de riesgos:

- Regularmente, una vez al año.
- Cuando haya cambios en los servicios esenciales prestados o cambios significativos en las infraestructuras que los soportan.
- Cuando ocurra un incidente de seguridad grave.

- Cuando se identifiquen amenazas severas que no hubieran sido tenidas en cuenta o vulnerabilidades graves que no están contrarrestadas por las medidas de protección implantadas.

Las conclusiones de los análisis de riesgos serán elevadas a la persona Responsable de Seguridad y ésta al Comité de Seguridad.

Para la armonización de los análisis de riesgos, el Comité de Seguridad establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad propiciará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas promoviendo inversiones de carácter horizontal.

El Comité de Seguridad TIC es el responsable de aceptar los riesgos residuales calculados en el análisis de riesgos, y de realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

La normativa de seguridad estará disponible para su consulta en el repositorio documental de la intranet de VIAFIRMA.

12. CLASIFICACIÓN Y CONTROL DE ACTIVOS

Los recursos tecnológicos y la información de VIAFIRMA se encontrarán inventariados, con una persona responsable asociada y, en caso de ser necesario, una persona custodia de los mismos. Los inventarios se mantendrán actualizados para asegurar su validez.

Los activos de información estarán clasificados de acuerdo con su sensibilidad y criticidad para el desarrollo de la actividad de VIAFIRMA, en función de la cual se establecerán las medidas de seguridad exigidas para su protección.

13. AUDITORÍA DE SEGURIDAD

Los sistemas de información serán objeto de una auditoría regular ordinaria, al menos cada dos años, que verifique el cumplimiento de los requerimientos del ENS y en el caso de otras normativas como UNE-EN ISO/IEC 27001:2017 y Reglamento Europeo de Firma Electrónica (eIDAS). Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo.

Estas auditorías ordinarias, así como las extraordinarias para el ENS se harán de acuerdo con lo establecido en el art. 31 del Real Decreto 311/2022, de 3 de mayo, y la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información, aprobada por Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública.

Los informes de auditoría serán presentados a la persona Responsable del Sistema competente, al Delegado de Protección de Datos, si afectara a estos, y a la persona Responsable de Seguridad. Estos informes serán analizados por esta última persona que presentará sus conclusiones a la persona Responsable del Sistema para que adopte las medidas correctoras adecuadas. Los resultados obtenidos determinarán las líneas de actuación a seguir y las posibles modificaciones a realizar sobre los controles y la normativa de seguridad.

Con el fin de optimizar la utilización de los recursos de la organización y garantizar una mejor coordinación entre seguridad TIC y seguridad de protección de datos, siempre que sea posible, las auditorías de seguridad de sistemas de información y las auditorías de protección de datos o medidas análogas de verificación, evaluación y valoración de seguridad de los tratamientos se realizarán de manera conjunta.

14. TERCERAS PARTES

Cuando VIAFIRMA preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad, estableciéndose canales para la comunicación y coordinación de los respectivos Comités de Seguridad y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando VIAFIRMA utilice servicios de terceras partes o ceda información a terceras partes, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que atañe a dichos servicios o información. Dichas terceras partes quedarán sujetas a las obligaciones establecidas en la citada normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de comunicación y resolución de incidencias. Se garantizará que el personal de terceras partes esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe de la persona Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por las personas responsables de la información y los servicios afectados antes de seguir adelante.

15. SEGUIMIENTO DE LA APLICACIÓN DE LA POLÍTICA Y ASPECTOS DISCIPLINARIOS

Todo el personal de VIAFIRMA que figure como destinatario de esta Política (véase apartado 3), ya sea interno o externo, tiene la obligación de conocer y cumplir la misma, así como el resto del cuerpo normativo y los procedimientos derivados; en especial, pero no sólo, las normas y procedimientos relativos a la protección de datos de carácter personal, siendo responsabilidad del Comité de Seguridad disponer de los mecanismos necesarios para que la información llegue a todos los afectados.

El canal de comunicación principal que utilizará el Comité de Seguridad para transmitir dicha información al personal afectado será la Intranet de VIAFIRMA y sus propios productos de firma.

El incumplimiento manifiesto de la presente Política, las normativas y los procedimientos derivados de ésta podrá acarrear el inicio de medidas disciplinarias oportunas y, en su caso, las responsabilidades legales correspondientes. Para ello, se seguirá el proceso disciplinario formal existente y contemplado en las normas internas de VIAFIRMA para las personas empleadas que violen la Política de Seguridad, así como las Normas y Procedimientos derivados de ella.

16. ESTRUCTURA DEL MARCO NORMATIVO EN SEGURIDAD DE LA INFORMACIÓN

La documentación relativa a la Seguridad de la Información estará clasificada en cuatro niveles, de manera que cada documento de un nivel se fundamenta en los de nivel superior:

- Primer nivel: Política de Seguridad TIC.
- Segundo nivel: Normativas de Seguridad.
- Tercer nivel: Procedimientos Seguridad.
- Cuarto nivel: Documentación técnica.

La persona Responsable de Seguridad TIC se encarga de la gestión de los documentos indicados, debiendo asegurar que ésta sea completa y proporcione información suficiente para definir las necesidades de protección de la información y los activos asociados a la misma en el ámbito de VIAFIRMA.

16.1. Primer nivel: Política de Seguridad

Documento de obligado cumplimiento por todo el personal, interno y externo, de la Organización, recogido en el presente documento y aprobado por el CEO de VIAFIRMA.

16.2. Segundo nivel: Normativa de Seguridad

De obligado cumplimiento de acuerdo con el ámbito organizativo, técnico o legal correspondiente.

La responsabilidad de aprobación de los documentos redactados en este nivel será competencia del Comité de Seguridad.

16.3. Tercer nivel: Procedimientos de Seguridad

Documentos técnicos orientados a resolver las tareas, consideradas críticas por el perjuicio que causaría una actuación inadecuada, de seguridad, desarrollo, mantenimiento y explotación de los sistemas de información.

La responsabilidad de aprobación de estos procedimientos técnicos es de la persona Responsable del Sistema de Información correspondiente. En caso de que los procedimientos afectarán a varios sistemas de información será responsabilidad de la persona Responsable de Sistemas aprobarlos.

16.4. Cuarto nivel: Documentación Técnica

Documentos de carácter técnico que recogen instrucciones técnicas para la realización de tareas específicas, el resultado y las conclusiones de un estudio o una valoración; documentos de carácter técnico que recogen amenazas y vulnerabilidades de los sistemas de información, así como también evidencias electrónicas generadas durante todas las fases del ciclo de vida del sistema de información. La responsabilidad de que existan este tipo de documentos es de cada una de las personas Responsables de los Sistemas de Información en su ámbito.

16.5. Otra documentación

Se podrá seguir en todo momento los procedimientos, normas e instrucciones técnicas STIC, así como las guías CCN-STIC de las series 400, 500, 600 y 800.

17. ACTUALIZACIÓN Y DISTRIBUCIÓN

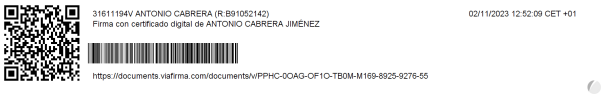
Esta Política será sometida a revisión, actualización y distribución anualmente por el órgano o figura competente establecida, así como cada vez que ocurran cambios significativos en los elementos del Sistema de Información que puedan afectar directa o indirectamente, distribuyéndose a todo el personal afectado. La versión actualizada y vigente de la Política de Seguridad, se publicará en la Intranet de VIAFIRMA.

18. APROBACIÓN Y ENTRADA EN VIGOR

Este texto será aprobado el día que figura al pie de página del presente documento por la persona titular de la responsabilidad de CEO de VIAFIRMA.

Esta Política de Seguridad es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política

Fdo. Antonio Cabrera Jiménez (CEO Viafirma)



19. ANEXO I- REQUISITOS MÍNIMOS

Para la correcta implementación y cumplimiento de la presente Política de Seguridad es necesario aplicar una serie de requisitos de obligatorio cumplimiento.

19.1. La Seguridad en la Organización

La seguridad debe comprometer a todas las personas integrantes de VIAFIRMA, sin excepción.

En el apartado *6 Organización y gestión de la seguridad TIC* del presente documento, se especifica la organización de la seguridad con la definición de la estructura organizativa.

Asimismo, la implementación de dicha organización está en el marco normativo cubierto por el establecimiento de un Sistema de Gestión de la Seguridad, basado en el ENS.

19.2. Análisis y Gestión de riesgos

Los servicios e infraestructuras bajo el alcance de la presente Política de Seguridad deberán estar sometidos a un análisis de riesgos para orientar las medidas de protección a minimizar los mismos como se indica en el apartado *11 Análisis y gestión de riesgos* del presente documento.

La descripción de la metodología y evaluación del riesgo están indicados en la *Normativa de gestión de ciclo de vida de las plataformas tecnológicas* y desarrollados en el documento *Metodología de análisis y gestión de riesgos*.

El análisis de riesgos se realizará igualmente cuando se vaya a iniciar o modificar un tratamiento de datos de carácter personal, en línea a lo establecido en el RGPD y la LOPDgdd. En estos casos se contemplarán en el alcance del análisis todos aquellos activos que intervengan en el tratamiento, considerando tanto activos relacionados con los sistemas de información, como humanos, locales o terceros.

A raíz de los resultados obtenidos en los mencionados análisis de riesgos se determinarán las medidas necesarias para proteger dichos datos.

19.3. Gestión de personal

En el apartado *7 Obligaciones del personal* de la presente Política de Seguridad, en la *Normativa sobre Recursos Humanos* y en la *Normativa de Gestión de Formación, concienciación y sensibilización*, se detalla la obligatoriedad de conocimiento y concienciación en materia de seguridad según sus responsabilidades. Los recursos necesarios para la implantación del sistema de seguridad, así como aquellos que lleven a cabo su operación, mantenimiento, supervisión, o tenga relación con el sistema se establecen en los planes estratégicos de VIAFIRMA, y son aprobados por la Dirección del organismo a propuesta del Comité de Seguridad TIC.

19.4. Profesionalidad

Siguiendo lo indicado en el apartado *10 Formación y concienciación en seguridad TIC* de la presente Política de Seguridad, en la *Normativa de Gestión de formación, concienciación y sensibilización,* se desarrollan los objetivos de las acciones de formación y concienciación.

Con periodicidad anual se diseñará un plan de formación específico en el que se tendrá en cuenta las necesidades de profesionalidad del sistema de seguridad.

19.5. Autorización y control de acceso

El acceso a los sistemas de información estará restringido y limitado a aquellas personas usuarias o procesos que lo necesiten para el desarrollo de su actividad y estén previamente autorizados siguiendo lo indicado en la *Normativa de gestión de acceso lógico* y la *Normativa de gestión de autorizaciones.*

El acceso a la información seguirá el principio de "necesidad de conocer", de forma que los privilegios otorgados a cada entidad sean los mínimos imprescindibles para el desarrollo de su actividad.

La identificación de las personas usuarias será tal que se pueda conocer en todo momento quién recibe los derechos de acceso y quién ha realizado alguna actividad, por lo que los identificadores serán personales, no compartidos e intransferibles, siguiendo lo indicado en la *Normativa de gestión de cuentas de usuario* y la *Normativa de gestión de logs de sistemas y aplicaciones*.

Los lugares con acceso restringido igualmente se controlarán y serán previamente autorizados por los responsables asignados, siguiendo lo indicado en la *Normativa de seguridad física y del entorno* y la *Normativa de gestión de autorizaciones*.

19.6. Protección de instalaciones

Los sistemas de información estarán ubicados en zonas protegidas, con acceso restringido, habilitado únicamente al personal autorizado, tal como se indica en la *Normativa de seguridad física y del entorno* y la *Normativa de gestión de autorizaciones*.

19.7. Adquisición de productos

Para las actividades de adquisición de nuevos productos, sistemas o servicios se establecen actuaciones de análisis de riesgos con proveedores y se mantendrán actualizados los listados de proveedores habituales, siguiendo lo indicado en la *Normativa de contratación y relaciones con terceros* y en la *Normativa de gestión de ciclo de vida de las plataformas tecnológicas*. Las adquisiciones se autorizará por los responsables del área implicada y el área de Compras a través de informes favorables del proveedor, en caso de requerirse, siguiendo lo indicado en la *Normativa de gestión de autorizaciones*.

19.8. Seguridad por defecto

Los sistemas y aplicaciones se diseñarán y construirán bajo el principio de seguridad por defecto, como se desarrolla en la *Normativa de gestión de desarrollo seguro*, de tal forma que:

- El sistema ofrecerá la funcionalidad mínima necesaria y ninguna adicional. Cualquier función que no sea de interés o innecesaria será deshabilitada o no implantada.
- La operación y explotación de los sistemas estará limitada a aquellas personas o ubicaciones que se autoricen, quedando prohibidas para el resto.
- El uso del sistema ha de ser seguro, de tal forma que el uso inseguro requerirá intención expresa por parte del usuario.

La seguridad estará presente desde la concepción de un sistema o aplicación y permanecerá presente durante todo su ciclo de vida.

En la concepción de un nuevo sistema o aplicación, o modificación sustancial de un sistema o aplicación existentes, se contará siempre, y desde el inicio, con la participación del Responsable de Seguridad de la Información.

19.9. Integridad y actualización del sistema

Se deberán seguir en todo momento las informaciones acerca de las vulnerabilidades que afectan a los sistemas de información, siguiendo lo indicado en la *Normativa de Gestión de ciclo de vida de las plataformas tecnológicas* y en la *Normativa de gestión de bastionados*.

Se seguirán las recomendaciones de los fabricantes de equipos y software en cuanto a actualizaciones de seguridad, que deberán ser analizadas en cuanto a su idoneidad y conveniencia, y aplicadas en caso positivo con la menor dilación.

19.10. Protección de la información almacenada y en tránsito

Se protegerán los entornos que contienen información almacenada y en tránsito entre entornos inseguros, siguiendo lo indicado en la *Normativa de gestión de la clasificación y tratamiento de la Información*. En este sentido se protegerán convenientemente los equipos portátiles que puedan contener información, siguiendo lo indicado en la *Normativa de uso y protección de portátiles*, así como los soportes extraíbles (lápices de memoria, discos duros extraíbles, etc.), siguiendo lo indicado en la *Normativa de gestión de soportes* y en la *Normativa de uso de recursos y accesos a sistemas de información*.

19.11. Prevención ante otros sistemas de información interconectados

Se desplegarán las protecciones necesarias para proteger el perímetro de la red corporativa de VIAFIRMA, de forma que se neutralicen las posibles intrusiones procedentes del exterior, ya sea iniciadas malintencionadamente por terceros o como consecuencia de la interconexión con sistemas de terceros, siguiendo lo indicado en la *Normativa de gestión de redes y comunicaciones*.

19.12. Registro de actividad

Los sistemas y aplicaciones generarán los registros de actividad necesarios para conocer la actividad de los sistemas, de forma que se pueda determinar en todo momento qué persona actúa, sobre qué datos, con qué operaciones y sus privilegios de acceso, siguiendo lo indicado en la *Normativa de gestión de logs de sistemas y aplicaciones*.

19.13. Gestión de incidentes de seguridad

VIAFIRMA definirá e implantará procedimientos de gestión de incidencias de seguridad que aseguren la correcta gestión y respuesta efectiva que permita anular o minimizar el impacto

del incidente en la información, los servicios, los empleados, las personas usuarias y, en general, en la actividad de VIAFIRMA, siguiendo lo expuesto en la *Normativa de gestión de incidentes*.

El procedimiento de gestión y respuesta a incidentes de seguridad contemplará la comunicación y notificación de los incidentes a los organismos receptores de dicha información de acuerdo con la legalidad vigente.

19.14. Continuidad de negocio

Para asegurar la disponibilidad de los servicios y sistemas de información, VIAFIRMA diseñará e implantará Planes de Continuidad de servicio que evitan las interrupciones de las actividades de VIAFIRMA y garanticen, ante una contingencia, la reanudación de los servicios y sistemas de información a los niveles adecuados de operatividad, siguiendo lo indicado en la *Normativa de continuidad del servicio*.

19.15. Gestión de la seguridad y mejora continua

Se deberá establecer un Sistema de Gestión de la seguridad que permita conocer en cada momento el estado de la seguridad, mediante la definición y medida de indicadores, y permita tomar las decisiones informadas pertinentes para cumplir los requisitos de seguridad establecidos, siguiendo lo indicado en la *Normativa de métricas e indicadores de seguridad* y en la *Normativa de monitorización*.

Se establecerá un proceso de mejora continua mediante el análisis de la situación, la implantación de nuevas medidas de seguridad, la mejora de las existentes y la aportación de mejoras sugeridas por el Comité de Seguridad y por todo VIAFIRMA en su conjunto.

20. ANEXO II FUNCIONAMIENTO Y MÉTODO DE TRABAJO DEL COMITÉ DE SEGURIDAD

Con objeto de ejercer un seguimiento periódico, el Comité de Seguridad se reunirá, al menos, una vez por semestre con carácter ordinario.

Por razones de urgencia, el Comité de Seguridad se reunirá de forma extraordinaria cuando el respectivo presidente lo estime oportuno, y siempre que:

- Aparezcan incidencias de seguridad graves que afecten a cualquier área de su competencia.
- Surjan nuevas necesidades de seguridad que requieran la participación de los componentes del Comité.

En cada reunión se ha de revisar los siguientes puntos con la frecuencia especificada:

Objeto	Frecuencia	Requiere Acta
Identificar Objetivos y requerimientos de medidas de seguridad RGPD.	Anual	SI
Revisión del Documento de Protección de Datos Personales y se debe asegurar su cumplimiento.		SI
Establecer planes de formación, concienciación y divulgación de las obligaciones de seguridad.		SI
Revisión y aprobación del Plan de tratamiento de riesgos.		SI
Revisión del riesgo residual aceptado.		SI
Revisión y actualización, si procede, de los integrantes del Comité de Seguridad.		SI
Aprobar planes de mejora de la seguridad de la información.		SI

Objeto	Frecuencia	Requiere Acta
Promover la realización de las auditorías periódicas.		SI
Analizar los informes de autoevaluación y los informes de auditorías.		SI
Monitorizar los principales riesgos residuales asumidos por Viafirma y recomendar posibles actuaciones respecto de ellos.		SI
Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.	Semestral	SI
Análisis de los indicadores de seguridad.		SI
Revisión y aprobación de las políticas, normativas y/o procedimientos de seguridad que han sido modificados.		SI
Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.		SI
Coordinar la aplicación de las medidas de seguridad de la Política y Documento de Protección de Datos Personales.		SI

Como método de trabajo y comunicación de los distintos miembros de los mismos se utilizarán preferentemente métodos telemáticos de transmisión de la información.