Política Local

Politica de Seguridad

NTT Spain Intelligent Technology and Services SL

General

5 de Febrero de 2025 | versión 2.0

Claudio Rodriguez Abad

Responsable de Seguridad
Risk & Compliance Senior Analyst

Indice

Historial de Revisiones

Version	Date	Comments
	12-Abril-2022	Politica de Seguridad pasa a denominarse Manual de Seguridad v13
2.00	5-Febrero-2025	Integración de la politica integrada de gestión, del grupo NTT Data inc y la del ENS

1. Introducción

NTT Spain Intelligent Technology and Services SL (en adelante 'NTT Spain') es una compañía multinacional, líder en su sector y que ofrece a sus clientes soluciones y servicios integrados de comunicaciones.

NTT Spain busca, a través de la calidad de sus soluciones y del servicio ofrecido, cubrir en todo momento las necesidades y expectativas de sus clientes, a través de siete pilares básicos: La rapidez, la excelencia, la confianza, el valor añadido, la integridad, el enfoque al cliente y el compromiso de sus empleados.

NTT Spain depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) proporcionados por el grupo NTT Data inc para alcanzar sus objetivos. Estos sistemas son 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 grupo NTT Data inc, la norma ISO 27001 y 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 requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo a las normas del grupo NTT Data inc, la ISO 27001, el manual de seguridad y el ENS.

1.1. Prevención

Los departamentos deben 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 los departamentos deben implementar las medidas mínimas de seguridad determinadas por el grupo NTT Data inc, la ISO 27001 y 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 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.

1.2. Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido por las normas del grupo NTT Data inc, las ISO 27001 y 20000-1 y el ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

1.3. Respuesta

Los departamentos 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 o en otros organismos.
- 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).

1.4. Recuperación

Para garantizar la disponibilidad de los servicios críticos, los departamentos deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

Los planes de Continuidad de NTT Spain están en la línea con las normas del grupo NTT Data inc, las ISO 27001 y 20000-1 y el ENS.

2. Alcance

Esta política se aplica a todos los miembros de la organización que soportan las actividades de negocio para el suministro, instalación y operación de soluciones integradas de comunicaciones para clientes de NTT Spain.

La política de seguridad está en sintonía con la del grupo NTT Data inc y con la política integrada de gestión de NTT Spain.

3. Misión

La Misión y Objetivos están recogidos en la política integrada del sistema de gestión de NTT Spain y son los siguientes:

- El Comportamiento ético y responsable.
- La respuesta rápida y eficaz a las necesidades de información, tanto de nuestros clientes externos como internos.
- La apuesta por el trabajo bien hecho y por la prevención y minoración de los riesgos, estableciendo los controles necesarios para asegurar la calidad del servicio, la preservación de los activos y de la información, la preservación ambiental y la seguridad de las personas.
- La apuesta conjunta con clientes y proveedores por la seguridad y la sostenibilidad, asegurando el cumplimiento de los requisitos tanto de clientes, como legales y reglamentarios, incluidos aquellos de carácter ambiental y los relativos a la seguridad de la información.
- El aprendizaje, innovación y mejora continua de todos los sistemas de gestión: Calidad, Medioambiente, Seguridad de la información y Gestión del servicio de tecnologías de la información.
- La formación y desarrollo permanente de todas las personas de su organización, que permitan mantener su apuesta por el aprendizaje, la innovación, y la calidad del servicio ofrecido.
- El compromiso de preservar la confidencialidad, integridad y disponibilidad de todos los activos de información física y electrónica en la organización, con el fin de que sean únicamente accesibles a las funciones que lo requieren y mantener su ventaja competitiva, la rentabilidad, el cumplimiento legal y contractual y la imagen comercial.
- El compromiso de mantener alineados los objetivos de la organización con los requisitos medioambientales y de seguridad de la información para reducir los riesgos a un nivel aceptable.

4. Marco Normativo

El marco normativo es el de toda la legislación, reglamentos y normativas nacionales e internacionales bajo las que opera NTT Spain, entre las que se encuentran:

- Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales.
- Ley Orgánica 7/2021 de protección de datos personales.
- Reglamento (UE) 2024/1689 de Inteligencia Artificial.
- Directiva (UE) 2022/2555 NIS2.
- Reglamento (UE) 2022/2554 de Resiliencia Operativa Digital del sector financiero (DORA).

NTT Spain por necesidades y cuestiones dentro del grupo NTT Data inc y por requisitos de clientes está sujeto a determinadas normas adicionales, entre las que caben destacar:

- ISO 9001
- ISO 14001
- ISO 27001
- ISO 20000-1
- Esquema Nacional de Seguridad. Real Decreto 311/2022.

5. Organización de la Seguridad

5.1. Comités: Funciones y Responsabilidades

El Comité Integrado del Sistema de Gestión tiene entre sus principales funciones constituir los comités de la Calidad, la Seguridad, el Servicio y la Sostenibilidad y está compuesto por los responsables de los principales procesos incluidos en los alcances de las ISOs 9001, 14001, 27001, 20000-1 y del ENS (Esquema Nacional de Seguridad).

Los responsables del Comité Integrado del Sistema de Gestión están nominados en cada uno de los procesos para el seguimiento y medición y sus funciones incluidas en el manual de gestión. El Comité realiza reuniones trimestrales de seguimiento y una reunión anual de revisión con el responsable de seguridad, el responsable del sistema y el comité de dirección. En la reunión anual se revisan las funciones e integrantes del comité y son reportados y aprobados por el Comité de Dirección.

Las principales responsabilidades y funciones de los Comités de Seguridad y del Servicio son la del seguimiento de los riesgos, los objetivos, indicadores y controles de la seguridad y del servicio.

La supervisión, la resolución de conflictos, la responsabilidad legal y la especificación de las necesidades o requisitos, corresponden al Comité de Dirección.

5.2. Roles: Funciones y Responsabilidades

Los roles y responsabilidades de la Seguridad de la Información de NTT Spain son los siguientes:

- El Responsable de la Información tiene la función de establecer los requisitos de la información en materia de seguridad y recae en el Comité integrado del Sistema de Gestión.
- El Responsable del Servicio determina los requisitos de los servicios prestados, es propietario de los riesgos del servicio y recae en el Comité del Servicio.
- El Responsable de Seguridad tiene las siguientes funciones:
    - Elaborar y proponer para aprobación por la organización las políticas de seguridad, que incluirán las medidas técnicas y organizativas, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados y para prevenir y reducir al mínimo los efectos de los ciberincidentes que afecten a la organización y los servicios.
    - Desarrollar las políticas de seguridad, normativas y procedimientos derivados de la organización, supervisar su efectividad y llevar a cabo auditorías periódicas de seguridad.
    - Elaborar el documento de Declaración de Aplicabilidad.
    - Actuar como capacitador de buenas prácticas en seguridad de las redes y sistemas de información, tanto en aspectos físicos como lógicos.
    - Constituirse como punto de contacto con la autoridad competente en materia de seguridad de las redes y sistemas de información y responsable ante aquella del cumplimiento de las obligaciones que se derivan del RD-l 12/2018 y de su Reglamento de Desarrollo.
    - Constituir el punto de contacto especializado para la coordinación con el CSIRT de referencia.
    - Notificar a la autoridad competente, a través del CSIRT de referencia y sin dilación indebida, los incidentes que tengan efectos perturbadores en la prestación de los servicios.
    - Recibir, interpretar y aplicar las instrucciones y guías emanadas de la Autoridad Competente, tanto para la operativa habitual como para la subsanación de las deficiencias observadas.

- Recopilar, preparar y suministrar información o documentación a la autoridad competente o el CSIRT de referencia, a su solicitud o por propia iniciativa.

- El Responsable del Sistema tiene las siguientes funciones:
  - Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
  - Definir la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.
  - Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad.

Los responsables de Seguridad, del Sistema, de la Información y del Servicio dependen jerárquicamente del Comité de Dirección.

5.3. Procedimientos de Designación

El Comité de Dirección designa a los responsables de la seguridad, del sistema y del tratamiento. Los nombramientos son revisados anualmente o cuando el puesto quede vacante y ratificados por el comité de dirección en la reunión anual del sistema integrado de gestión.

Los responsables de la Información y del Servicio son nombrados por los responsables de los procesos y departamentos incluidos en el alcance y ratificados por el Comité de Dirección. Los nombramientos son revisados anualmente o cuando el puesto quede vacante y y ratificados por el comité de dirección en la reunión anual del sistema integrado de gestión o en los seguimientos trimestrales.

5.4. Política de Seguridad de la Información

Será misión del Comité de Seguridad, la revisión anual de la Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de ésta. La Política será aprobada por el responsable de seguridad, ratificada por el comité de dirección y difundida para que la conozcan todas las partes afectadas.

6. Datos de Caracter Personal

NTT Spain trata datos de carácter personal pero no dispone de delegado de protección de datos personales o DPO debido a la naturaleza y volumen de la información personal tratada. La figura del DPO está representada dentro del grupo NTT Data inc.

Toda la información sobre medidas técnicas y organizativas, acuerdos de protección de datos, etc, están disponibles públicamente en la página de Data Privacy and Protection.

Todos los sistemas de información de NTT Spain se ajustan a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en los acuerdos de protección de datos.

7. Gestión de Riesgos

Todos los sistemas sujetos a esta Política realizan un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año
- Cuando cambie la información manejada
- Cuando cambien los servicios prestados
- Cuando ocurra un incidente grave de seguridad
- Cuando se reporten vulnerabilidades graves

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

8. Desarrollo de la Política de Seguridad de la Información

Esta Política de Seguridad de la Información complementa las políticas y normativas de seguridad de NTT Data inc disponibles en internet en la página de Policies and Statements.

La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

9. Obligaciones del personal

Todos los miembros de NTT Spain tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de NTT Spain atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de NTT Spain, en particular a los 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.

10. Terceras partes

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

Cuando NTT Spain utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está 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 del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.