

Medidas técnicas y organizativas

Privacidad y protección de datos

Contenido

Índice de Contenido

1.	**Introducción**	**3**
2.	**Medidas de Privacidad y Protección de Datos**	**4**
2.1.	Gobernanza y Modelo Operativo	4
2.2.	Políticas, procesos y directrices	4
2.3.	Protección de datos desde el diseño	4
2.4.	Mapa de datos	4
2.5.	Gestión del ciclo de vida de la información	4
2.6.	Derechos de los interesados	5
2.7.	Transferencias internacionales	5
2.8.	Regulación	5
2.9.	Formación y concienciación	5
2.10.	Seguridad para la privacidad	6
2.11.	Respuesta y notificación de brechas de datos	6
2.12.	Gestión de terceros	6
3.	**Medidas de seguridad de la información**	**7**
3.1.	Funciones y responsabilidades de la seguridad de la información	7
3.2.	Políticas de seguridad de la información	7
3.3.	Gestión de dispositivos móviles	7
3.4.	Recursos humanos	7
3.5.	Uso aceptable	7
3.6.	Controles de acceso	8
3.7.	Gestión y clasificación de activos	8
3.8.	Seguridad física y ambiental	8
3.9.	Seguridad operativa	9
3.10.	Adquisición, desarrollo y mantenimiento de sistemas	9
3.11.	Gestión de terceros	9
3.12.	Gestión de incidentes de seguridad de la información	9
3.13.	Continuidad del negocio	9
3.14.	Compliance	9

Introducción

Desde consultoría estratégica hasta las tecnologías de vanguardia, NTT DATA ofrece experiencias que transforman organizaciones para conseguir sus objetivos de negocio, revolucionan industrias y crean una sociedad mejor para todos.

Nuestras medidas técnicas y organizativas describen cómo garantizamos la protección de los datos personales de manera transparente, justa, ética y legal. Éstas se basan en las mejores prácticas de la industria y en los requisitos legales aplicables en las jurisdicciones en las que operamos, teniendo en cuenta la naturaleza de los datos procesados y el coste de implementación.

Si tiene preguntas sobre estas medidas o su relación con nuestros productos, servicios y soluciones, por favor contacte a su client manager.



Nuestras medidas técnicas y organizativas describen cómo garantizamos la protección de los datos personales de manera transparente, justa, ética y legal.

Medidas de Privacidad y Protección de Datos

2.1. Gobernanza y Modelo Operativo

NTT DATA está comprometida con la responsabilidad en el procesamiento de datos personales. Contamos con estructuras organizativas específicas y roles definidos para gestionar y supervisar el procesamiento de datos personales.

En cada jurisdicción donde operamos, se requiere que las unidades organizativas asignen los recursos apropiados para cumplir con las leyes de protección de datos. Esto incluye el nombramiento de especialistas en privacidad de datos para supervisar el cumplimiento y establecer estructuras de reporting adecuadas.

Periódicamente, NTT DATA informa a la alta dirección sobre el diseño y la efectividad operativa de sus actividades de privacidad y protección de datos.

2.2. Políticas, procesos y directrices

NTT DATA implementa y comunica sus políticas, procesos, estándares y directrices que detallan cómo se espera que los empleados de NTT DATA procesen los datos personales.

NTT DATA define e implementa avisos de privacidad que proporcionan información a los empleados, clientes y otras partes interesadas sobre cómo se procesan los datos personales.

NTT DATA implementa procesos y plantillas para realizar evaluaciones de riesgos, incluidas las evaluaciones de impacto de la protección de datos (EIPD), las evaluaciones de interés legítimo (LIA) y las evaluaciones de riesgos de transferencias internacionales (TIA), de acuerdo con las leyes de protección de datos aplicables.

2.3. Protección de datos desde el diseño

NTT DATA se compromete a implementar medidas razonables para respaldar la capacidad de sus clientes para cumplir con las leyes de protección de datos. En la medida de lo posible, los principios de protección de datos desde el diseño y por defecto se aplican durante el desarrollo de los productos, servicios y soluciones de NTT DATA.

2.4. Mapa de datos

NTT DATA ha implementado procesos para identificar, registrar, evaluar y analizar los datos personales que procesa.

NTT DATA mantiene un registro de los datos personales procesados de acuerdo con las leyes de protección de datos aplicables.

2.5. Gestión del ciclo de vida de la información

NTT DATA ha implementado políticas y procesos para garantizar que los datos personales se procesen adecuadamente en todo su ciclo de vida (desde la recopilación hasta el uso, la retención, la divulgación y la destrucción).

NTT DATA mantiene políticas y programas de retención de datos, que están alineados con las leyes aplicables. NTT DATA conserva los datos personales solo cuando existe una razón comercial legítima para hacerlo, y de acuerdo con sus obligaciones legales. NTT DATA destruye, elimina o anonimiza los datos personales cuando expira el período de retención y no existe un interés comercial legítimo para conservar los datos personales durante un período más largo.

NTT DATA conserva los datos personales procesados en nombre de sus clientes de acuerdo con los requisitos del cliente y destruirá, eliminará, anonimizará o devolverá de forma segura los datos personales cuando se soliciten y cuando no existan más obligaciones de conservar los datos personales en virtud de la legislación aplicable.

NTT DATA realiza todos los esfuerzos razonables para garantizar que los datos personales sean precisos, completos y estén actualizados.

2.6. Derechos de los interesados

Las leyes de protección de datos de ciertos países otorgan a los interesados derechos específicos en relación con sus datos personales. NTT DATA se compromete a defender estos derechos y a responder a las solicitudes de los interesados de manera oportuna, transparente, justa, ética y legal.

NTT DATA ha implementado políticas y procedimientos adecuados para defender los derechos de los interesados de acuerdo con las leyes de protección de datos aplicables.

NTT DATA respalda los siguientes derechos de los interesados:

- Derecho a ser informado
- Derecho de acceso
- Derecho de rectificación
- Derecho al olvido
- Derecho a la portabilidad de los datos
- Derecho a la limitación del tratamiento
- Derecho de oposición (incluido el derecho a excluirse del marketing directo y de la venta de datos personales)
- Derecho a impugnar las decisiones automatizadas
- Derecho a la no discriminación
- Derecho de reclamación

NTT DATA garantiza que los interesados dispongan de los canales adecuados para que puedan ejercer sus derechos en relación con los datos personales que NTT DATA pueda tratar sobre ellos.

NTT DATA mantiene un registro de todas las solicitudes de los interesados recibidas y las acciones tomadas en respuesta a estas solicitudes.

NTT DATA proporcionará todo el apoyo razonable a los clientes para responder a las solicitudes de los interesados, de conformidad con los acuerdos existentes.

NTT DATA ha establecido políticas y procedimientos para responder a las solicitudes de las autoridades para acceder a los datos personales de acuerdo con las leyes aplicables y los requisitos contractuales. NTT DATA mantiene un registro de estas solicitudes y sus resultados.

2.7. Transferencias internacionales

NTT DATA establece las salvaguardas adecuadas (como decisiones de adecuación, cláusulas contractuales estándar y otras herramientas establecidas en la legislación aplicable) al participar en transferencias de datos transfronterizas.

Cuando los datos personales se transfieren a través de las fronteras, NTT DATA realiza evaluaciones de impacto de la transferencia (TIA) para garantizar que el país de destino ofrezca un nivel de protección de los derechos y libertades de los interesados equivalente al país donde se recopilaron originalmente los datos. En caso de que no exista dicha equivalencia, evaluaremos y adoptaremos medidas complementarias para respaldar los derechos de los interesados de conformidad con nuestras políticas y requisitos legislativos. En caso de que no se puedan implementar dichas medidas complementarias, NTT DATA evitará la transferencia de datos personales.

NTT DATA se basa en cláusulas contractuales estándar para respaldar la transferencia legal de datos personales fuera del país donde se recopilaron originalmente. Para respaldar dichas transferencias, se han establecido acuerdos apropiados con las subsidiarias, las empresas del grupo, las filiales, los encargados, subencargados y clientes de NTT DATA.

2.8. Regulación

NTT DATA supervisa los cambios en las leyes de protección de datos en los países en los que opera y ha implementado procesos y herramientas para respaldar el cumplimiento.

2.9. Formación y concienciación

NTT DATA se compromete a implementar una cultura de concienciación y cumplimiento a través de iniciativas continuas de formación y concienciación. Requerimos que todos los empleados completen una capacitación obligatoria sobre privacidad y protección de datos de forma periódica. Los materiales de capacitación y las políticas, procesos, normas y directrices relacionadas están disponibles para los empleados y se comunican regularmente. Cuando sea necesario, se proporciona formación local, regional o funcional para ayudar a los empleados a actuar de acuerdo con los requisitos de determinados países, regiones o sectores.

2.10. Seguridad para la privacidad

NTT DATA ha implementado medidas técnicas y organizativas adecuadas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales, teniendo en cuenta el estado de la técnica, el coste de implementación y la naturaleza, el alcance, el contexto y la finalidad del tratamiento de los datos personales, así como los riesgos para los derechos y libertades de los interesados.

Las metodologías de seguridad de NTT DATA están alineadas con la norma ISO 27001 y el Marco de Ciberseguridad (CSF) del Instituto Nacional de Estándares y Tecnología (NIST).

2.11. Respuesta y notificación de brechas de datos

NTT DATA cuenta con políticas, procesos y procedimientos para identificar, detectar, responder y recuperarse de una violación de datos personales, así como para notificar a las partes interesadas correspondientes en caso de dicha violación. Estos incluyen mecanismos para realizar un análisis de causa raíz y emprender acciones correctivas.

NTT DATA se compromete a garantizar que las autoridades de protección de datos aplicables, los clientes afectados y los interesados afectados sean notificados en caso de brecha de datos personales, de conformidad con las leyes de protección de datos aplicables y cualquier compromiso contractual.

NTT DATA mantiene un registro de todas las brechas de datos personales y las acciones tomadas en respuesta a estos eventos.

La Sección 3: Medidas de seguridad de la información describe nuestras medidas de gestión de incidentes para identificar, detectar, responder y recuperarse de incidentes de seguridad de la información.

2.12. Gestión de terceros

NTT DATA es responsable de las acciones de los encargados y subencargados que procesan datos personales en nuestro nombre. Evaluamos la capacidad de estos encargados y subencargados para proteger los datos personales de acuerdo con los estándares de NTT DATA en el momento de la selección y de forma periódica a partir de entonces.

Los encargados y subencargados de NTT DATA están obligados a firmar los acuerdos apropiados que rigen el procesamiento y la protección de datos personales. Estos acuerdos incluyen requisitos para garantizar que las mismas obligaciones se transfieran a cualquier otro procesador que pueda procesar datos personales.



Medidas de seguridad de la información

NTT DATA se compromete a garantizar que la seguridad de la información se implemente y se gestione adecuadamente para proteger la confidencialidad, integridad y disponibilidad de los datos personales.

NTT DATA ha establecido políticas, procesos, procedimientos, estándares y directrices adecuados para garantizar la seguridad de los datos que procesa. Las metodologías de seguridad de NTT DATA están alineadas con la norma ISO 27001, así como con otras mejores prácticas de la industria.

3.1. Funciones y responsabilidades de la seguridad de la información

Se han asignado formalmente las funciones y responsabilidades en materia de seguridad de la información, incluido un CISO global y sus representantes locales junto a una oficina de seguridad de la información corporativa que da servicio a toda la organización, con líneas jerárquicas que garantizan la independencia de la función.

Los empleados de NTT DATA son responsables de actuar de acuerdo con nuestras políticas, procesos, normas y directrices de seguridad de la información en sus actividades comerciales diarias.

3.2. Políticas de seguridad de la información

NTT DATA ha documentado y publicado un conjunto de políticas de seguridad de la información. Estas políticas y la documentación de respaldo se revisan periódicamente.

3.3. Gestión de dispositivos móviles

NTT DATA ha establecido un marco de arquitectura Zero Trust para implementar y mantener controles de seguridad para acceder e interactuar con los sistemas y activos de información de NTT DATA. Este marco incluye:

- Políticas de administración de dispositivos de usuario final (EDM) y procedimientos de soporte.
- Controles y herramientas para mantener la seguridad.
- Confidencialidad, disponibilidad e integridad de los datos de la empresa. Estos datos podrían estar alojados o ser accesibles a través de los dispositivos de los usuarios finales (incluidos teléfonos móviles, tabletas y dispositivos que permiten el acceso remoto).

3.4. Recursos humanos

NTT DATA realiza una investigación de antecedentes y empleo de sus empleados, en la medida en que lo permita la ley aplicable, para validar su idoneidad para la contratación y para el manejo de la información de la empresa y del cliente (incluidos los datos personales). El alcance de la evaluación es proporcional a los requisitos comerciales y la clasificación de la información a la que tendrá acceso el empleado.

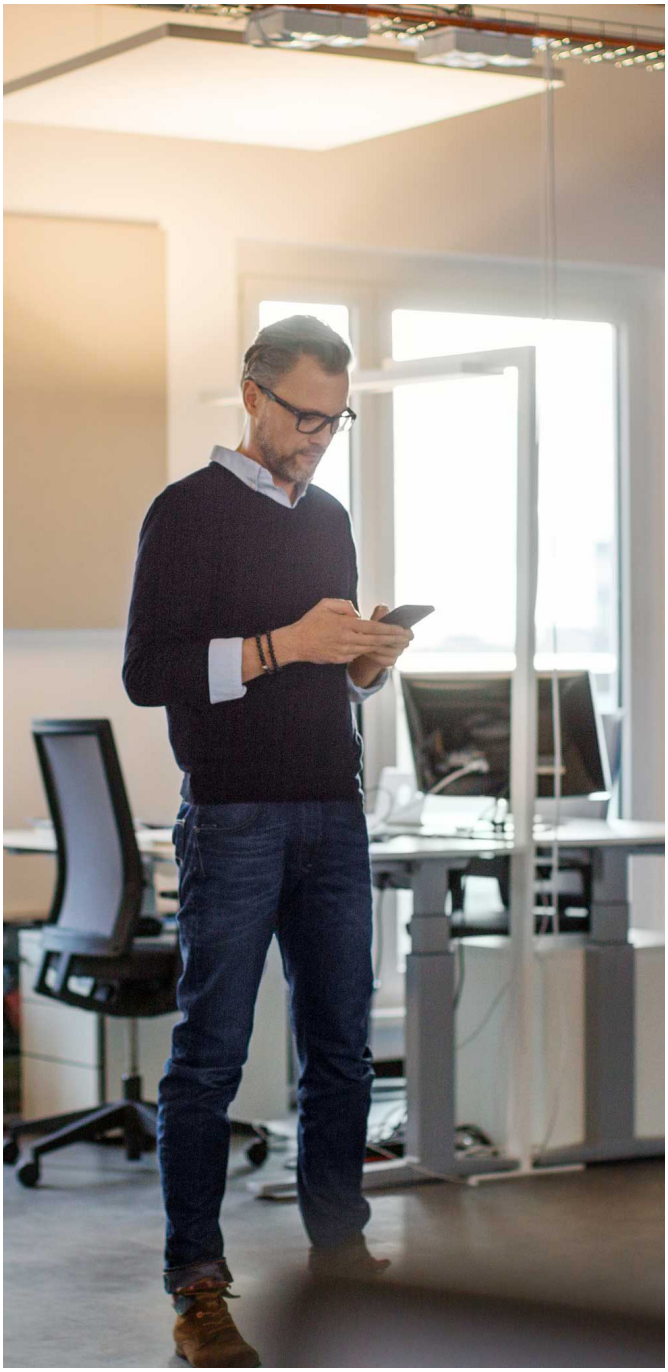
NTT DATA exige que todos los empleados (incluidos los subcontratados y los empleados temporales) se comprometan a mantener la confidencialidad de los datos de la empresa y de los clientes (incluidos los datos personales).

Los empleados de NTT DATA deben completar una formación sobre seguridad de la información y una capacitación de actualización periódica. Las políticas de seguridad de la información y los procedimientos, procesos y directrices de apoyo se ponen a disposición de los empleados. Los empleados también reciben información relevante sobre tendencias, amenazas y mejores prácticas. Periódicamente se llevan a cabo campañas de concienciación sobre la seguridad para garantizar una concienciación continua.

3.5. Uso aceptable

NTT DATA ha establecido políticas que respaldan el uso adecuado y eficaz de nuestros activos de información, que incluyen recursos informáticos y de comunicaciones, productos, servicios, soluciones e infraestructura de TI.

NTT DATA ha establecido políticas de clasificación de información para respaldar los controles adecuados para el manejo de información en función de su clasificación. La información y los activos se protegen de acuerdo con la etiqueta de clasificación.



> “Las metodologías de seguridad de NTT DATA están alineadas con la norma ISO 27001, así como con otras mejores prácticas de la industria.”

3.6. Controles de acceso

NTT DATA ha establecido políticas de control de acceso, procedimientos de apoyo y medidas de acceso lógico y físico para garantizar que solo las personas autorizadas tengan acceso a la información, sobre la base de los principios de privilegio mínimo.

Cuando corresponda, NTT DATA ha aplicado el cifrado estándar de la industria en reposo y en tránsito para garantizar que los datos personales estén protegidos contra cualquier acceso o divulgación no autorizados.

Las revisiones de acceso se realizan periódicamente para garantizar que solo las personas autorizadas tengan acceso a los sistemas y activos de información de NTT DATA.

NTT DATA ha realizado esfuerzos razonables para limitar el número de usuarios que tienen acceso privilegiado a los sistemas y activos de información de NTT DATA.

NTT DATA no permite compartir cuentas o credenciales a menos que esto haya sido aprobado a través del proceso de gestión de excepciones correspondiente.

3.7. Gestión y clasificación de activos

NTT DATA ha establecido políticas que rigen la clasificación y el manejo de los activos físicos y electrónicos, incluida la eliminación segura de los activos, para garantizar que la información esté protegida al nivel adecuado.

Los activos se basan en la criticidad del negocio para determinar los requisitos de confidencialidad. La guía de la industria para el manejo de datos personales proporciona el marco para las salvaguardas técnicas, organizativas y físicas. Estas salvaguardas pueden incluir controles como la gestión del acceso, el cifrado, el registro y la supervisión, y la destrucción de datos.

3.8. Seguridad física y ambiental

NTT DATA ha implementado medidas razonables y apropiadas de acuerdo con nuestras políticas de seguridad física para evitar el acceso físico no autorizado o el daño o la interferencia con la información, las aplicaciones, los sistemas, las bases de datos y la infraestructura. Entre ellas se encuentran:

- Controles de acceso físico
- Supervisión y auditoría del acceso físico
- Protección contra los peligros medioambientales
- Protección de los activos físicos
- Manejo de activos físicos
- Mantenimiento y destrucción de activos físicos
- Prácticas de escritorio y pantalla limpias
- Acceso y supervisión de visitas

3.9. Seguridad operativa

NTT DATA ha establecido equipos de especialistas apropiados que son responsables de administrar y proteger los sistemas de información y la infraestructura de NTT DATA.

NTT DATA ha establecido políticas y procedimientos de apoyo para gestionar los cambios en los procesos de negocio, los sistemas de información y la infraestructura. NTT DATA ha establecido varias estructuras de gobernanza para revisar y aprobar cualquier cambio en función del tamaño y el alcance del cambio y los objetivos estratégicos. Todas las solicitudes y sus resultados se registran y documentan.

NTT DATA ha establecido programas de gestión de amenazas y vulnerabilidades, respaldados por herramientas estándar de la industria, para identificar, administrar y mitigar los riesgos para la información de la empresa, incluidos los datos personales de empleados y clientes. Esto incluye la detección y respuesta de endpoints (EDR) de última generación para herramientas antivirus y antimalware, el análisis regular de entornos, los protocolos de aplicación de parches y la administración de actividades de corrección y mejora.

Los requisitos de capacidad se supervisan continuamente y se revisan periódicamente. Los sistemas y las redes se gestionan y escalan de acuerdo con estas revisiones.

La disponibilidad del sistema incluye arquitectura, diseño de alta disponibilidad, recuperación ante desastres y/o copias de seguridad en función de los requisitos de riesgo y disponibilidad de cada sistema. El método para mantener la disponibilidad o recuperación del sistema, incluido el alcance y la frecuencia de las copias de seguridad, está determinado por los requisitos comerciales de NTT DATA, incluidos los requisitos del cliente, y la criticidad de la información. Los planes de recuperación ante desastres se prueban periódicamente. Los procesos de copia de seguridad se supervisan para garantizar la finalización correcta de las copias de seguridad, así como para gestionar cualquier problema, excepción o error de copia de seguridad.

NTT DATA realiza esfuerzos razonables para mantener el registro de auditoría en las aplicaciones y los sistemas. Los registros se revisan periódicamente y están disponibles para fines de investigación. El acceso a los registros está estrictamente limitado únicamente al personal autorizado.

3.10. Adquisición, desarrollo y mantenimiento de sistemas

NTT DATA ha establecido un marco de arquitectura Zero Trust para regir el diseño, la adquisición, el desarrollo y el mantenimiento de los sistemas y la arquitectura de la información.

Existen políticas de arquitectura y diseño, así como normas y procedimientos de apoyo, para garantizar que los principios de seguridad por diseño se apliquen en el ciclo de vida del desarrollo de software.

3.11. Gestión de terceros

NTT DATA ha establecido políticas y prácticas para la gestión de terceros con el fin de garantizar que los activos de información estén protegidos cuando NTT DATA contrata a proveedores de servicios y/o encargados de terceros. Estos incluyen requisitos para la debida diligencia en materia de seguridad de la información y evaluaciones de riesgos de seguridad de la información que se deben realizar para garantizar que:

- Los requisitos de seguridad de la información están claramente articulados y documentados en acuerdos de acuerdo con los estándares de seguridad de la información de NTT DATA.
- Los proveedores de servicios y encargados de tratamiento de NTT DATA implementan el mismo nivel de protección y control que NTT DATA.
- Los proveedores de servicios y encargados de tratamiento están obligados a informar de cualquier incidente de seguridad de la información presunto o real a NTT DATA de manera oportuna.

3.12. Gestión de incidentes de seguridad de la información

NTT DATA cuenta con políticas, procesos y procedimientos para identificar, detectar, responder y recuperarse de un incidente de seguridad de la información, incluidas las violaciones de datos personales, y notificar a las partes interesadas correspondientes en caso de que se produzca un incidente de este tipo. Estos incluyen mecanismos para realizar un análisis de causa raíz y emprender acciones correctivas para remediar y evitar que vuelva a ocurrir.

NTT DATA ha establecido operaciones de seguridad en toda la empresa para supervisar y gestionar de forma proactiva todos los activos informáticos y de red. Estas operaciones están respaldadas por herramientas técnicas para la respuesta y recuperación de incidentes de seguridad de la información.

3.13. Continuidad del negocio

NTT DATA ha establecido planes de continuidad del negocio y recuperación ante desastres. NTT DATA ha adoptado un enfoque por capas para la continuidad del negocio con el fin de garantizar la disponibilidad de los sistemas y los datos.

3.14. Compliance

NTT DATA ha establecido funciones y responsabilidades para identificar las leyes y regulaciones que afectan nuestras operaciones comerciales. La responsabilidad del cumplimiento de las leyes y regulaciones se establece a nivel de grupo y regional para garantizar que NTT DATA cumpla con los requisitos globales y locales.


NTT DATA