ÍNDICE DE CONTENIDOS

1. OBJETO

[01] El objetivo de la presente **Política** es establecer un marco integral, adecuado a las características de la FNMT-RCM (naturaleza, escala, complejidad y criticidad de sus actividades), que repercuta directamente en su entorno operativo, dependencias y cultura organizativa. Este marco permitirá:

- Identificar, desarrollar, implantar, operar, mantener, revisar y probar las medidas necesarias para garantizar la Continuidad de Negocio, asegurando el correcto funcionamiento de los planes establecidos ante la materialización de un incidente.
- Definir la organización y su contexto, considerando estatutos, misión, objetivos y marco legal y regulatorio.
- Detallar los principios básicos que deben regir las decisiones en materia de Seguridad, Privacidad y Continuidad, incluyendo objeto, alcance, aprobación, entrada en vigor, aplicación, incumplimientos, sanciones, revisión y mejora.
- Describir la documentación normativa que desarrolla la política y regula la gestión de activos, clasificación de la información y uso seguro de los sistemas.
- Organizar la Seguridad y Privacidad de la Información, incluyendo roles, responsabilidades y estructura de comités.
- Garantizar la confidencialidad, integridad y disponibilidad de la información y la prestación continuada de los servicios, actuando preventivamente y reaccionando con diligencia ante incidentes, protegiendo en todo momento la privacidad de los datos personales tratados.

2. ALCANCE

[02] El alcance de la presente Política abarca todos los servicios de negocio desarrollados por la FNMT-RCM en sus sedes de Madrid y Burgos, incluyendo los procesos de producción, personalización y los sistemas de información utilizados en las actividades. La sede principal se encuentra en Calle Jorge Juan, 106, Madrid.

[03] Esta política es de aplicación a:

- **Todo el personal** de la FNMT-RCM, así como a **visitantes, contratistas y terceras partes** que desarrollen actividades vinculadas con la organización.
- **Todos los sistemas de información**, infraestructuras y servicios que proporcionen soporte a la FNMT-RCM, así como a los usuarios que interactúan con dichos sistemas.
- **Procesos, servicios, información, instalaciones y proveedores**, que se apoyan principalmente en los sistemas gestionados por la **Dirección de Sistemas de Información y Económica-Financiera**.
- Aspectos relacionados con la **privacidad y protección de datos**, bajo la supervisión del **Delegado de Protección de Datos (DPD)** y el departamento de Asesoría Jurídica.

[04] Dentro de este alcance:

- Se **evalúan riesgos e impactos** de cualquier incidente que pueda afectar la continuidad de los servicios.
- Se **definen operaciones críticas**, roles y responsabilidades aplicables.
- Se establecen **objetivos y estrategias de prevención y gestión de crisis** para minimizar costes y daños ante amenazas.

[05] El presente documento, junto con aquellos que lo complementen, implementen o desarrollen, está sujeto a **revisiones y modificaciones**, comunicadas mediante los mecanismos oficiales de la organización. La última versión estará disponible en la **Intranet corporativa** para consulta por todas las partes interesadas.

[06] El **SGCN** y el **SGSIP** gobiernan toda la entidad, asegurando la **confidencialidad, integridad y disponibilidad** de la información y la prestación continuada de los servicios críticos, conforme al marco legal y normativo aplicable. El detalle del contexto y los servicios prestados se encuentra en el **Manual del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSIP 301)**.

3. PRINCIPIOS GENERALES

[07] La presente Política se sustenta en los siguientes principios y compromisos fundamentales, que garantizan la seguridad, privacidad y continuidad de negocio en la FNMT-RCM:

1. Protección y Seguridad Integral:

[08] Priorizar la protección de las personas, bienes y activos de la organización, tanto en condiciones normales como ante escenarios de contingencia o crisis.

[09] Adoptar un enfoque de **seguridad integral**, que incluya elementos técnicos, humanos, materiales y organizativos, con especial énfasis en la concienciación y formación de todo el personal.

2. Gobernanza y Responsabilidad:

[10] Establecer un modelo de gobierno claro para la gestión de la seguridad y continuidad, con roles y responsabilidades definidos para cada proceso, servicio y sistema.

[11] Designar representantes con experiencia en cada área para participar en la elaboración, implantación, revisión y actualización de los planes.

[12] Diferenciar funciones críticas: responsable de la información, del sistema, del servicio y de la seguridad.

3. Gestión del Riesgo y Mejora Continua:

[13] Basar la gestión de seguridad, privacidad y continuidad en el **análisis y gestión de riesgos**, manteniéndolo actualizado para minimizar amenazas a niveles aceptables.

[14] Revisar periódicamente el SGSIP, el SGCN y las medidas implantadas, adaptándolas a la evolución tecnológica, normativa y de riesgos.

[15] Aplicar el principio de **proporcionalidad en coste**, equilibrando medidas de seguridad con la naturaleza de la información y el presupuesto disponible.

4. Prevención, Reacción y Recuperación:

[16] Implementar medidas de prevención, detección y corrección para evitar que las amenazas se materialicen y, en caso de incidente, garantizar una recuperación rápida.

[17] Desarrollar estrategias y planes de recuperación que permitan restablecer procesos y servicios críticos dentro de los tiempos definidos en los planes de continuidad.

5. Continuidad del Negocio:

[18] Mantener planes de contingencia actualizados y probados periódicamente o ante cambios significativos en políticas, procesos, tecnología o personal.

[19] Dotar de medios y recursos necesarios para cumplir los objetivos del SGCN.

[20] Garantizar la prestación continua de servicios críticos y la recuperación inmediata ante contingencias.

6. Seguridad y Privacidad desde el Diseño:

[21] Incorporar la protección de datos y la seguridad de la información desde la fase inicial de diseño de sistemas y proyectos.

[22] Cumplir los principios del RGPD: licitud, lealtad, transparencia, limitación de finalidad, minimización de datos, exactitud, limitación del plazo de conservación y responsabilidad proactiva.

7. Principios de Privacidad Avanzada:

[22.01] **Desvinculación:** evitar la vinculación indebida de datos personales entre dominios.

[22.02] **Transparencia:** garantizar que el tratamiento de datos sea comprensible y reproducible por todas las partes implicadas.

[22.03] **Control:** permitir la intervención de los interesados para ejercer derechos y aplicar medidas correctivas.

8. Cultura de Seguridad:

[23] Promover la concienciación y formación continua del personal sobre seguridad, privacidad y continuidad.

[24] Fomentar la profesionalidad y la responsabilidad proactiva en la gestión de la seguridad.

9. Requisitos Mínimos de Seguridad:

[25] Considerando todos estos principios generales se identifican los siguientes requisitos mínimos de Seguridad y Continuidad que deben ser considerados:

[25.01] Organización e implantación del proceso de seguridad mediante una estructura clara y procesos efectivos.

[25.02] Autorización y control de accesos bajo el principio de mínimo privilegio.

[25.03] Protección física de instalaciones y seguridad lógica de sistemas.

[25.04] Actualización e integridad de sistemas mediante parches y controles.

[25.05] Protección de la información en reposo y en tránsito.

[25.06] Registro de actividad y detección de código dañino.

[25.07] Gestión y respuesta rápida ante incidentes de seguridad.

[25.08] Vigilancia continua y reevaluación periódica de los parámetros de seguridad.

[25.09] Mejora continua en los procesos y controles de seguridad.

4. NORMATIVA

[26] Sin ánimo de ser exhaustivos y sin perjuicio de la normativa específica aplicable a las actividades incluidas en el alcance del **SGSIP** y del **SGCN**, la presente política toma como referencia los siguientes marcos legales, reglamentarios y normativos:

[27] **En materia de sistemas de información y seguridad:**

- **Real Decreto 311/2022**, de 3 de mayo: Regula el **Esquema Nacional de Seguridad (ENS)**.
- **Directiva (UE) 2022/2555 (NIS2)**: Seguridad de redes y sistemas de información.
- **Directiva (UE) 2022/2557 (CER)**: Resiliencia de las entidades críticas.
- **Real Decreto-ley 12/2018**, de 7 de septiembre: Seguridad de redes y sistemas de información.
- **Real Decreto 43/2021**, de 26 de enero: Desarrollo del RD-ley 12/2018.
- **Real Decreto 4/2010**, de 8 de enero: Regula el **Esquema Nacional de Interoperabilidad**.
- **Reglamento (UE) 910/2014 (eIDAS)**: Identificación electrónica y servicios de confianza.
- **Ley 34/2002**, de 11 de julio: Servicios de la sociedad de la información y comercio electrónico.
- **Normas UNE-ISO/IEC 27001, 27002 y 27701**: Gestión de la seguridad y privacidad de la información.
- **ISO 22301**: Sistema de Gestión de la **Continuidad del Negocio**.

[28] **En materia de protección de datos personales:**

- **Reglamento (UE) 2016/679 (RGPD)**: Protección de datos personales.
- **Ley Orgánica 3/2018**, de 5 de diciembre: Protección de Datos Personales y garantía de derechos digitales.
- **Ley 59/2003**, de 19 de diciembre: Firma electrónica.

[29] **Otras referencias:**

- **Real Decreto 51/2023**, de 31 de enero: Estatuto de la FNMT-RCM como Entidad Pública Empresarial.

[30] Estas referencias constituyen el marco normativo que orienta la implantación, mantenimiento y mejora continua del **Sistema de Gestión de Seguridad y Privacidad de la Información (SGSIP)** y del **Sistema de Gestión de la Continuidad del Negocio (SGCN)**, asegurando el cumplimiento legal y la alineación con estándares internacionales.

5. ROLES Y RESPONSABILIDADES

[31] La FNMT-RCM ha definido las funciones y responsabilidades necesarias para garantizar el cumplimiento de los compromisos y directrices establecidos en esta política. La asignación de roles se realiza con los siguientes propósitos fundamentales:

- **Ratificar y difundir** la Política de Continuidad de Negocio en toda la organización.
- **Asignar y facilitar recursos y medios** para alcanzar los objetivos de continuidad y el nivel de riesgo aceptado.
- **Definir las estrategias de Continuidad de Negocio**, asegurando su alineación con los objetivos corporativos.
- **Gestionar, coordinar y responder** ante eventos disruptivos que puedan afectar procesos, servicios críticos o sistemas de información dentro del alcance definido.

[32] El modelo de gobierno de la continuidad del negocio y las funciones específicas se detallan en el **Documento de Funciones y Responsabilidades de la Continuidad del Negocio**, dentro del marco del **SGCN**.

[33] Asimismo, la asignación de roles en materia de **Seguridad de la Información y Privacidad** se basa en el principio de **"la seguridad como función diferenciada"**, estableciendo responsabilidades claras en los procesos que manejan información. Entre los roles definidos se incluyen:

- **Responsable de la Información**: Custodia y gestión del ciclo de vida de la información.
- **Responsable del Servicio**: Garantiza la prestación segura y continua del servicio.
- **Responsable de la Seguridad de la Información**: Supervisa el cumplimiento de las políticas y medidas de seguridad.
- **Responsable del Sistema**: Administra la infraestructura tecnológica que soporta los servicios.
- **Administrador de la Seguridad del Sistema**: Implementa y controla las medidas técnicas de seguridad.
- **Delegado de Protección de Datos (DPD)**: Punto de contacto para las partes interesadas en relación con el tratamiento de datos personales.

[34] De acuerdo con el principio de jerarquía, cualquier conflicto entre roles será resuelto por el órgano jerárquicamente superior.

[35] El **Comité de Seguridad Integral** emitirá instrucciones para el Responsable de la Seguridad de la Información conforme a las funciones establecidas en esta política y su normativa de desarrollo.

25388473S MARIA ISABEL VALLDECABRES (R: Q2826004J)

Firmado digitalmente por 25388473S MARIA ISABEL VALLDECABRES (R: Q2826004J)
Fecha: 2025.11.05 18:38:27 +01'00'