TÉRMINOS Y CONDICIONES DE COMPRA ESTÁNDAR

ANEXO A

SEGURIDAD DE LA INFORMACIÓN DE CARRIER

Las siguientes disposiciones de esta política se incorporan a los Términos y Condiciones de Compra de Carrier que pueden encontrarse en https://www.corporate.carrier.com/suppliers/terms-conditions/ (los "Términos") y a cualquier Acuerdo en el que el Vendedor almacene Información de Carrier. Todos los términos en mayúsculas utilizados en esta política, pero no definidos tendrán el significado asignado en los Términos.

1. El Vendedor realizará todos los esfuerzos comercialmente razonables para establecer, mantener y cumplir las salvaguardas administrativas, técnicas y físicas diseñadas para (*a*) proteger la seguridad, disponibilidad e integridad de la red, sistemas y operaciones del Vendedor, los Servicios y la Información de Carrier; (b) evitar Problemas de Seguridad; y (c) satisfacer los requisitos de certificación de la norma ISO 27001. El Vendedor desarrollará, implementará y mantendrá un programa de seguridad por escrito, razonablemente aceptable para el Comprador, que incluya las salvaguardas administrativas, técnicas, organizativas y físicas adecuadas, la concienciación en materia de seguridad y las medidas de seguridad diseñadas para proteger la Información de Carrier frente al acceso y uso no autorizados.

2. El Vendedor se compromete a instalar e implementar hardware, software, procedimientos y políticas de seguridad que proporcionen una seguridad eficaz de la información y que sean aceptables para el Comprador. El Vendedor se compromete a supervisar y actualizar dicho hardware, software, procedimientos y políticas para utilizar la tecnología mejorada y responder a las amenazas de seguridad en desarrollo con el fin de mantener un nivel de protección de la seguridad, preparación y resistencia adecuado para la información en cuestión y el estado actual de las soluciones de seguridad. Previa solicitud, el Vendedor facilitará al Comprador todos los informes o resultados de cualquier auditoría interna relacionada con la seguridad de TI realizada por el Vendedor o en su nombre durante la vigencia del Acuerdo y/u Orden, o cualquier informe de auditoría emitido, incluidos, entre otros, en virtud del informe SSAE 16 o ISAE 3402.

3. Además, el vendedor se compromete a lo siguiente:

    3.1 Sólo recopilará, accederá, utilizará o compartirá la Información de Carrier, o transferirá la Información de Carrier a terceros autorizados, en cumplimiento de sus obligaciones en virtud del Contrato y/u Orden, de conformidad con las disposiciones establecidas en esta política, o para cumplir con las obligaciones legales. El Vendedor no hará ningún uso secundario o de otro tipo (por ejemplo, con fines de extracción de datos) de la Información de Carrier salvo (a) cuando el Comprador lo autorice expresamente por escrito en relación con la compra de Servicios por parte del Comprador en virtud del presente, o (b) cuando lo exija la ley.

    3.2 Mantener y aplicar políticas de seguridad de la información que aborden, como mínimo, los siguientes ámbitos:

        3.2.1 política de seguridad de la información

        3.2.2 organización de la seguridad de la información

        3.2.3 administración de activos

        3.2.4 seguridad de los recursos humanos

        3.2.5 seguridad física y ambiental

        3.2.6 administración de comunicaciones y operaciones

3.2.7 control de acceso

3.2.8 adquisición, desarrollo y mantenimiento de sistemas de información

3.2.9 gestión de incidentes de seguridad de la información

3.2.10 gestión de la continuidad de las actividades

3.2.11 cumplimiento de la normativa

3.3 Proporcionar al Comprador un índice o un resumen similar de sus políticas suficiente para demostrar, a satisfacción razonable del Comprador, que cada ámbito se aborda de forma consistente con esta Sección. El Vendedor proporcionará al Comprador un índice o resumen actualizado, a petición del Comprador, e indicará cualquier plan, incluido un calendario de aplicación, de las actualizaciones previstas para cumplir la política. El Vendedor implementará aquellas solicitudes razonables de modificación de dicha política solicitadas por el Comprador.

3.4 Permitir al Comprador o a la persona que éste designe realizar una auditoría de seguridad en sus instalaciones con un día de antelación, y permitir al Comprador en cualquier momento realizar (o hacer que se realice) una auditoría de la red. Si la Información de Carrier se almacena en un entorno compartido por acuerdo del Comprador, éste recurrirá a un tercero para realizar dichas auditorías. Las auditorías incluirán todas las instalaciones con Información de Carrier, incluidas las instalaciones de almacenamiento de copias de seguridad.

3.5 Separar toda la Información de Carrier en una base de datos independiente a la que sólo puedan acceder el Comprador y sus agentes, así como aquellos empleados y agentes del Vendedor que necesiten acceder para prestar los Servicios o para mantener el equipo y el programa en el que se ejecuta, a menos que el Comprador acuerde lo contrario. La separación lógica de los datos, si así lo aprueba el Comprador, puede ser una alternativa aceptable a este requisito. El Vendedor utilizará todos los esfuerzos razonables, de acuerdo con la tecnología disponible en cada momento, para evitar que cualquier persona que no sean sus empleados autorizados y el Comprador y sus agentes accedan a la Información de Carrier.

3.6 Garantizar que toda la Información de Carrier y el software aplicable cuenten con las copias de seguridad adecuadas y sean recuperables en caso de desastre o emergencia, y que el plan de recuperación de desastres del Vendedor (según se requiera en el presente documento) incorpore dichos requisitos.

3.7 Proporcionar al Comprador, en el momento de la firma de este Acuerdo y/u Orden, un plan de rescisión que aborde cómo se devolverá la Información de Carrier al Comprador al finalizar este Acuerdo y/u Orden, incluida la información de copia de seguridad y archivo, y cómo se eliminará permanentemente toda la Información de Carrier de los equipos e instalaciones del Vendedor. Este plan deberá incluir el suministro de los datos al Comprador en una base de datos no propietaria reconocida por la industria y, en su defecto, una licencia de uso del software de base de datos propietario para acceder a los datos.

3.8 Proporcionar información y cooperar plenamente con el Comprador en respuesta a cualquier citatorio, investigación o similar que requiera Información de Carrier y proporcionar información y asistencia al Comprador para solicitar certificaciones y similares relativas a su información, incluida la información en posesión del Vendedor. El Vendedor notificará inmediatamente al Comprador de la recepción de cualquier solicitud que requiera que la Información de Carrier sea entregada a un tercero.

3.9 Cuando así lo solicite el Comprador, el Vendedor se compromete a cumplir, en un plazo razonable, las políticas de seguridad de la Información de Carrier facilitadas al Vendedor por el Comprador.

3.10 El Vendedor no proporcionará Información de Carrier a ninguna otra entidad sin la aprobación previa por escrito del Comprador. La solicitud de aprobación del Comprador incluirá el acuerdo por parte del Vendedor, y de dicha otra entidad, de que (i) todos los requisitos de esta disposición son aplicables a su desempeño y (ii) el Comprador tendrá derecho a realizar las auditorías descritas anteriormente.

4. Requisitos de encriptación. El Vendedor utilizará, y hará que el Personal del Vendedor utilice, formas adecuadas de cifrado u otras tecnologías seguras en todo momento en relación con el Procesamiento de la Información de Carrier, incluso en relación con cualquier transferencia, comunicación, acceso remoto o almacenamiento (incluido el almacenamiento de respaldo) de la Información de Carrier, según lo autorizado o permitido en virtud del Acuerdo y/u Orden. Sin perjuicio de cualquier disposición en contrario contenida en el presente documento, los Datos Personales del Comprador no se almacenarán en ningún dispositivo informático móvil del Vendedor (por ejemplo, computadoras portátiles, APD (asistentes personales digitales), etc.).

5. Notificación. El Vendedor notificará inmediatamente por escrito al Comprador de (i) cualquier incumplimiento de las normas vigentes en materia de seguridad de la información, y (ii) todos y cada uno de los Problemas de Seguridad razonablemente sospechados y/o confirmados. Dicha notificación resumirá de forma razonablemente detallada el impacto en el Comprador o en cualquier persona afectada por dicho Problema de Seguridad y las medidas correctoras y los esfuerzos de reparación adoptados o propuestos por el Vendedor. Inmediatamente después de cualquier Problema de Seguridad o cualquier otro incumplimiento de las normas de seguridad de la información, ya sea identificado por el Vendedor o por el Comprador, el Vendedor tomará medidas para mitigar los riesgos planteados, consultará de buena fe con el Comprador en relación con los esfuerzos de corrección y emprenderá un plan de corrección que el Comprador determine, a su entera pero razonable discreción, que es necesario, razonable o apropiado dadas las circunstancias proporcionales a la naturaleza del Problema de Seguridad o del incumplimiento, o según lo solicite cualquier organismo gubernamental. El Vendedor será el único responsable de todos los costos y gastos, incluidos, entre otros, los costos razonables de las nuevas pruebas realizadas para verificar que se ha subsanado cualquier Problema de Seguridad. El incumplimiento de la obligación de subsanar los riesgos derivados de un problema o fallo de seguridad en el plazo y de la forma especificados por el Comprador se considerará un incumplimiento sustancial de esta política, de los Términos y/o del Acuerdo.