TLP: WHITE

SGSI-100

NOVIEMBRE 2020

Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

MARCO NORMATIVO DE SEGURIDAD DE LA INFORMACIÓN

NORMA DEL SGSI

SGSI-100

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE FNMT-RCM

Toda la información contenida en este documento está clasificada como **TLP: WHITE**, definición esta descrita en la norma SGSI-202 Gestión de Activos y Clasificación de la Información y como tal está sujeta en todo momento a las restricciones y medidas de protección adecuadas a ese nivel de clasificación de la información.

ÍNDICE DE CONTENIDOS

MENSAJE DE LA PRESIDENTA DE LA FÁBRICA NACIONAL DE MONEDA Y TIMBRE 5

1. INTRODUCCIÓN 6

2. ALCANCE 8

3. OBJETIVO 9

4. MARCO LEGAL Y NORMATIVO 10

5. FÁBRICA NACIONAL DE MONEDA Y TIMBRE 13

5.1. Estatutos 13

5.2. Misión y objetivos 13

6. PRINCIPIOS BÁSICOS 16

7. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 17

7.1. Objeto 17

7.2. Alcance 17

7.3. Aprobación 18

7.4. Entrada en vigor y aplicación 18

7.5. Incumplimientos y sanciones 18

7.5.1. Sanciones disciplinarias según lo dispuesto en el Convenio Colectivo 19

7.5.2. Sanciones jurídicas según lo dispuesto en la legislación vigente 19

7.6. Revisión y mejora 20

8. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 21

8.1. Gestión de riesgos de seguridad de la Información 22

8.2. Gestión y clasificación de los recursos de la información 22

8.3. Seguridad relativa a los recursos humanos 22

8.4. Control de acceso a los sistemas de información 23

8.5. Seguridad física 23

8.6. Seguridad en la operación y las comunicaciones 23

8.7. Adquisición, desarrollo y mantenimiento de los sistemas de información 23

8.8. Gestión segura de terceros 23

8.9. Gestión de incidentes de seguridad de la información 24

8.10. Gestión de la continuidad del negocio 24

8.11. Gestión del cumplimiento 24

8.12. Mantenimiento de instalaciones 24

9. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 25

9.1. Comité de Seguridad de la Información 25

9.2. Roles y funciones en la organización de la seguridad 27

9.2.1. Funciones del Responsable de la Información 27

9.2.2. Funciones del Responsable del Servicio 27

9.2.3. Funciones del Responsable de Seguridad de la Información 28

9.2.4. Funciones del Responsable del Sistema 28

9.2.5. Funciones del administrador de seguridad del sistema 29

9.2.6. Delegado de protección de datos 29

9.3. Asignación de roles y responsabilidades 30

9.4. Relaciones con terceros 32

10. DATOS DE CARÁCTER PERSONAL 33

11. EXCEPCIONES E INCUMPLIMIENTOS 34

ANEXO 1. ACRÓNIMOS Y DEFINICIONES 35

A1.1. Acrónimos 35

A1.2. Definiciones 35

MENSAJE DE LA PRESIDENTA DE LA FÁBRICA NACIONAL DE MONEDA Y TIMBRE

La Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda (FNMT-RCM), como productor de elementos y servicios de seguridad, considera los sistemas TIC (Tecnologías de la Información y Comunicaciones) y la Seguridad de la Información que maneja en el desarrollo de su actividad un elemento clave para el cumplimiento de sus objetivos estratégicos.

El objetivo de la Seguridad de la Información es garantizar la calidad de la información que da soporte a las actividades de negocio y la prestación continuada de los servicios, actuando preventivamente y reaccionando con diligencia ante los incidentes.

La política de Seguridad de la Información define los principios esenciales y responsabilidades que permiten asegurar que la información, los sistemas de información, los soportes en los que ésta se encuentra y las redes de comunicaciones de FNMT-RCM están adecuadamente protegidos.

Esta política tiene en cuenta el valor de la información gestionada por nuestra organización, así como las obligaciones legales derivadas de su custodia. Su contenido y organización sigue los principios y requisitos mínimos que establece el Esquema Nacional de Seguridad, desarrollado por Real Decreto 3/2010 de 8 de enero.

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

Cada uno de los miembros de FNMT-RCM, y la propia entidad como organización, debe responsabilizarse de la información a la que tiene acceso en el desempeño de sus funciones, de modo que su utilización permita realizarlas de forma eficiente, suponiendo una ventaja competitiva. Una custodia de información negligente puede suponer importantes pérdidas económicas y de imagen para FNMT-RCM, así como incurrir en responsabilidades legales.

La política de Seguridad de la Información, así como la normativa, estándares, guías y procedimientos que la desarrollan, ha sido definida para afrontar de forma eficaz y eficiente los riesgos y amenazas a los que están sometidos todos nuestros activos de información. Por tanto, la presente política ha de ser conocida, comprendida y asumida por todos los miembros de nuestra organización y por todos aquellos que tengan acceso a la información de FNMT-RCM.

Dña. Lidia Sánchez Milán

Presidenta - Directora General

1. INTRODUCCIÓN

La política de Seguridad de la Información de FNMT-RCM[A05] forma parte del cuerpo normativo del Sistema de Gestión de Seguridad de la Información[D19] (en adelante SGSI) de la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda (en adelante FNMT-RCM).

El cuerpo normativo del SGSI[A11] está formado por documentos de diferentes niveles, que detallan, y complementan al nivel superior. El orden de los niveles del SGSI es:

- La política de Seguridad de la Información de FNMT-RCM.
- Las políticas del SGSI.
- Las normas del SGSI.
- Las guías del SGSI.
- Los procedimientos del SGSI.
- Las instrucciones técnicas del SGSI.

La política de seguridad deberá referenciar y ser coherente con lo establecido en el Documento de Seguridad que exige el Real Decreto 1720/2007, en lo que corresponda.

El presente documento define las directrices de Seguridad de la Información conforme a los intereses de FNMT-RCM y sus partes interesadas. En concreto, entre los objetivos de la política, se encuentran:

Con la aparición del Esquema Nacional de Seguridad, en adelante ENS[A04], los sistemas de información de la Administración quedan sujetos a una serie de requisitos de seguridad (preceptos legales) determinados por dicho Esquema.

En este contexto, la normativa interna de seguridad informática ha venido incorporando numerosos mandatos legales en diversos aspectos de la gestión de la seguridad.

El ENS está constituido por los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información. Será aplicado por las Administraciones públicas para asegurar el acceso, integridad[D13], disponibilidad[D09], autenticidad[D03], confidencialidad[D04], trazabilidad[D21] y conservación de los datos[D08], informaciones y servicios[D18] utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias.

Según el art. 27 del R.D. 3/2010 que regula el ENS, se establece que, para dar cumplimiento a los requisitos mínimos establecidos en el presente real decreto, las Administraciones públicas aplicarán las medidas de seguridad indicadas en el Anexo II, teniendo en cuenta:

- Los activos[D01] que constituyen el sistema.
- La categoría del sistema, según lo previsto en el Artículo 43.

- Las decisiones que se adopten para gestionar los riesgos[D17] identificados.

Por ello, se establece esta norma sobre la gestión de los activos y clasificación de la información, tratando de regularizar un uso adecuado y seguro a través de los sistemas de información disponibles en la FNMT-RCM.

El ENS, en su artículo 11. Requisitos mínimos de seguridad, indica:

- Todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad, que será aprobada por el titular del órgano superior correspondiente.

El artículo 12. Organización e implantación del proceso de seguridad, indica que:

- La seguridad deberá comprometer a todos los miembros de la organización.
- La política de seguridad se redactará y cumplirá los criterios que se detallan en el Anexo II, sección 3.1, debiendo identificar unos claros responsables, que deberán velar por el cumplimiento de la política y así como por el conocimiento de la misma por todos los miembros de la organización administrativa.

Este documento responde al cumplimiento de las medidas de seguridad del ENS, contempladas dentro del marco organizativo, donde se establece en la medida de seguridad org.1 lo siguiente:

Que debe existir una política de seguridad, la cual será aprobada por el órgano superior competente que corresponda, de acuerdo con lo establecido en el Artículo 11, y se plasmará en un documento escrito, de forma clara, los siguientes puntos:

Los objetivos o misión de la organización.

- El marco legal y regulatorio en el que se desarrollarán las actividades.
- Los roles o funciones de seguridad, definiendo para cada uno, los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.
- La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización.
- Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

2. ALCANCE

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

Todo el personal, directa o indirectamente, relacionado con FNMT-RCM y su SGSI, al cual afecte el presente documento en el ámbito del desarrollo de sus funciones profesionales, deberá respetar y promover los contenidos aquí descritos.

Este documento y procesos[D16] están sujetos a revisiones y modificaciones, así como aquellos que lo complementen, implementen o desarrollen, siendo de aplicación a todos los sistemas de información de la FNMT-RCM, así como en aquella infraestructura y sistemas que les proporcione soporte y usuarios pertenecientes al sistema y subyacentes. Cualquier cambio en el mismo será comunicado utilizando los mecanismos oficiales de la organización. Asimismo, la última versión estará disponible para su consulta en la Intranet.

3. OBJETIVO

Este documento tiene por objetivo el describir la organización y su contexto, teniendo en cuenta sus estatutos, misión, objetivos, marco legal y regulatorio.

Para ello, se definen los siguientes puntos u objetivos a tratar:

- Buscará definir los principios básicos de Seguridad de la Información.
- Detallara todos los aspectos relacionados con la política de Seguridad de la Información de FNMT-RCM (objeto, alcance, aprobación, entrada en vigor y aplicación, incumplimientos y sanciones, y revisión y mejora).
- Describirá la documentación que desarrolla la política de Seguridad de la Información de FNMT-RCM.
- Detallara la organización de la Seguridad de la Información en FNMT-RCM.
- Describirá la situación de FNMT-RCM en lo relativo a datos de carácter personal.

4. MARCO LEGAL Y NORMATIVO

[01] Sin ánimo de ser exhaustivos y sin perjuicio de la normativa o regulación específica de las actividades descritas en el apartado anterior, se toman como referencias:

[01.01] 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).

[01.02] 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.

[01.03] Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación[D10] electrónica y servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (Reglamento eIDAS).

[01.04] Resolución de 25 de noviembre de 2011, de la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, por la que se crea y regula su registro electrónico.

[01.05] Real Decreto 390/2011, de 18 de marzo, por el que se modifican los estatutos de la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda y del Instituto de Crédito Oficial, aprobados, respectivamente, por el Real Decreto 1114/1999, de 25 de junio, y por el Real Decreto 706/1999, de 30 de abril, y por el que se autoriza la extinción de la Fundación Real Casa de la Moneda.

[01.06] Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

[01.07] 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.

[01.08] Real Decreto 199/2009, de 23 de febrero, por el que se modifica el Estatuto de la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, aprobado por el Real Decreto 1114/1999, de 25 de junio, por el que se adapta la Fábrica Nacional de Moneda y Timbre a la Ley 6/1997, de 14 de abril, de organización y funcionamiento de la Administración General del Estado, se aprueba su Estatuto y se acuerda su denominación Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda.

[01.09] Orden EHA/2357/2008, de 30 de julio, por la que se regulan los ficheros de datos de carácter personal de la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda.

[01.10] Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (Directiva NIS).

[01.11] Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

[01.12] Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

[01.13] Ley 59/2003, de 19 de diciembre, de firma electrónica.

[01.14] Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

[01.15] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales[A08] (LOPDGDD).

[01.16] 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 vigente en todas aquellas disposiciones que no contradigan el Reglamento General de Protección de Datos.

[01.17] Real Decreto 1114/1999, de 25 de junio, por el que se adapta la Fábrica Nacional de Moneda y Timbre a la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado, se aprueba su Estatuto y se acuerda su denominación como Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda.

[01.18] Ley 46/1998, de 17 de diciembre, sobre introducción del euro.

[01.19] Ley Orgánica 10/1998, de 17 de diciembre, complementaria de la Ley sobre introducción del euro.

[01.20] Ley 50/1998, de 3 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social.

[01.21] Ley 66/1997, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social.

[01.22] Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado.

[01.23] Real Decreto Legislativo 1/1996 por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual.

[01.24] Ley 42/1994, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social.

[01.25] Ley 31/1990, de 27 de diciembre, de Presupuestos Generales del Estado para 1991.

[01.26] Real Decreto 1417/1982, de 14 de mayo, por el que se autoriza la emisión y acuñación de las monedas integrantes del nuevo sistema de moneda metálica.

[02] La FNMT-RCM debe asegurar que la información recibe un apropiado nivel de protección en función de la importancia que tiene para la organización.

[03] Otras normas o regulaciones:

[03.01] UNE[A13]-ISO[A07]/IEC[A06] 27002:2015. Código de buenas prácticas para la Gestión de la Seguridad de la información.

[03.02] UNE-ISO/IEC 27001:2015. Especificaciones para los Sistemas de Gestión de la Seguridad de la Información.

[03.03] ISO/IEC 9001:2000 Sistemas de gestión de la calidad.

[03.04] CCN[A02]-STIC[A12] 805 ENS- Política de Seguridad.

5. FÁBRICA NACIONAL DE MONEDA Y TIMBRE

[04] En este apartado, se presenta a FNMT-RCM como entidad empresarial y, por otro lado, se describe el contexto legal y regulatorio de dicha organización.

5.1. Estatutos

[05] FNMT-RCM es una entidad pública empresarial de las previstas en el artículo 43.1, b), de la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado, que, como organismo público, tiene personalidad jurídica pública diferenciada, patrimonio y tesorería propios y autonomía de gestión en los términos de dicha ley.

[06] Está adscrita al Ministerio de Hacienda, el cual, a través de la Subsecretaría correspondiente, ejercerá respecto de ella la dirección estratégica y el control de eficacia en los términos previstos en los artículos 43 y 59 de la Ley 6/1997.

[07] Los estatutos de FNMT-RCM quedan aprobados en el Real Decreto 1114/1999, de 25 de junio, por el que se adapta la Fábrica Nacional de Moneda y Timbre a la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado, se aprueba su Estatuto y se acuerda su denominación como Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda.

[08] Con posterioridad al Real Decreto 1114/1999 se publican los siguientes Reales Decretos que modifican al primero y, por tanto, a los estatutos de FNMT-RCM:

[08.01] Real Decreto 199/2009, de 23 de febrero, por el que se modifica el Estatuto de la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, aprobado por el Real Decreto 1114/1999, de 25 de junio, por el que se adapta la Fábrica Nacional de Moneda y Timbre a la Ley 6/1997, de 14 de abril, de organización y funcionamiento de la Administración General del Estado, se aprueba su Estatuto y se acuerda su denominación Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda.

[08.02] Real Decreto 390/2011, de 18 de marzo, por el que se modifican los estatutos de la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda y del Instituto de Crédito Oficial, aprobados, respectivamente, por el Real Decreto 1114/1999, de 25 de junio, y por el Real Decreto 706/1999, de 30 de abril, y por el que se autoriza la extinción de la Fundación Real Casa de la Moneda.

[09] Los estatutos de esta entidad pueden encontrarse en la dirección https://www.fnmt.es.

5.2. Misión y objetivos

[10] Constituyen fines de FNMT-RCM:

[10.01] La acuñación de monedas de todas clases, de acuerdo con la legislación aplicable.

[10.02] La elaboración de cospeles y la acuñación de medallas y trabajos análogos para el estado o particulares.

[10.03] La impresión de billetes de banco, de conformidad con su legislación reguladora y en los términos que se acuerde con el Banco de España o banco emisor correspondiente.

[10.04] La elaboración de los documentos por los que se hacen efectivos cualesquiera tributos o precios públicos, billetes, impresos y listas de Lotería Nacional, así como cualquier documento relativo a otros juegos que le sean encomendados por las Administraciones públicas o sus organismos públicos, vinculados o dependientes.

[10.05] La elaboración de documentos de valor o de seguridad que le sean encargados por cualquier Administración pública o sus organismos públicos, vinculados o dependientes.

[10.06] La estampación de toda clase de documentos, sellos, signos o efectos postales y de franqueo, de acuerdo con lo establecido por la legislación aplicable, para el Estado o, en su caso, para organismos o entidades públicas o privadas.

[10.07] La prestación, en el ámbito de las Administraciones públicas y sus organismos públicos, vinculados o dependientes, de servicios de seguridad, técnicos y administrativos, en las comunicaciones a través de técnicas y medios electrónicos, informáticos y telemáticos (EIT), así como la expedición, fabricación y suministro de los títulos o certificados de usuario o soportes en tarjeta necesarios a tal fin, de acuerdo con lo establecido en el artículo 81 de la Ley 66/1997, de 30 de diciembre, y en su normativa de desarrollo o, en su caso, en los términos que establezcan las disposiciones legales correspondientes.

En el ejercicio de las facultades derivadas de este apartado, la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda quedará sometida a lo dispuesto en el artículo 2.2, y demás de aplicación, de la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, así como a la normativa que se cita en este párrafo g), sin perjuicio del resto de supuestos en que resulte de aplicación, de acuerdo con el artículo 53.2 de la Ley 6/1997, de 14 de abril.

[10.08] La realización de actividades o prestación de servicios relacionados con los ramos propios de la entidad a que se refieren los apartados anteriores, para personas o entidades públicas o privadas, tanto nacionales como extranjeras.

En la prestación de servicios electrónicos, informáticos o telemáticos, así como en la expedición, fabricación y suministro de títulos o certificados de usuario y soportes o tarjetas destinados al ámbito privado, la entidad actuará a todos los efectos en régimen de derecho privado.

[10.09] Cualquier otro que se le atribuya por disposición legal o reglamentaria.

[11] Sin perjuicio del carácter preferente de las diferentes actividades y prestaciones a realizar para el Estado español y sus organismos públicos, vinculados o dependientes, FNMT-RCM podrá desarrollar sus actividades para otros Estados y para organismos dependientes de los mismos, así como para entidades públicas o privadas no nacionales,

según proceda por la naturaleza de su actividad, de acuerdo con lo establecido por la normativa aplicable o, en su caso, en los términos y condiciones de los correspondientes contratos o acuerdos.

[12] Asimismo, FNMT-RCM ostenta la consideración de Laboratorio Oficial del Estado, en los términos que reglamentariamente se determinen, de conformidad con la disposición adicional vigésima, párrafo segundo, de la Ley 31/1990, de 27 de diciembre.

[13] Finalmente, señalar que FNMT-RCM es medio propio y servicio técnico de la Administración General del Estado en los términos de la Ley 30/2007, de 30 de octubre, de Contratos del Sector Público y de su Estatuto.

6. PRINCIPIOS BÁSICOS

[14] El objetivo de la Seguridad de la Información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente y reaccionando con diligencia ante los incidentes. Ésta será dirigida desde un SGSI cuyos principios básicos son los siguientes:

[14.01] Seguridad integral, entendida como un proceso constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con el sistema de información[D20], donde la concienciación y formación de todas las personas involucradas, desde los máximos responsables hasta el empleado, es de máxima importancia.

[14.02] Gestión de la Seguridad de la Información basada en el análisis de riesgos[d17.1], parte esencial del proceso y que deberá mantenerse permanentemente actualizado. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables en los que establecerá un equilibrio entre la naturaleza y valor de la información, su tratamiento, los riesgos a los que está expuesta y los costes, económicos y operativos, de las medidas de seguridad.

[14.03] Prevención, reacción y recuperación. La gestión de la Seguridad de la Información debe contemplar los aspectos de prevención, detección y corrección para conseguir que las amenazas[D02] sobre la misma no se materialicen y, en el peor de los casos, no afecten gravemente, pudiéndose corregir la situación en caso de incidente.

[14.04] Líneas de defensa estructuradas en capas de seguridad constituidas por medidas de naturaleza organizativa, física y lógica.

[14.05] Reevaluación periódica del SGSI y de las medidas de seguridad que responda a la constante evolución de los riesgos y sistemas de protección.

[14.06] La Seguridad de la Información como función diferenciada, asignando diferentes responsabilidades en los procesos de negocio que manejen información y diferenciando claramente la seguridad de los mismos frente a la prestación de los servicios. Concretamente, dentro de los sistemas de información, se diferenciará el responsable de la información, el responsable del sistema, el responsable del servicio y el responsable de la seguridad.

7. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

[15] En este apartado, se detallan todos los aspectos relacionados con la política de Seguridad de la Información de FNMT-RCM.

7.1. Objeto

[16] Esta política define las responsabilidades para la adecuada gestión de la Seguridad de la Información y los pilares para el desarrollo de normativa, procesos y medidas de seguridad necesarias al objeto de que todos los activos de información de FNMT-RCM estén adecuadamente protegidos.

[17] El desarrollo de esta política contribuye a:

[17.01] Considerar la información, y los sistemas que la soportan, como activos estratégicos, manifestando así la determinación de la Dirección en alcanzar los niveles de seguridad que garanticen el acceso, integridad, disponibilidad, autenticidad, confidencialidad y trazabilidad de la información y de los servicios gestionados por la FNMT-RCM en el ejercicio de sus competencias.

[17.02] Facilitar la consecución de los objetivos de la Seguridad de la Información.

[17.03] Asegurar la gestión de la Seguridad de la Información conforme a los principios básicos antes mencionados.

[17.04] Promover la concienciación de los usuarios y la comprensión de los riesgos asociados a la utilización de tecnologías de la información y redes de comunicaciones.

[17.05] Preservar los derechos legalmente reconocidos de FNMT-RCM y de los usuarios de los sistemas de información y velar por el cumplimiento de la legislación vigente.

7.2. Alcance

[18] Esta política:

[18.01] Es de aplicación a los soportes de información, sistemas de información y redes de comunicaciones empleados por FNMT-RCM en el desarrollo de sus actividades de negocio, así como a la información en sí misma.

[18.02] Aplica durante todo el ciclo de vida de la información, es decir, durante la creación, almacenamiento, transmisión, actualización, consulta y destrucción.

[18.03] Es de obligado cumplimiento para todos los empleados de FNMT-RCM, cualquiera que sea su relación con la organización, y para cualquier tercero que tenga acceso a activos de información o recursos de tratamiento de FNMT-RCM.

[19] Las actividades de FNMT-RCM como Prestador de Servicios de Certificación son especialmente sensibles a los riesgos de Seguridad de la Información que se presentan en la actualidad. Por este motivo, y dado que estos servicios son considerados

estratégicos en la sociedad de la información de hoy en día, se observará especialmente la presente política en este ámbito.

[20] Toda excepción a la presente política y su normativa de desarrollo requerirá la correspondiente solicitud escrita por parte del interesado y con la debida justificación. Dicha solicitud será estudiada por el Comité de Seguridad de la Información para su aprobación o rechazo.

[21] La ausencia de tratamiento en el SGSI de FNMT-RCM de alguna casuística específica no deberá considerarse como una autorización implícita para el uso o acceso a ningún recurso de información o sistema de tratamiento.

[22] Cualquier deficiencia o ambigüedad en el SGSI deberá ser notificada al responsable de Seguridad de la Información para su corrección inmediata.

7.3. Aprobación

[23] El Presidente – Director General de FNMT-RCM aprobará la presente política de Seguridad de la Información y se la dará difusión para que sea conocida y asumida por todos los miembros de la organización y terceros afectados.

[24] Esta política está sujeta a la ratificación por parte del Comité de Dirección de FNMT- RCM.

7.4. Entrada en vigor y aplicación

[25] La presente política tiene su entrada en vigor en la fecha de su aprobación.

7.5. Incumplimientos y sanciones

[26] Cualquier acción encaminada a reducir o eliminar la eficacia de los controles[D05] implementados para garantizar la Seguridad de la Información, para alterar las propiedades de Seguridad de la Información, o para dificultar o impedir la investigación de cualquier violación de la política de Seguridad de la Información y su normativa de desarrollo, será considerada una violación de confianza y podría ser causa de investigación y, en su caso, de las correspondientes acciones disciplinarias o legales contra los responsables.

[27] Se considerará falta grave:

[27.01] Violaciones malintencionadas de la política de Seguridad de la Información de FNMT-RCM y su normativa de desarrollo

[27.02] Distribución deliberada y sin aprobación de datos sensibles de FNMT-RCM.

[27.03] Cualquier comportamiento negligente que exponga a FNMT-RCM a responsabilidades legales, como puede ser la piratería de software.

[27.04] La realización de ataques informáticos contra los sistemas de FNMT-RCM o desde éstos contra terceros.

[28] La resolución de estas violaciones podrá dar lugar a acciones disciplinarias y, en su caso, responsabilidades legales, contra los responsables en función de la gravedad de los hechos y las posibles circunstancias agravantes o atenuantes, como pueden ser las reincidencias o el desconocimiento.

[29] La resolución de estos incidentes ser realizará según la legislación vigente y los procedimientos de FNMT-RCM.

7.5.1. Sanciones disciplinarias según lo dispuesto en el Convenio Colectivo

[30] Las faltas y las sanciones disciplinarias aplicables a la Seguridad de la Información, se encuentran recogidas en el Artículo 62 del XI Convenio Colectivo de FNMT-RCM, considerándose faltas muy graves.

[30.01] "Serán faltas muy graves:

…

La publicación o utilización indebida de la documentación o información a que tengan o hayan tenido acceso los trabajadores por razón de su cargo o función.

La negligencia en la custodia[D07] de secretos oficiales, declarados así por la Ley o clasificados como tales, que sea causa de su publicación o que provoque su difusión o conocimiento indebido.

…"

[31] Se castigarán con las sanciones disciplinarias estipuladas para faltas muy graves, descritas también en dicho Régimen.

[31.01] "Las sanciones que podrán imponerse en función de la calificación de las faltas serán las siguientes:

…

Por faltas muy graves:

Suspensión de empleo y sueldo de treinta y uno a noventa días. Inhabilitación para el ascenso por un periodo de dos a seis años. Traslado forzoso sin derecho a indemnización.

Despido."

7.5.2. Sanciones jurídicas según lo dispuesto en la legislación vigente

[32] La violación de la normativa de Seguridad de la Información podría dar lugar a su vez a infracciones descritas en la legislación vigente.

[33] Si un trabajador incumple las obligaciones descritas para el colectivo de "Usuarios" de FNMT-RCM y da acceso, difunde o utiliza información de forma indebida, podría estar incumpliendo el articulado del Título XIX, Capítulo IV, de la Ley Orgánica 10/1995, de

[34] 23 de noviembre, del Código Penal, por lo que se podrían aplicar las sanciones oportunas, tipificadas en dicha Ley.

7.6. Revisión y mejora

[35] El SGSI de FNMT-RCM, y en particular esta política, estará sometido a un proceso de revisión periódica y actualización permanente para garantizar su adecuación a las necesidades de la organización, a la legislación vigente y a los continuos avances tecnológicos.

[36] La entidad responsable de la revisión regular de la política de Seguridad de la Información de FNMT-RCM es el Comité de Seguridad.

[37] Estas revisiones podrán ser ejecutadas de forma específica ante cualquier cambio relevante que pudiera afectar a la Seguridad de la Información.

[38] No obstante, se establece un periodo mínimo de un año entre revisiones de la presente política.

8. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

[39] La documentación relativa a la Seguridad de la Información presenta la siguiente estructura:

[39.01] Política de Seguridad de la Información de FNMT-RCM: El presente documento.

[39.02] Políticas específicas: Conjunto de reglas sobre un aspecto específico de la gestión de la Seguridad de la Información. Son tecnológicamente independientes y su contenido es conforme a las recomendaciones internacionales y legislación de aplicación.

[39.03] Normas: Normativa general sobre Seguridad de la Información que desarrolla la presente política y cuyo objetivo es normalizar diferentes aspectos de la gestión de la Seguridad de la Información. Son tecnológicamente independientes y su estructura y contenido es conforme a las recomendaciones internacionales y legislación de aplicación.

[39.04] Guías: Desarrollan un aspecto concreto de las normas de Seguridad de la Información y describen directrices para realizar procesos de Seguridad de la Información (nivel operativo). Pueden ser tecnológicamente dependientes, por lo que pueden incluir información concreta relacionada con los controles y tecnologías empleadas por FNMT-RCM. Su contenido es conforme a las recomendaciones internacionales y legislación de aplicación.

[39.05] Procedimientos: Describen los pasos para realizar un determinado proceso de Seguridad de la Información (nivel operativo), así como las responsabilidades asociadas. Pueden ser tecnológicamente dependientes, por lo que pueden incluir información concreta relacionada con los controles y tecnologías empleadas por FNMT-RCM.

[39.06] Instrucciones técnicas: Describen y explican con detalle la metodología de realización de una determinada tarea o proceso (nivel operativo). Son tecnológicamente dependientes, por lo que incluyen información concreta relacionada con los controles y tecnologías empleadas por FNMT-RCM.

[39.07] Registros de seguridad: Estructuras de datos e información cuyo objetivo es controlar -y dejar evidencia- de la ejecución de determinadas tareas de Seguridad de la Información (nivel operativo).

[40] El desarrollo más inmediato de la presente política viene dado por un conjunto de normas (12) cuyos objetivos se describen a continuación.

[41] Estas normas serán publicadas y difundidas al objeto de que sean conocidas y asumidas por todo el personal de FNMT-RCM.

8.1. Gestión de riesgos de seguridad de la Información

[42] Establecer pautas para la gestión de riesgos de Seguridad de la Información en FNMT-RCM, las cuales se fundamentan la gestión cíclica del riesgo y tienen en cuenta los principios de la mejora continua.

[43] Desarrollar los criterios para la estimación y gestión del riesgo, incluyendo la aceptación del mismo.

[44] Definir cómo llevar a cabo la gestión de la Seguridad de la Información en los proyectos de FNMT-RCM.

8.2. Gestión y clasificación de los recursos de la información

[45] Proporcionar una categorización para la información, y por ende de los recursos de tratamiento de información, de FNMT-RCM, de forma que se proporcionen los criterios básicos para la protección de la información de manera proporcional y de acuerdo con la legislación vigente, su valor y los objetivos de FNMT-RCM.

[46] Establecer las medidas de seguridad mínimas a implementar para proteger la información de acuerdo con su clasificación.

[47] Definir la gestión de soportes en FNMT-RCM durante todo su ciclo de vida.

[48] El documento SGSI-202 Gestión de Activos y Clasificación de la Información, es la norma en la que se establece los criterios y directrices para la clasificación de la información y la documentación. En esta norma se establecen los criterios de la gestión de la documentación en materia de seguridad del sistema y los accesos. Asimismo, el documento SGSI-204 Control de acceso a los sistemas de información, indica cómo se llevan a cabo estos, criterios y regulación al respecto.

8.3. Seguridad relativa a los recursos humanos

[49] Reducir el riesgo de error, robo, fraude y uso inadecuado de la información de FNMT-RCM mediante el control de los procesos de gestión de personal propio y de terceros.

[50] Determinar las pautas a seguir en la gestión del personal antes del empleo, comprendiendo el proceso de selección y la inclusión de términos y condiciones relacionados con Seguridad de la Información en los contratos.

[51] Establecer los requerimientos para una adecuada gestión de los recursos humanos durante el empleo, especificando responsabilidades, detallando las reglas de FNMT- RCM relativas a formación y concienciación del personal, y describiendo el proceso disciplinario en la organización.

[52] Definir las directrices de Seguridad de la Información a tener en cuenta en FNMT-RCM durante la finalización del empleo o cambio en el puesto de trabajo.

8.4. Control de acceso a los sistemas de información

[53] Garantizar el control de acceso[D06] a la información y servicios de FNMT-RCM basado en los principios de "necesidad de conocer" y "mínimo privilegio".

[54] Definir las directrices de la gestión de usuarios y del control de acceso a sistemas y aplicaciones, estableciendo las responsabilidades correspondientes.

[55] Establecer las pautas del control de acceso a dispositivos móviles.

8.5. Seguridad física

[56] Proteger los recursos e instalaciones (salas, oficinas, locales) de FNMT-RCM, y la información contenida en ellos, de acuerdo con la legislación vigente, su valor y los objetivos de FNMT-RCM.

[57] Definir las áreas de seguridad establecidas en FNMT-RCM y los requerimientos aplicables a cada una de ellas.

8.6. Seguridad en la operación y las comunicaciones

[58] Asegurar el funcionamiento correcto y seguro de la operación de los sistemas y de las instalaciones de tratamiento de información, de modo que se mantenga un nivel aceptable de la Seguridad de la Información y se minimicen los riesgos.

[59] Garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.

[60] Asegurar la protección de la información en las redes, manteniendo la Seguridad de la Información que se transfiere dentro de una organización y con cualquier entidad externa.

8.7. Adquisición, desarrollo y mantenimiento de los sistemas de información

[61] Establecer pautas para la adquisición, desarrollo y mantenimiento de los sistemas de información, garantizando que la Seguridad de la Información es una parte integral de los mismos, a través de todo el ciclo de vida.

[62] Estas pautas afectan a cualquier componente de los sistemas de información (hardware y software).

8.8. Gestión segura de terceros

[63] Determinar las directrices para la gestión de proveedores, clientes y partners.

[64] Establecer las pautas en la relación y comunicación con las autoridades y con los grupos de interés.

[65] Describir los principales riesgos asociados a las relaciones con terceros y definir las directrices a seguir en cada caso para minimizar el impacto[D11] en la organización.

8.9. Gestión de incidentes de seguridad de la información

[66] Establecer los mecanismos preventivos que reduzcan la probabilidad de que se produzcan incidentes de seguridad[D12] de la información y faciliten su detección y/o resolución precoz en caso de producirse.

[67] Definir las pautas para identificar los incidentes de seguridad, reales o aparentes, y poder responder de forma eficiente y con arreglo a protocolos definidos al objeto de minimizar el daño, resolver el incidente, preservar evidencias y, finalmente, certificar las responsabilidades pertinentes.

[68] Para la correcta gestión y notificación de incidentes de seguridad de la información existe la guía SGSI-308 Guía de Gestión y Notificación de Incidentes de Seguridad de la Información, adaptada y adecuada a toda la normativa de aplicación a la FNMT-RCM, así como a la directiva europea NIS que regula esta materia.

8.10. Gestión de la continuidad del negocio

[69] Establecer los criterios para el desarrollo de planes de continuidad de negocio de la información y servicios de FNMT-RCM.

[70] Definir las medidas de seguridad adecuadas para reducir el riesgo de interrupción significativa de la operativa de los servicios de FNMT-RCM en caso de que ocurrieran incidentes graves o desastres, de modo que impacte lo menos posible en la organización.

[71] Para la correcta gestión, notificación y planes de contingencia adecuados a la gestión de la continuidad, existen en el sistema documental una serie de guías que regulan este punto en materia de gestión, notificación y demás, que cumple con la normativa que regula este punto.

8.11. Gestión del cumplimiento

[72] Asegurar el cumplimiento de la legislación vigente y de los requerimientos contractuales establecidos por FNMT-RCM con terceros.

[73] Definir las directrices para asegurar que la Seguridad de la Información se implementa y opera de acuerdo a la normativa interna y a los requisitos de negocio de FNMT-RCM.

[74] Proteger especialmente los datos de carácter personal que FNMT-RCM maneje en el ejercicio de sus actividades y de acuerdo con la legislación en la materia.

8.12. Mantenimiento de instalaciones

[75] Establecer las directrices a seguir para el mantenimiento de las instalaciones de la organización, gestionando de manera adecuada el equipamiento asociado y garantizando la seguridad de la información contenida en dichas instalaciones.

[76] Definir las medidas de seguridad adecuadas para reducir los riesgos asociados a la climatización, alimentación, cableado, etc.

9. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

[77] FNMT-RCM establecerá un marco de gestión para el control de la implementación y operación de la Seguridad de la Información.

[78] Las funciones y áreas de responsabilidad deben segregarse para reducir la posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de FNMT-RCM.

[79] A continuación, se definen todos los roles y responsabilidades en Seguridad de la Información.

9.1. Comité de Seguridad de la Información

[80] Para la coordinación de la Seguridad de la Información a nivel organizativo se compone un Comité de Seguridad de la Información formado por:

[80.01] Director Industrial.

[80.02] Director de la Fábrica de Papel (Burgos).

[80.03] Director de Sistemas de Información.

[80.04] Director de Seguridad.

[80.05] Director de Informática.

[80.06] Representante del Comité de Gestión del Prestador de Servicios de Confianza (CERES).

[80.07] Responsable de Seguridad de la Información.

[81] En función de los temas a tratar, se podrán incorporar puntualmente al Comité de Seguridad de la Información aquellas personas que se considere oportuno.

[82] Se considerará especialmente la invitación del Delegado de Protección de datos cuando se traten aspectos en materia de protección de datos de carácter personal y privacidad.

[83] Es responsabilidad del Comité de Seguridad de la Información:

[83.01] Atender las inquietudes de la alta dirección y de las diferentes partes interesadas del SGSI.

[83.02] Monitorizar los cambios en el contexto externo e interno de la organización que afecten al SGSI.

[83.03] Revisar regularmente el estado y el comportamiento de la Seguridad de la Información, abarcando:

[83.03.01] Acciones llevadas a cabo desde anteriores Comités de Seguridad.

[83.03.02] No conformidades y acciones correctivas.

[83.03.03] Resultados de auditoría.

[83.03.04] Seguimiento y resultados de mediciones.

[83.03.05] Cumplimiento de objetivos de Seguridad de Información.

[83.04] Identificar riesgos específicos para el negocio e informar al Presidente – Director General, el Comité de Dirección y, si fuera conveniente, al Consejo de Administración de FNMT-RCM.

[83.05] Revisar los resultados de las evaluaciones del riesgo de activos de la organización, así como los planes de tratamiento asociados.

[83.06] Monitorizar los riesgos de Seguridad de la Información.

[83.07] Aprobar planes de mejora de la Seguridad de la Información de FNMT-RCM. En particular velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.

[83.08] Coordinar los esfuerzos de las diferentes áreas en materia de Seguridad de la Información para asegurar que éstos son consistentes y están alineados con los objetivos de FNMT-RCM y con la estrategia de seguridad.

[83.09] Velar porque la Seguridad de la Información se tenga en cuenta en todos los proyectos, desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas de información.

[83.10] Priorizar las actuaciones en materia de Seguridad de la Información cuando los recursos sean limitados.

[83.11] Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad de la información y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas en la gestión de incidentes de seguridad de la información.

[83.12] Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones de FNMT-RCM en materia de seguridad.

[83.13] Promover la mejora continua del SGSI y los diferentes aspectos regulados en él, elaborando la estrategia de evolución de la organización en lo que respecta a Seguridad de la Información, incluyendo la revisión regular de la política de Seguridad de la Información de FNMT-RCM y la normativa de desarrollo.

[83.14] Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización.

[83.15] Nombrar un sustituto del Responsable de Seguridad de la Información que asumiría las funciones de éste si fuese necesario ante la ausencia del responsable titular.

9.2. Roles y funciones en la organización de la seguridad

[84] La asignación de roles, funciones y responsabilidades en materia de Seguridad de la Información está basada en el principio de "la seguridad como función diferenciada".

[85] Entre otros, se establecen los siguientes roles:

[85.01] Responsable de la Información.

[85.02] Responsable del Servicio.

[85.03] Responsable de la Seguridad de la Información.

[85.04] Responsable del Sistema.

[85.05] Administrador de la Seguridad del Sistema.

[85.06] Delegado de protección de datos

[86] De acuerdo con el principio de jerarquía que rige las administraciones públicas españolas, en caso de conflicto, éste deberá ser resuelto por el superior jerárquico.

[87] El Comité de Seguridad de la Información dará instrucciones al responsable de la Seguridad de la Información para el desarrollo del proceso de seguridad. Los diferentes roles actuarán conforme a las siguientes funciones y según lo establecido en la presente política y su desarrollo normativo.

9.2.1. Funciones del Responsable de la Información

[88] Los Responsables de la Información tienen la responsabilidad última del uso que se haga de la información en cuestión y, por tanto, de su protección. Para ello, deberán:

[88.01] Determinar los niveles y requisitos de Seguridad de la Información conjuntamente con el Responsable del Servicio que utiliza dicha información y, en caso de que hubiera datos de carácter personal, junto con el responsable del fichero correspondiente. Para esta tarea, podrán recabar una propuesta del Responsable de Seguridad de la Información y es conveniente que tengan en cuenta la opinión del Responsable del Sistema.

[88.02] Velar por la aplicación de los criterios definidos en la política y su normativa de desarrollo en los activos de información que están bajo su custodia. El cumplimiento de esta responsabilidad requerirá la cooperación de los Responsables de Sistemas y del Responsable de Seguridad de la Información.

[88.03] Designar al responsable de la gestión de los accesos a la información.

9.2.2. Funciones del Responsable del Servicio

[89] El Responsable del Servicio tiene la obligación de determinar los niveles y requisitos de seguridad del servicio conjuntamente con el responsable de la información que es utilizada por el servicio en cuestión.

[90] En los casos en que el servicio gestione información con diferentes niveles de seguridad se deberán aplicar los criterios más restrictivos.

9.2.3. Funciones del Responsable de Seguridad de la Información

[91] El Responsable de Seguridad de la Información deberá:

[91.01] Realizar el análisis de riesgos asociado a la información de FNMT-RCM.

[91.02] Desarrollar y coordinar el SGSI de FNMT-RCM y, en especial, la implementación de las políticas, normas, guías, procedimientos y soluciones de seguridad.

[91.03] Elaborar y mantener actualizada la política de seguridad, así como su normativa de desarrollo.

[91.04] Recomendar y aconsejar en la determinación de los niveles de seguridad aplicables a la información y las actividades de diseño, evaluación, selección e implementación de soluciones de seguridad de red y de sistemas.

[91.05] Tomar las decisiones oportunas para satisfacer los requisitos de seguridad.

[91.06] Supervisar la gestión de la Seguridad de la Información realizada por los diferentes departamentos de negocio de FNMT-RCM y el cumplimiento de la normativa de seguridad.

[91.07] Investigar las violaciones de seguridad de la información o incidencias relacionadas con la información de FNMT-RCM.

[91.08] Promover la formación y concienciación en materia de Seguridad de la Información dentro de su ámbito de responsabilidad.

[91.09] Convocar las reuniones del Comité de Seguridad de la Información y preparar los temas a tratar en el orden del día.

[91.10] Dirigir el Área de Seguridad de la Información y Normalización, que dispondrá de los medios técnicos y humanos necesarios para asumir todas las funciones que tiene asignadas.

9.2.4. Funciones del Responsable del Sistema

[92] La función principal de los Responsables de Sistemas es la de desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, verificando su correcto funcionamiento conforme a los objetivos del servicio y teniendo en cuenta la normativa de Seguridad de la Información aplicable.

[93] Para ello, entre otras cosas, deberá:

[93.01] Definir la topología y el SGSI estableciendo los criterios de uso y los servicios disponibles en el mismo conforme a las necesidades de los usuarios y la presente política de Seguridad de la Información y su normativa de desarrollo.

[93.02] Gestionar los sistemas y redes de comunicaciones que estén en el ámbito de sus competencias de acuerdo con las políticas, normas, guías y procedimientos de Seguridad de la Información vigentes, considerando, adicionalmente, la legislación aplicable.

[93.03] Cerciorarse de que se implementen las medidas específicas de seguridad establecidas en la normativa de aplicación y conforme al nivel de seguridad definido para el servicio que soporta el sistema o la información que maneja.

[94] Estas responsabilidades también son aplicables a otros empleados o terceros que gestionen sistemas de información o redes de comunicaciones en nombre de FNMT- RCM o que intervengan en los servicios de la misma.

9.2.5. Funciones del administrador de seguridad del sistema

[95] Este rol depende del responsable del sistema y sus funciones son:

[95.01] Implementar, gestionar y mantener las medidas de seguridad aplicables al sistema de Información.

[95.02] Si así lo determina el Responsable de la Información, gestionar las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización[D14] de que la actividad desarrollada en el sistema se ajusta a lo autorizado.

[95.03] Aplicar los procedimientos operativos de seguridad.

[95.04] Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.

[95.05] Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la Seguridad de la Información no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.

[95.06] Informar al Responsable de Seguridad de la Información y del Sistema de cualquier anomalía, compromiso o vulnerabilidad[D22] relacionada con la seguridad.

[95.07] Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

9.2.6. Delegado de protección de datos

[96] Las funciones el Delegado de Protección de datos serán las indicadas en el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016 y demás disposiciones reguladoras de la materia.

9.3. Asignación de roles y responsabilidades

[97] Para el desarrollo de la presente política y del SGSI de FNMT-RCM se realiza la siguiente asignación de roles, estableciendo en algunos casos responsabilidades específicas adicionales a las funciones definidas anteriormente para cada rol:

[97.01] El Comité de Seguridad nombrará al Responsable de Seguridad de la Información y, en caso de ser necesario, a su sustituto.

[97.02] Los Directores, responsables de la gestión de los distintos departamentos de negocio, deben:

[97.02.01] Cumplir con la legislación vigente en materia de seguridad, así como con la política y normativa de Seguridad de la Información.

[97.02.02] Proporcionar los recursos necesarios para el cumplimiento de la política.

[97.02.03] Designar a los Responsables de la Información y los Responsables del Servicio, pudiendo ser, en ambos casos, ellos mismos y ambas responsabilidades coincidir en la misma persona.

[97.02.04] Asegurar que las personas que gestionen el desarrollo y soporte de aplicaciones de negocio informáticas implementen, durante todo su ciclo de vida y a un coste razonable, los controles de seguridad derivados de la presente política, su normativa de desarrollo y los requisitos específicamente establecidos.

[97.02.05] Colaborar y facilitar la supervisión regular del cumplimiento de esta política, del SGSI y de la gestión de la Seguridad de la Información realizada en los departamentos.

[97.02.06] Colaborar y facilitar la información necesaria para la realización de los análisis de riesgos.

[97.03] Director de Sistemas de Información:

[97.03.01] Designará a los Responsables de Sistemas.

[97.03.02] Notificará a los Responsables de la Información y de Servicios las designaciones realizadas.

[97.04] Usuarios (empleados propios y de terceros): Todas las personas que gestionen o tengan acceso, directo o indirecto, a información de FNMT-RCM o sean usuarios de los sistemas de tratamiento de información (automatizados o manuales) tienen las siguientes responsabilidades:

[97.04.01] Cumplir con la legislación vigente, políticas, normas, guías y procedimientos de Seguridad de la Información y, en especial, en lo relativo al uso de los recursos de tratamiento de la información y de la propia información.

[97.04.02] Preservar la confidencialidad de la información, actuando con la máxima discreción y en su deber de secreto. En cualquier caso, toda la información

deberá manejarse con la discreción que el nivel de confidencialidad establecido requiera para la misma. A menos que se autorice de forma expresa, no está permitido divulgar información con una clasificación distinta a la de “pública” o de “libre difusión” en cualquiera de sus formas.

[97.04.03] Mantener los objetivos de seguridad sobre la información y sistemas que se encuentren bajo su responsabilidad o de los que sea propietario y aplicar los controles de seguridad definidos.

[97.04.04] No utilizar los recursos de tratamiento de la información o la información en sí misma para fines personales, quedando su uso limitado de forma exclusiva a las actividades propias de FNMT-RCM.

[97.04.05] Cooperar con los esfuerzos internos de desarrollo e implementación de controles y procedimientos de seguridad para la creación de un ambiente de control adecuado en el ámbito de la Seguridad de la Información.

[97.04.06] Estar alerta para detectar violaciones reales, aparentes o potenciales de esta política.

[97.04.07] Notificar cualquier incidencia de seguridad, incluyendo las violaciones de la presente política, de la que tengan evidencia o sospecha al Responsable de Seguridad de la Información. Lo anterior incluye cualquier pérdida o compromiso de cualquier credencial de acceso a los sistemas (contraseñas, tarjetas, tokens, etc.).

[97.04.08] Estas obligaciones son también de aplicación a los Responsables de la Información, de Servicios y Directores de los diferentes departamentos de negocio.

[97.05] Auditores: Tienen la responsabilidad de revisar periódicamente el desarrollo y grado de implantación del SGSI de FNMT-RCM y, en particular, verificar el efectivo cumplimiento de todos los aspectos reflejados en esta política, así como en las normas, guías y procedimientos que la desarrollan.

[98] FNMT-RCM se reserva el derecho de revisar cualquier información almacenada, intercambiada o procesada en sus sistemas de información, redes de comunicaciones o soportes de información con el fin de analizar el uso dado a esta información y tomar las medidas necesarias para garantizar el uso correcto de los mismos.

[99] FNMT-RCM se reserva el derecho de revocar las autorizaciones de sistema a cualquier usuario, tanto interno como externo, en cualquier momento.

[99.01.01]

[100] Se prohíbe cualquier comportamiento que interfiera con la operativa normal de los sistemas de información de FNMT-RCM, que pueda afectar de forma adversa a la capacidad de otros empleados para usar esos sistemas de información, o sea dañina u ofensiva para FNMT-RCM y sus empleados, clientes o colaboradores.

9.4. Relaciones con terceros

[101] Cuando FNMT-RCM preste servicios a otras entidades o maneje información de otros organismos, se les hará partícipes de la presente política y se establecerán canales para reporte y coordinación de los respectivos comités y responsables.

[102] Uno de los objetivos de esta participación será el del establecimiento de procedimientos de actuación para la prevención y reacción ante incidentes de seguridad.

[103] Se deberán establecer los correspondientes acuerdos de confidencialidad previa concesión de acceso a la información de FNMT-RCM por parte de un tercero y, en cualquier caso, éste deberá adherirse a la presente política de seguridad, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

[104] Cuando algún aspecto de la presente política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, será preciso un informe del responsable de Seguridad de la Información que identifique los riesgos en que se incurre y la forma de minimizarlos. Se requerirá la aprobación de este informe por parte de los responsables de la información y los servicios afectados antes de proceder con las relaciones con la entidad interesada.

[105] FNMT-RCM trata datos de carácter personal para el desempeño de sus actividades de negocio y soporte.

[106] Los documentos de seguridad relativos a los ficheros de datos de carácter personal propiedad de FNMT-RCM pueden encontrarse en el sistema de gestión documental corporativo y son accesibles por todas las partes implicadas (responsables y usuarios del fichero).

[107] Todos los sistemas de tratamiento de información de FNMT-RCM se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal tratados. Las medidas establecidas para su adecuada protección estarán recogidas en el correspondiente documento de seguridad.

10. DATOS DE CARÁCTER PERSONAL

[108] FNMT-RCM trata datos de carácter personal para el desempeño de sus actividades de negocio y soporte.

[109] Se aplicarán a los tratamientos de datos de carácter personal las medidas de seguridad requeridas en las siguientes normativas:

[109.01] 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).

[109.02] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

[109.03] 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 vigente en todas aquellas disposiciones que no contradigan el Reglamento General de Protección de Datos.

[109.04] Anexo II 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.

11. EXCEPCIONES E INCUMPLIMIENTOS

[110] Debido a requisitos legales, contractuales, técnicos u organizativos es posible requerir excepciones de la presente norma.

[111] En dicho caso y en aquellos en los que se detecte incumplimiento en la presente norma o en el marco normativo que lo desarrolla, se deberá proceder siguiendo la norma **SGSI-201 Gestión de riesgos de seguridad de la información** siguiendo las siguientes directrices:

[111.01] Analizar los riesgos derivados de las excepciones o incumplimientos.

[111.02] Establecer las medias oportunas proporcionalmente a los recursos y situación actual de la FNMT-RCM para reducir, o eliminar el riesgo.

[111.03] Aprobar el riesgo objetivo por el personal competente.

ANEXO 1. ACRÓNIMOS Y DEFINICIONES

A continuación, se incluye la relación de acrónimos y definiciones.

A1.1. Acrónimos

[A01] ***ASIN****: Área de Seguridad de la Información y Normalización.*

[A02] ***CCN****: Centro Criptológico Nacional.*

[A03] ***CISO****: Chief Information Security Officer. Oficial[D15] de Seguridad de la Información.*

[A04] ***ENS****: Esquema Nacional de Seguridad.*

[A05] ***FNMT-RCM****: Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda.*

[A06] ***IEC****: Comisión Electrotécnica Internacional.*

[A07] ***ISO****: Organización Internacional de Normalización. Organización Internacional de Estandarización.*

[A08] ***LOPD-GDD:*** *Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.*

[A09] ***RIS:*** *Responsable de la Información y/o Servicio.*

[A10] ***RSI:*** *Responsable de Seguridad de la Información.*

[A11] ***SGSI:*** *Sistema de Gestión de Seguridad de la Información.*

[A12] ***STIC****: Servicio de las Tecnologías de la Información y las Comunicaciones.*

[A13] ***UNE:*** *Asociación Española de Normalización.*

A1.2. Definiciones

[D01] ***ACTIVO****: Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.*

[d01.1] ***ACTIVOS ESENCIALES:*** *La información y los servicios proporcionados a los usuarios finales.*

[d01.2] ***ACTIVOS SUBORDINADOS****: Activos que forman parte de activos esenciales[D01].*

[D02] ***AMENAZA****: Eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.*

[D03] ***AUTENTICIDAD****: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.*

[D04] ***CONFIDENCIALIDAD:*** *Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.*

[D05] ***CONTROL o SALVAGUARDA:*** *Medida de seguridad que reduce, elimina un riesgo, o proporciona un mayor conocimiento del mismo.*

[D06] ***CONTROL DE ACCESOS:*** *Medio para asegurar que el acceso a los activos está autorizado y restringido en base a los requerimientos de negocio y seguridad.*

[D07] ***CUSTODIA:*** *Proceso en el cual se asegura que un activo es protegido frente a diferentes amenazas que puedan afectar a su confidencialidad, integridad o disponibilidad cuando este no está almacenado en un lugar definido como seguro.*

[D08] ***DATOS:*** *Representación de la información usando algún formato que permita su comunicación, interpretación, almacenamiento y procesado automático.*

[D09] ***DISPONIBILIDAD:*** *Propiedad o característica de los activos, consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.*

[D10] ***IDENTIFICACIÓN:*** *Proceso mediante el cual un usuario, proceso, aplicación u otra entidad proporciona información sobre quién o qué es.*

[D11] ***IMPACTO:*** *Consecuencia que sobre un activo tiene la materialización de una amenaza.*

[D12] ***INCIDENTE DE SEGURIDAD:*** *Suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información.*

[D13] ***INTEGRIDAD:*** *Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.*

[D14] ***MONITORIZACIÓN:*** *Determinación (verificación, supervisión u observación) del estado de un sistema, proceso o actividad.*

[D15] ***OFICIAL DE SEGURIDAD DE LA INFORMACIÓN****: O director de seguridad de la información es el responsable máximo en planificar, desarrollar, controlar y gestionar las políticas, procedimiento y acciones con el fin de mejorar la seguridad de la información dentro de los pilares fundamentales de confidencialidad, integridad y disponibilidad.*

[D16] ***PROCESO****: Conjunto organizado de actividades que se llevan a cabo para producir a un producto o servicio; tiene un principio y fin delimitado, implica recursos y da lugar a un resultado.*

[D17] ***RIESGO****: Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.*

[d17.1] ***ANÁLISIS DE RIESGOS:*** *Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.*

[D18] ***SERVICIO****: Función o prestación desempeñada por la organización o por un tercero destinada a cuidar intereses o satisfacer necesidades de los ciudadanos o clientes de la entidad.*

[D19] ***SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN****: Sistema de gestión que, basado en el estudio de los riesgos, se establece para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos.*

[D20] ***SISTEMA DE INFORMACIÓN****: Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.*

[D21] ***TRAZABILIDAD****: Posibilidad o capacidad de identificar el origen de un objeto o servicio desde un punto de origen a un punto final en un proceso de producción y/o distribución.*

[D22] ***VULNERABILIDAD:*** *Debilidad que puede ser aprovechada por una amenaza para causar un incidente.*