HITACHI
Inspire the Next

ANEXO D
REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN

1. Introducción

Estos Requisitos de Seguridad de la Información (el "ISR") reflejan el acuerdo de las Partes con respecto a los estándares mínimos que el Proveedor empleará durante todo el período del Acuerdo Maestro de Servicios Profesionales, incluyendo cualquier SOW en virtud de este (colectivamente, el "MPSA").

2. Definiciones

A menos que se defina expresamente en este ISR, todos los términos en mayúscula tendrán el mismo significado que en el MPSA. En este ISR, los siguientes términos tienen los siguientes significados:

Datos de Hitachi: cualquier Dato de Hitachi, incluidos, entre otros, los datos compartidos en virtud de MPSA, Servicios, Entregables, facturación y procesos comerciales o relacionados con ellos. Los Datos de Hitachi incluyen datos de Clientes de Hitachi.

Datos de Hitachi Restringidos: Datos de Hitachi clasificados como Restringidos, que requieren un mayor nivel de protección y que incluyen, entre otros, información personal, propiedad intelectual, planes financieros y otra información confidencial.

Entorno de Producción: Sistemas del Proveedor, utilizados para proporcionar Servicios o Entregables a Hitachi.

Sistemas de Hitachi: cualquier red, sistema informático, aplicación, servicio en la nube de Hitachi que brinde acceso a, o almacene, procese o transmita Datos de Hitachi.

Sistemas de Proveedores: redes de proveedores, sistemas informáticos, aplicaciones y/o servicios en la nube que acceden, brindan acceso a, almacenan, procesan o transmiten Dados o Sistemas de Hitachi.

Entorno de Prueba y Desarrollo: los sistemas del Proveedor que se utilizan con el fin de desarrollar y/o probar un Servicio, pero que no se utilizan directamente para entregar Servicios o Entregables a Hitachi o al cliente de Hitachi.

3. Requerimientos Generales

(a) El Proveedor mantendrá salvaguardas organizativas, físicas y técnicas que cumplan o superen las mejores prácticas de la industria, p. Ej. como se establece en ISO/IEC 27001: 2013/27002: 2013 o NIST SP 800-53 y proporcionará a Hitachi una copia de la documentación de su programa y prácticas de seguridad de la información a pedido.

(b) El Proveedor mantendrá un programa de seguridad de la información bajo la supervisión de un Director de Seguridad de la Información (CISO) o un líder senior que sea responsable de un programa de seguridad de la información eficaz y ejerza la supervisión necesaria y adecuada sobre el Personal pertinente para mantener la confidencialidad, integridad y disponibilidad y seguridad adecuadas a los Sistemas del Proveedor.

(c) El Proveedor proporcionará durante la vigencia del MPSA un informe SOC 2 Tipo II o una certificación ISO/IEC 27001: 2013 con la Declaración de aplicabilidad asociada o una atestación o certificación equivalente, de un tercero independiente que cubra su operación en relación con los Servicios o Entregables.

4. Gestión de Terceros

(a) El Proveedor evaluará los riesgos de seguridad de la información asociados con los servicios de terceros que son importantes para la prestación de los Servicios o Entregables e identificará las acciones correctivas para mitigar dichos riesgos. Los servicios de terceros existentes serán monitoreados y evaluados periódicamente para detectar riesgos de seguridad de la información y el Proveedor tomará medidas de mitigación de riesgos.

(b) El Proveedor deberá revelar por adelantado los nombres de los subcontratistas externos que puedan acceder, procesar, almacenar o transmitir Datos de Hitachi.

5. Seguridad del Personal

(a) El Proveedor se asegurará de que todo el Personal con acceso a los Datos y Sistemas de Hitachi se someta a una capacitación formal de concientización sobre seguridad de la información, anualmente.

(b) El Proveedor se asegurará de que todo el personal con acceso a los Datos y Sistemas de Hitachi se haya sometido a una verificación de antecedentes adecuada antes de acceder a los Datos y Sistemas de Hitachi.

6. Control de Acceso

(a) El Proveedor deberá asegurar el acceso a los Datos y Sistemas de Hitachi y los Sistemas de Proveedor mediante múltiples técnicas que se ajusten a los estándares y pautas de la industria de seguridad, como contraseñas seguras o autenticación multifactor (MFA).

(b) El acceso a los Datos de Hitachi se otorga estrictamente en función de las necesidades comerciales.

(c) El Proveedor se asegurará de que todo el Personal que se conecte de forma remota (desde fuera de las instalaciones del Proveedor) para acceder a los Datos y Sistemas de Hitachi o los Sistemas del Proveedor relevantes esté autenticado mediante autenticación multifactor y las conexiones remotas estén encriptadas.

7. Seguridad del Sistema

El Proveedor utilizará medios técnicos y de procedimiento para asegurar continuamente los Sistemas del Proveedor, incluidos, entre otros:

(a) *anti-malware*, protección avanzada contra amenazas;

(b) *firewalls*, pasarelas seguras, seguridad de acceso a la red, sistemas de prevención de intrusiones (IPS), sistemas de detección de intrusos (IDS);

(c) endurecimiento seguro y configuración de los Sistemas del Proveedor;
(d) exploraciones periódicas de vulnerabilidades y reparación de vulnerabilidades proporcionales a la criticidad de las vulnerabilidades;
(e) parcheo de *firmware*, sistema operacional, *middleware*, aplicaciones al último parche disponible;
(f) pruebas de penetración de sistemas de proveedores accesibles desde el exterior al menos una vez al año; y
(g) registro, monitoreo y respuesta a eventos de seguridad de la información y condiciones anormales.

8. Protección de Datos

El Proveedor se asegurará de que los siguientes controles técnicos y de procedimiento estén en vigor para proteger los Datos de Hitachi, a menos que Hitachi apruebe previamente por escrito lo contrario:
(a) Los Datos de Hitachi se almacenan y procesan separados física o lógicamente de los de los otros clientes del Proveedor y separados de los demás entornos del Proveedor.
(b) Los Datos de Hitachi se cifran cuando están en tránsito (transmitidos) utilizando métodos y protocolos de cifrado sólidos y seguros (específicamente TLS 1.2 y superior).
(c) Los Datos de Hitachi Restringidos siempre se cifran cuando se almacenan en reposo, incluso en medios de almacenamiento de respaldo o cuando se almacenan efímeramente durante el tránsito utilizando métodos de cifrados sólidos.
(d) El acceso a los Datos y Sistemas de Hitachi se otorga estrictamente según sea necesario y el acceso se revoca inmediatamente cuando ya no se necesita.
(e) El acceso programático a los Datos y Sistemas de Hitachi está protegido mediante tokens o certificados de autenticación, y los tokens o certificados se rotan de forma regular.
(f) Los Entornos de Producción están separados de los Entornos de Prueba y Desarrollo, y los Datos de Hitachi están separados. Las actividades de prueba y desarrollo no se realizan en Entornos de Producción ni en los Datos de Hitachi almacenados en ningún Entorno de Producción.
(g) Todos los Datos de Hitachi utilizados para pruebas o desarrollo están adecuadamente protegidos, es decir, utilizando solo datos de prueba (no datos de producción) o enmascarando u ofuscando los datos de producción.
(h) El acceso a los Datos de Hitachi se registra y los registros se conservan durante al menos 1 (un) año.
(i) No se almacenan Datos de Hitachi Restringidos en medios extraíbles personales, como discos duros portátiles, unidades USB, DVD, etc.
(j) No se almacenan Datos de Hitachi Restringidos en servicios en la nube de terceros sin la aprobación previa por escrito de Hitachi.
(k) Si el Proveedor almacena Datos de Hitachi, estos estarán respaldados para respaldar el Objetivo de Punto de Recuperación (RPO) y el Objetivo de Tiempo de Recuperación (RTO) de los entregables y servicios como: (1) se especifica en elMPSA; o (2) con un RPO de 24 horas y un RTO de 24 horas, el que sea menor.
(l) Todos los Datos de Hitachi, incluidos los medios que contengan Datos de Hitachi, se devolverán a Hitachi o quedarán totalmente incobrables al finalizar el MPSA o una SOW aplicable.

9. Seguridad de la Aplicación

El Proveedor se asegurará de que las prácticas de seguridad de las aplicaciones y los sistemas estén vigentes para todo el software y los servicios online proporcionados a Hitachi, incluidas, entre otras, las siguientes prácticas:
(a) Garantizar que los desarrolladores estén calificados y capacitados en aplicaciones seguras y técnicas de desarrollo de sistemas.
(b) Aplicar prácticas de codificación seguras (por ejemplo, OWASP Top 10 o CMM SEI CERT Coding Standards).
(c) Aplicar modelos de amenazas a aplicaciones y sistemas.
(d) Aplicar análisis de código fuente estático.
(e) Realizar pruebas de penetración.
(f) Realizar análisis de composición de software de terceros.
(g) Realizar Análisis Autenticadas de Seguridad de Aplicaciones Web Dinámicas.
(h) Informar de inmediato a Hitachi de cualquier vulnerabilidad de seguridad, junto con su calificación CVSS, que se haya encontrado, ya sea por escrito o en una publicación accesible para Hitachi.
(i) Remediar las vulnerabilidades de seguridad encontradas durante las pruebas dentro de los 15 días (Crítico), 30 días (Alto), 60 días (Moderado) y 90 días (todos los demás niveles de gravedad).

10. Seguridad Física

(a) El Proveedor se asegurará de que los Datos de Hitachi solo sean almacenados, procesados y accedidos por Personal autorizado en un entorno seguro.
(b) El Proveedor se asegurará de que todos los medios que contengan Datos de Hitachi sean almacenados y accesibles por personal autorizado en un entorno seguro.
(c) El Proveedor se asegurará de que los Sistemas del Proveedor solo se puedan eliminar o agregar con la autorización de la gerencia del Proveedor.

(d) El Proveedor se asegurará de que su fuerza laboral remota esté capacitada y requerida para aplicar prácticas seguras cuando trabaje de forma remota.

11. Informes de incidentes de seguridad

(a) El Proveedor deberá informar los incidentes de seguridad que afecten los datos de Hitachi o los sistemas de Hitachi dentro de las 24 horas, pero en ningún caso más de 48 horas, por correo electrónico a cybersecurity@hitachivantara.com.

(b) El Proveedor proporcionará un punto de contacto de correo electrónico o teléfono para consultas de seguridad y seguimiento de incidentes por parte de Hitachi antes del comienzo de los Servicios.