Medidas Técnicas y Organizativas

En NTT es nuestra visión, a través de la tecnología y la innovación, permitir un futuro seguro y conectado. Hemos establecido nuestras Medidas Técnicas y Organizativas NTT (TOMs) que describen cómo garantizamos la protección de datos personales de una manera transparente, justa, ética y legal.

Nuestras TOMs se basan en las mejores prácticas del sector y en los requisitos legales aplicables en jurisdicciones en las que operamos teniendo en cuenta la naturaleza de los datos que procesamos y el costo de implementación.

Contenido

(A) Privacidad y Protección de Datos

1 Gobernanza y Modelo Operativo

1.1 NTT está comprometido demostrar la rendición de cuentas cuando NTT procesa datos personales y haya implementado una estructura organizativa, así como funciones y responsabilidades para gestionar y supervisar el tratamiento de datos personales.

1.2 Se han puesto en práctica varias estructuras de gobernanza para garantizar que las cuestiones relativas a la privacidad y la protección de los datos sean examinadas por la administración apropiada en el marco de la NTT. La Junta de NTT Ltd es la responsable última de la privacidad y la protección de datos y está respaldada por funciones designadas en toda la empresa, incluidos los responsables designados de protección de datos o funciones equivalentes, cuando así lo exijan las leyes de protección de datos.

2 Políticas, procesos y directrices

2.1 NTT ha implementado y comunicado sus políticas, procesos, estándares y directrices que detallan cómo se espera que los empleados de NTT procesen datos personales.

Esto incluye las siguientes políticas:

2.1.1 Privacidad de datos y Política de protección de datos;

2.1.2 Política de derechos del sujeto de datos; y

2.1.3 Directiva de notificación para violaciones de datos personales.

2.2 NTT ha definido y comunicado avisos de privacidad que proporcionan información a empleados, clientes y otros interesados acerca de cómo se procesan los datos personales.

2.3 NTT tiene un proceso de evaluación del impacto de la protección de datos ("DPIA") y realiza los DPIA cuando es necesario y de conformidad con las leyes de protección de datos.

3 Protección de datos por diseño

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

4 Panorama de datos

4.1 NTT ha implementado procesos para identificar, registrar, evaluar y mantener un entendimiento de los datos personales que trata NTT.

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

5 Administración del ciclo de vida de la información

5.1 NTT ha implementado políticas y procesos para garantizar el tratamiento adecuado de los datos personales todo su ciclo de vida (desde la recopilación hasta el uso, retención, divulgación y destrucción).

5.2 En algunos países, las leyes de protección de datos otorgan a los interesados derechos específicos en relación con sus datos personales. NTT se compromete a defender estos derechos y a garantizar que NTT responda solicitudes de los interesados en los datos en forma transparente, justa, ética y de manera legal.

5.3 NTT ha implementado una política de derechos de los sujetos de datos y un proceso de solicitudes de sujetos para defender los derechos de los sujetos de acuerdo con las l eyes de protección de datos aplicables.

5.4 NTT mantiene un registro de todas las solicitudes de datos recibidas y las medidas adoptadas para responder a esas solicitudes. NTT proporcionará todo apoyo razonable a los clientes para responder a las solicitudes de los interesados, cuando así se les solicite, y de conformidad con los acuerdos con ellos.

5.5 NTT mantiene una Política de Retención de Datos y un programa que se ajustan a las leyes aplicables. NTT sólo conserva datos personales cuando existe un propósito comercial legítimo y de conformidad con sus obligaciones legales. NTT destruye, elimina o desidentifica los datos personales cuando el período de retención termina y no hay razón comercial legítima para retener los datos personales durante un período más largo.

5.6 NTT mantiene los datos personales procesados por cuenta de sus clientes de acuerdo con los requisitos del cliente y destruirá, borrará, desidentificará o devolverá los datos personales cuando se solicite, al cliente, y cuando no haya otras obligaciones de conservar los datos personales con arreglo a la legislación aplicable.

5.7 NTT ha realizado todos los esfuerzos razonables para garantizar que los datos personales sean correctos, completos y actualizados.

5.8 La NTT se basa en las cláusulas contractuales estándar para apoyar la transferencia legal de datos personales fuera del país en el que estaba recogidos riginalmente y que hayan establecido acuerdos adecuados con las filiales, filiales, transformadores de NTT, subencargados y clientes para apoyar las transferencias transfronterizas.

6 Capacitación y sensibilización en materia de protección y privacidad de los datos

6.1 NTT requiere que todos los empleados completen la formación sobre la protección y la privacidad de datos en un base anual. Todas las políticas, procesos, normas y directrices sobre la protección y la privacidad de datos están a disposición de los empleados y se comunican periódicamente. Cuando es necesario, también se imparte capacitación local, regional o funcional para ayudar a los empleados a actuar de conformidad con los requisitos de protección de datos en determinados países, regiones o funciones empresariales.

7 Seguridad de la privacidad

7.1 Los equipos de la privacidad y la protección de datos NTT y de seguridad de la información trabajan juntos para garantizar que se implementen la gestión y el control adecuados de protección de datos para proteger la confidencialidad, integridad y disponibilidad de los datos personales. Nuestras metodologías de seguridad están alineadas con ISO27001 y NIST Cyber Security Framework ("**CSF**").

8 Respuesta y notificación de infracciones

8.1 NTT tiene políticas, procesos y procedimientos para identificar, detectar, responder, recuperar y notificar a los interesados pertinentes en caso de violación de datos personales. Esto incluye mecanismos para realizar un análisis de causa de origen y emprender acciones correctivas.

8.2 NTT se compromete a garantizar que NTT notifique a las autoridades de protección de datos aplicables, a los clientes afectados y a los interesados afectados en caso de violación de los datos personales, de conformidad con las leyes de protección de datos aplicables y los compromisos contractuales.

8.3 NTT mantiene un registro de todas las infracciones de datos personales y de las acciones tomadas para responder a estos eventos.

8.4 Medidas de gestión de incidentes de NTT para identificar, detectar, responder y recuperarse de incidentes de seguridad de la información se describen en la sección B (Seguridad de la información) de estas TOMs.

9 Administración de Terceros

9.1 NTT es responsable de las acciones de sus procesadores (es decir, subencargados) que procesan datos personales en nombre de NTT y evalúan la capacidad de nuestros procesadores para proteger datos personales en el momento de la selección y posteriormente de forma periódica, de acuerdo con las políticas NTT.

9.2 Los subencargados de NTT deben firmar los acuerdos adecuados que regulen el tratamiento y la protección de datos personales y que exijan las mismas obligaciones. según se indica en el acuerdo de tratamiento de datos, que se transferirá a cualquier otro transformador que NTT pueda comprometerse. NTT ha realizado todos los esfuerzos razonables para garantizar que los acuerdos de procesamiento de datos estén en vigor con sus procesadores.

10 Monitorear y evaluar

10.1 NTT informa sobre diseño y eficacia operativa de sus actividades de protección y protección de datos al Comité de Auditoría y Riesgo NTT Ltd y al personal directivo superior periódicamente. Esto incluye el panel informes, autoevaluaciones de la gestión, certificaciones, exámenes de auditoría interna y auditorías y evaluaciones independientes.

(B) Medidas de seguridad

NTT se compromete a garantizar que el control de la seguridad de la información se lleve a cabo y se gestione adecuadamente, a fin de proteger la confidencialidad, integridad y disponibilidad de los datos personales tratados por cuenta de sus clientes y bajo su instrucción.

NTT ha establecido una sistema de gestión de la seguridad de la información para todo el grupo ("**ISMS**") que se ajusta a las prácticas y normas de seguridad de la información más importantes de todo el mundo, incluida la serie ISO27000 y el marco de ciberseguridad del NIST.

11 Seguridad de la Información

11.1 Funciones y responsabilidades para la seguridad de la información se han asignado formalmente líneas jerárquicas que garantizan la independencia de la función, entre ellas un director de seguridad (en lo sucesivo, "**CSO**"), los directores de seguridad de la información (en lo sucesivo, "**CISO**") y los responsables de seguridad de la información (en lo sucesivo, "**ISO**").

11.2 Los empleados de NTT son responsables de garantizar que actúan de conformidad con las políticas, procesos, normas y directrices de seguridad de la información en sus actividades diarias de negocios.

11.3 NTT ha documentado y publicó un conjunto de seguridad de la información políticas que respaldan el los requisitos del SEMA. Políticas y apoyo documentación revisado periódicamente.

11.4 El NTT ha adoptado medidas garantizar que los dispositivos móviles (incluidas las computadoras portátiles, móviles teléfonos, tabletas, dispositivos que permitan el acceso remoto y "Traigan su propio dispositivo") y su contenido están protegidos. NTT se han realizado esfuerzos razonables para garantizar que la administración de dispositivo móviles ("**MDM**") está instalado en todos los dispositivos móviles con acceso a la red de empresa NTT.

11.5 Los teletrabajadores sólo pueden acceder de forma remota a NTT infraestructura a través de uso de Virtual Private Servicios de red ("**VPN**"), siempre que sea posible.

12 Recursos Humanos

12.1 NTT realiza el fondo y el control del empleo para sus empleados, extensión permitida en virtud de la legislación aplicable, para garantizar su idoneidad para la contratación y la sociedad de gestión y información sobre el cliente (incluida datos personales). El alcance de la prueba y el acceso de detección es proporcional a los requisitos comerciales y la información de clasificación a la que tendrá acceso el empleado.

12.2 NTT requiere que sus empleados (incluidos contratistas y temporales empleados) aceptan mantener la confidencialidad de los datos internos y de clientes (incluidos los datos personales).

12.3 Se requieren de NTT empleados completar la información formación en materia de seguridad anualmente. Políticas de seguridad de la información y procedimientos de apoyo, procesos y directrices están disponibles para empleados y empleados reciben información pertinente sobre las tendencias, las amenazas y mejores prácticas a través de plataformas internas de comunicación.

13 Controles de Acceso

13.1 NTT tiene una directiva de uso aceptable compatible con uso adecuado, eficaz y protección de la empresa NTT activos, incluido el equipo y recursos de telecomunicaciones, productos, servicios, soluciones y infraestructura de TI.

13.2 NTT tiene una directiva de clasificación de información que describe el técnico y los controles organizativo de manipulación información basada en su clasificación. Información y los activos están protegidos en línea con la etiqueta de clasificación.

14 Gestión de Activos

14.1 NTT tiene una política de control de acceso, procedimientos de apoyo y lógico y medidas físicas de acceso, para garantizar que sólo las personas autorizadas tendrán acceso a la información basado en el principio de "menos privilegio."

14.2 Los revisiones de acceso son realizado periódicamente en activos de TI, aplicaciones, sistemas y bases de datos garantizar únicamente la autorización las personas tienen acceso.

14.3 Procesadores NTT (es decir, subencargados) deben tener acceso a las sistemas de NTT con cuentas nombrados. Cuentas genéricas y/o intercambio de credenciales está prohibido a menos que la excepción es autorizado explícita por la dirección o clientes.

14.4 Se ha puesto en marcha NTT esfuerzos razonables para limitar estrictamente el número de usuarios privilegiados ("Admin") de sus aplicaciones, sistemas y bases de datos.

15 Física y Seguridad Ambiental

15.1 Se ha puesto en práctica NTT medidas razonables y adecuadas en consonancia con el política de seguridad física para prevenir acceso físico no autorizado, daño o interferencia con los, aplicaciones, sistemas, bases de datos y infraestructura de NTT en todo el dominios siguientes:

15.1.1 Controles de acceso físico;

15.1.2 Supervisión y auditoría de acceso físico;

15.1.3 Protección contra riesgos medioambientales;

15.1.4 Asegurar los activos físicos;

15.1.5 Seguridad del cableado;

15.1.6 Manejo físico y los activos de información;

15.1.7 Mantenimiento y eliminación de activos físicos;

15.1.8 Suprimir escritorio y prácticas de pantalla;

15.1.9 Acceso de los visitantes y supervisión; y

15.1.10 Salud y seguridad procedimientos.

16 Seguridad Operativay

16.1 La función NTT Information and Technology ("**I&T**") es responsable de la gestión de aplicaciones, sistemas, los bases de datos y infraestructura de NTT. I&T documenta, mantiene e implementa todas las políticas y procedimientos operativos de TI que están alineados con los estándares COBIT e ITIL.

16.2 NTT tiene una política y procedimientos de soporte para administrar los cambios en nuestros procesos de negocios, aplicaciones, sistemas, bases de datos e infraestructura. NTT ha establecido varias estructuras de gobernanza para examinar y aprobar cualquier cambio basado en el tamaño y el alcance del cambio y objetivos estratégicos. Todas las solicitudes y sus resultados se registran y documentan.

16.3 NTT ha establecido un programa de gestión de amenazas y vulnerabilidad apoyado por la industria herramientas estándar para identificar, gestionar y mitigar los riesgos para la información de la empresa, incluidos los datos personales de empleados y clientes. Esto incluye la próxima generación Detección de Endpoint y Respuesta ("EDR") para anti-virus y anti-malware herramientas, escaneo regular de entornos, parcheo protocolos y manejo de remediación y actividades de mejora.

16.4 Las necesidades de capacidad se supervisan continuamente y se examinan periódicamente. Los sistemas y las redes se gestionarán y ampliarán de conformidad con esos exámenes.

16.5 La disponibilidad del sistema incluye arquitectura, diseño de alta disponibilidad y/o backups basados en los requerimientos de riesgo y disponibilidad para cada sistema. El método para mantener la disponibilidad o recuperación del sistema, la inclusión del alcance y la frecuencia de los backups se determina en función de los requerimientos del negocio de NTT, incluidos los requerimientos del cliente, y la importancia de la información. Supervisión de copias de seguridad realizadas para garantizar la realización satisfactoria de copias de seguridad, como además de administrar cualquier problema, excepción o error de copia de seguridad.

16.6 NTT realiza esfuerzos razonables para mantener el registro de auditoría en aplicaciones y sistemas Los registros son se examinan periódicamente y se pueden consultar a efectos de investigación. El acceso a los registros está estrictamente limitado únicamente al personal autorizado.

17 Adquisición, Desarrollo y Mantenimiento de Sistemas

17.1 NTT tiene una política de seguridad de arquitectura y diseño, normas y procedimientos de apoyo para garantizar la seguridad los principios de diseño se aplican en el ciclo de vida del desarrollo de software.

17.2 NTT no permite la producción, el cliente, los datos personales o cualquier información confidencial que se utilice para pruebas. En casos excepcionales, los datos de producción o de cliente podrán utilizarse con la aprobación del cliente o del propietario del negocio correspondiente.

18 Administración de Terceros

18.1 NTT tiene una política de seguridad de terceros y procedimientos de soporte para garantizar que los activos de información estén protegidos cuando NTT involucre a terceros proveedores de servicios y/o procesadores. Esto incluye los requisitos de diligencia debida en materia de seguridad de la información y las evaluaciones de riesgos que deben realizarse, a fin de garantizar:

18.1.1 Los requisitos de seguridad de la información se articulan y documentan claramente en los acuerdos con procesadores NTT;

18.1.2 Los procesadores NTT aplican el mismo nivel de protección y control que los de NTT;

18.1.3 Los procesadores deben informar oportunamente a NTT de cualquier incidente de seguridad de la información sospechoso o real.

18.2 NTT ha realizado esfuerzos razonables para garantizar la existencia de acuerdos adecuados con los procesadores que tienen acceso a la información, las aplicaciones, los sistemas de NTT, bases de datos e infraestructura. Estos acuerdos incluyen normas de seguridad de la información NTT para garantizar la confidencialidad, integridad y disponibilidad de información.

19 Administración de Incidentes de Seguridad de la Información

19.1 NTT tiene políticas, procesos y procedimientos para identificar, detectar, responder, recuperar e informar a las partes interesadas pertinentes en caso de incidente de seguridad de la información, incluso personal incumplimientos de datos. Esto incluye mecanismos para realizar un análisis de causa de origen y emprender acciones correctivas.

19.2 NTT ha establecido operaciones de seguridad de todo el grupo para monitorear y administrar de manera proactiva todos los activos informáticos y de red. Esto está respaldado por herramientas técnicas para respuesta y recuperación de incidentes de seguridad de la información.

20 Continuidad del Negocio

20.1 NTT ha establecido planes de continuidad del negocio y recuperación ante desastres. NTT ha adoptado un enfoque por niveles para garantizar la disponibilidad de nuestros sistemas y datos.

21 Conformidad

21.1 NTT ha establecido funciones y responsabilidades para identificar las leyes y reglamentos que afectan a las operaciones comerciales de NTT. Responsabilidad por el cumplimiento de las leyes y reglamentos se establecen a nivel de grupo y regional para garantizar que el NTT cumpla los requisitos globales y locales.

21.2 NTT está impulsando un enfoque consistente de seguridad de la información en todas sus operaciones comerciales. Los productos, servicios y soluciones de NTT están alineados con la norma ISO 27001 y, cuando están certificados según lo establecido en el contrato de cliente, se auditan anualmente de acuerdo con esta norma

Para cualquier pregunta, por favor contacte con la Oficina de Privacidad en **privacyoffice@global.ntt**

Together we do great things