Seguridad de la información

Término de la seguridad de la información	Definición
Afiliada:	significa una entidad que, sea directa o indirectamente, controla, es controlada por, o se encuentra bajo el control común con, la entidad relevante, donde "control" significa la capacidad de dirigir los asuntos de otro por medio de propiedad, contrato o de otra manera.
Contrato:	significa el contrato conformado por la Orden y sus términos que incorpora este anexo sobre seguridad de la información.
Activo:	significa: (i) cualquier ítem o elemento de hardware, software o equipo que es o puede ser usado para efectos de crear, acceder, procesar, proteger, monitorear, almacenar, recuperar, exhibir o trasmitir datos de cualquier tipo (incluyendo voz); y (ii) cualquier documentación (en cualquier medio) que se relacione con el uso u operación de dichos ítems y elementos.
Comprador:	significa la persona que compra los Servicios bajo el Contrato.
Información del Comprador:	significa información que: (a) el Comprador, o una persona que actúa en su nombre, proporciona al Vendedor, o permite que el Vendedor acceda, en conexión con el Contrato; o (b) el Vendedor crea en conexión con el Contrato.
Grupo del Comprador:	significa el Comprador y todas sus Afiliadas (y "miembro del Grupo del Comprador" será interpretado por consiguiente).
Sistema del Comprador:	significa un Sistema al cual el Comprador (ya sea por sí mismo o por medio de un tercero) proporciona acceso en conexión con el Contrato.
Sujeto de Datos:	significa una persona natural o jurídica identificada o identificable; una persona "identificable" es una que puede ser identificada, directa o indirectamente, en particular por referencia a un número de identificación o a uno o más factores específicos a su identidad física, fisiológica, mental, económica, cultural o social.
Buenas Prácticas de Seguridad y Protección de Datos:	significa medidas y prácticas consistentes con: (a) las medidas y prácticas técnicas y organizacionales que se requieren por, o se recomienda en, normas de gestión y códigos de práctica internacionalmente aceptados relacionados con la Seguridad de la Información (tal como ISO/IEC 27001 (Sistemas de Gestión de Seguridad de la Información – Requisitos) y ISO/IEC 27002 (Código de Práctica para Gestión de Seguridad de la Información)); y (c) Práctica de Protección de la Información CT-007 (b) normas y pautas de seguridad (incluyendo principios generalmente aceptados relacionados con la segregación de los deberes de gobierno, implementación, administración y control) y técnicas tales como fuerte autenticación, control de acceso y auditoría, asignación de "mínimo privilegio", todo según se haga disponible razonablemente al público en general o profesionales de seguridad de la información y personas interesadas por parte de autoridades y organizaciones generalmente reconocidas relacionadas con la Seguridad de la

	Información, según las mismas sean expandidas, variadas y reemplazadas de tiempo en tiempo.
Seguridad de la Información:	significa: (a) la protección y aseguramiento de: (i) la confidencialidad, integridad, confiabilidad y disponibilidad de información y Sistemas; y (ii) propiedades de información relacionadas tales como autenticidad, responsabilidad, y no repudiación; y (b) cumplimiento con todas las regulaciones aplicables al Procesamiento de la información.
Información Personal:	significa cualquier información relacionada con un Sujeto de Datos.
referencias a "**personal**"**:**	dichas referencias incluyen también referencias a los subcontratistas y proveedores de servicio de la parte relevante.
"**Procesar**" (y variaciones de ello, tales como "Procesamiento")**:**	significa realizar cualquier operación o grupo de operaciones sobre los datos personales, sea o no por medios automáticos, tales como cobros, grabaciones, organización, almacenamiento, adaptación o alteración, recuperación, consulta, utilización, divulgación (por transmisión, diseminación o puesto a disposición de otra manera), alineación o combinación, bloqueo, eliminación o destrucción.
Servicios:	significa los servicios que se prestan por el Vendedor bajo el Contrato.
Vendedor:	significa la persona que presta los Servicios al Comprador bajo el Contrato.
Sistema del Vendedor:	significa un sistema al cual el Vendedor (ya sea por sí mismo o por medio de un tercero) proporciona acceso en conexión con el Contrato.
Sistema:	significa un sistema de comunicaciones o tecnología de la información, red, servicio o solución (incluyendo todos los Activos que ya sea (a) forman parte de éste, o (b) se utilizan para proporcionarlo).

El Vendedor deberá:

(a) proporcionar los Servicios y realizar sus obligaciones bajo el Contrato de acuerdo con:

(i) este anexo de seguridad de la información; y

(ii) Buenas Prácticas de Seguridad y Protección de Datos; y

(b) proteger los Servicios y la Información del Comprador, incluyendo por medio de la implementación de las medidas técnicas y organizacionales descritas en la siguiente tabla (las "**Medidas de Seguridad**").

Tipo de Medidas de Seguridad	**Detalles de las Medidas de Seguridad**
Cumplimiento con políticas internas:	1. El Vendedor ha expedido, y deberá implementar y mantener, políticas internas que: (a) requieren que los empleados mantengan la Información del Comprador de manera confidencial y cumplan con las medidas técnicas y organizacionales del Vendedor establecidas para proteger la Información del Comprador; y (b) rijan, como mínimo: (i) el uso de computadoras, dispositivos móviles, correo electrónico e internet; y (ii) cómo proteger la información de la compañía y la Información Personal. 2. El Vendedor deberá: (a) capacitar a sus empleados y terceros relevantes (tales como contratistas) sobre estas políticas y sobre aspectos relacionados de seguridad y TI; y

	(b) requerir que sus empleados, y terceros relevantes, sigan estas políticas. Los empleados y contratistas son específicamente instruidos a no compartir o apuntar las claves.
Construcción de controles de acceso:	El Vendedor controla el acceso a sus edificios donde la Información del Comprador puede ser Procesada, incluyendo con: 1. tarjetas de acceso, monitoreo por video u otras verificaciones (o una combinación de lo anterior); y 2. mecanismos automáticos para monitorear el acceso (e intentos de acceso) y de disparar alarmas en caso de acceso no autorizado o intentos de acceso no autorizado. Adicionalmente, en la medida en que el Vendedor almacene la Información del Comprador de otra manera que directamente en los Sistemas del Comprador, el Vendedor deberá asegurar la implementación de mecanismos automáticos para los lugares donde la Información del Comprador se encuentra almacenada para monitorear el ambiente y disparar alarmas en caso de condiciones inapropiadas para los sistemas de computadores en operación debido a (entre otros) incendio, temperatura, electricidad o humedad.
Controles de acceso para Sistemas utilizados por el Vendedor:	El Vendedor deberá: 1. Procesar Información del Comprador únicamente (a) a través de dispositivos (incluyendo servidores, estaciones de trabajo (tales como computadoras de escritorio y portátiles), y dispositivos móviles (por ejemplo, PDAs, celulares etc.)) controlados efectivamente por el Vendedor; o (b) dentro de aplicaciones controladas por el Vendedor, y, en ambos casos, proteger adecuadamente la Información del Comprador inactiva y en tránsito; y 2. mantener una lista de los lugares de los centros donde su personal Procesa Información del Comprador bajo su control.
Controles de sistema y seguridad de la infraestructura subyacente:	En la medida en que la Información del Comprador sea Procesada en un Sistema del Vendedor, y en la medida en que el Vendedor Procese Información del Comprador en un Sistema del Comprador y pueda ejercer dicho control sobre el Sistema, el Vendedor deberá: 1. restringir el acceso a los Sistemas que contienen Información del Comprador, y declarar la constancia de aquellos que acceden a ella, incluyendo: (a) restringiendo el número de personas con acceso privilegiado; (b) restringiendo acceso por usuarios solo a aquellas partes del Sistema a las cuales necesitan acceso para desempeñar su trabajo; y (c) restringiendo el tiempo durante el cual pueden ejercer acceso; 2. revisar los privilegios de acceso del usuario por o en nombre del Vendedor para acceder los Sistemas del Comprador con la frecuencia requerida por las políticas de seguridad del Comprador y en cualquier caso no menos frecuentemente que una vez por año calendario; 3. asegurar que el personal que tiene acceso al Sistema actúe responsablemente y con debido cuidado; 4. mantener listas de control de acceso a los sistemas de producción y los permisos otorgados a cuentas de

	usuario; 5. inhabilitar o revocar los derechos de acceso de un usuario cuando el usuario ya no necesite dichos derechos de acceso; 6. tener un proceso para asegurar que los derechos de acceso a los Sistemas del Vendedor, y a otros Sistemas (por ejemplo, Sistemas del Comprador) a los cuales el Vendedor (sea por sí mismo o por medio de un tercero) haya otorgado acceso, sean revocados desde el momento en que termine el empleo; 7. cuando el Vendedor requiera acceso a, o copias de, cualquier Información del Comprador para efectos del desarrollo de software o pruebas, proteger la Información del Comprador con las mismas restricciones de acceso de sistema según apliquen para la Información del Comprador en ambientes de producción; 8. mantener especificaciones de recursos técnicos y organizacionales (que cubran autenticación, autorización y contabilidad del sistema informático) requerido para asegurar la confidencialidad, integridad y disponibilidad de la información que es Procesada; 9. asegurar que las versiones maestras de la Información del Comprador se ubican únicamente en servidores de red que satisfacen todas las siguientes condiciones: (i) son controladas efectivamente por el Vendedor; (ii) se encuentran seguras; y (iii) tienen acceso restringido al sistema; y 10. instalar y mantener protección adecuada actualizada en contra de software malicioso. El Vendedor deberá controlar el acceso a Sistemas del Vendedor: 11. manteniendo la seguridad con relación al internet por medio de firewalls y otras medidas que traten los intentos no autorizados de acceder a aplicaciones, sitios o servicios que se encuentran disponibles por internet, o para acceder datos transmitidos por internet; 12. restringiendo el acceso a características del sistema (incluyendo configuraciones del sistema) y otras herramientas relevantes para la seguridad del sistema a personal autorizado; 13. aplicando medidas de protección criptográfica a los datos utilizados para autenticación (por ejemplo, contraseñas hash utilizando algoritmos generalmente seguros y aceptados por la industria); 14. aprovisionamiento y desaprovisionamiento de identificaciones/cuentas de usuarios finales; permitiendo la autenticación y single-sign-on que requieren una identificación/cuenta y contraseña de usuario individual válida; 15. exigiendo una política de contraseña que (a) requiera que cada contraseña comprenda 8 o más caracteres y contenga al menos tres de los siguientes cuatro grupos de caracteres: (i) letras en minúscula (a a la z); (ii) letras en mayúscula (A a la Z); (iii) numerales (0 a 9); y (iv) caracteres especiales (tales como!, $, #, %); y (b) hace que las contraseñas venzan automáticamente dentro de intervalos predefinidos; luego del vencimiento, se debe crear una nueva contraseña;

	16. deshabilitar automáticamente las cuentas de usuario después de 5 intentos de ingreso inválidos; 17. cerrar automáticamente sesiones de ingreso individual inactivas luego de un periodo establecido de hasta 15 minutos; y 18. manejar los derechos, nombres de usuario y contraseñas de los usuarios. El Comprador y el Vendedor podrá, en una base caso por caso, acordar que los párrafos 14 a 16 anteriores no aplicarán para partes de los Sistemas que se pretende sean accesibles públicamente. En la medida en que el Vendedor permita al Comprador mismo administrar los derechos de acceso de los usuarios, el Vendedor deberá: 19. asegurar que el acceso del Comprador a tales Sistemas sea seguro; y 20. proporcionar al Comprador las herramientas para permitirle desempeñar las funciones indicadas en los párrafos 14 a 18 anteriores.
Procedimientos internos de gestión de seguridad:	En la medida en que el Vendedor Procese Información del Comprador diferente a directamente en los Sistemas del Comprador, el Vendedor ha establecido, e implementa, procedimientos internos de gestión de seguridad que cubran los siguientes elementos: 1. solicitar y aprobar derechos de procesamiento de información en los Sistemas del Vendedor; otorgando tales derechos en los Sistemas; y quién es responsable por solicitar, aprobar, otorgar y revisar tales derechos; 2. métodos y recursos para autenticar usuarios de Sistema, y procedimientos relacionados con administrar y utilizar dichos métodos y recursos; 3. cómo crear y usar copias de datos, programas y herramientas de programa del Sistema utilizados para respaldar y restaurar los Sistemas, así como cómo crear y mantener los datos del Sistema requeridos para las pruebas y migración del Sistema; 4. la protección adecuada de cualquier copia requerida para efectos de respaldo y archivo del Sistema y otros; 5. cómo asegurar los Sistemas en contra de acceso no autorizado; 6. cómo los Sistemas registran quién ha accedido a dichos Sistemas, indicando la fecha y alcance de dicho acceso; 7. cómo realizar revisiones y mantenimiento de medios y Sistemas utilizados para el Procesamiento de datos; 8. cómo disponer de manera segura de información que ya no tiene que ser retenida; y 9. procedimientos para detectar y prevenir incidentes de seguridad, incluyendo: (i) gestión de activos; (ii) evaluación de impacto; y (iii) remediación y escalamiento oportuno a todas las partes adecuadas.
Procesamiento de Información del Comprador:	En la medida en que el Vendedor Procese Información del Comprador diferente a directamente en los Sistemas del Comprador, el Vendedor deberá mantener y exigir procedimientos relacionados con la transmisión y protección de información e Información del Comprador, incluyendo: 1. manteniendo pautas para la retención y

	disposición de la correspondencia comercial y otros registros; 2. manteniendo políticas que regulen la descarga, uso y retención de software y datos de terceros; 3. asegurando la seguridad de la información de la Información del Comprador que es transmitida electrónicamente (directamente o vía instalaciones de montaje) entre Sistemas (sea en las instalaciones del Vendedor o de otras partes); 4. administrando medios removibles y móviles de acuerdo con las Mejores Prácticas de Seguridad, incluyendo según aplique: (a) almacenándolos en un ambiente seguro de acuerdo con las especificaciones de los fabricantes; (b) asegurando su transporte, eliminación y disposición segura; y (c) almacenando medios de respaldo en una ubicación remota, a una distancia suficiente para escapar cualquier daño por un desastre en el sitio principal; 5. protegiendo la Información del Comprador en tránsito e inactiva utilizando las Mejores Prácticas de Seguridad tales como cifrado y controles de acceso; 6. restringiendo el acceso a Información del Comprador a aquel personal que requiera acceso para efectos de prestar los Servicios, y asegurar que dicho personal Procese dicha Información del Comprador únicamente en la medida necesaria para efectos de prestar los Servicios; 7. devolver toda la Información del Comprador al Comprador cuando el Vendedor ya no requiere acceso a, o uso de, dicha Información del Comprador para efectos de prestar los Servicios; y 8. una vez el Comprador haya confirmado al Vendedor por escrito que cualquier Información del Comprador devuelta a éste en virtud del párrafo 7 anterior ha sido recibido exitosamente, eliminar toda dicha Información del Comprador.
Gestión de Activos:	Si el Vendedor debe sacar fuera de servicio o eliminar cualquier Activo que contenga Información del Comprador, el Vendedor deberá asegurar: 1. que el Activo sea destruido irremediablemente o devuelto al Comprador; o 2. que la Información del Comprador o información relevante tenida en el Activo sea eliminada e irrecuperable antes de sacar fuera de servicio o eliminar el Activo.
Transmisiones:	1. El Vendedor no deberá transmitir, o solicitar a ningún usuario que transmita, contraseñas en texto claro por los Sistemas o entre Sistemas. 2. El Vendedor no deberá transmitir, o permitir la transmisión por ningún miembro de su personal de, cualquier información no estructurada a/del Comprador o cualquiera de sus Afiliadas utilizando cualquier medio diferente a por medio de Sistemas corporativos del Vendedor. Como parte de lo anterior, para efectos de alojar o transmitir datos no estructurados como parte de los Servicios, o para efectos de alojar o transmitir Información del Comprador, el Vendedor no deberá usar, y no permitirá, el uso para este propósito de: (a) cuentas de correo electrónico no corporativas (por ejemplo, Yahoo!, Gmail, etc.); (b) FTP no asegurado; o

	(c) servicios para compartir archivos para consumidores. 3. El Vendedor no enviará ningún CD/DVD/ medio de disco que contenga Información del Comprador a ningún receptor (incluyendo al Comprador o cualquiera de sus Afiliadas) vía cualquier servicio de correo o Courier salvo con el previo acuerdo por escrito del contacto de seguridad designado del Comprador. Cuando el Vendedor solicite y obtenga tal acuerdo por escrito, dicha aprobación será válida únicamente para esa transmisión individual.
Revisión, informes, notificación:	1. El Vendedor tomará medidas adecuadas para revisar que: (a) cumple con este Anexo; y (b) las medidas que toma en cumplimiento con este Anexo son efectivas para lograr Buenas Prácticas de Seguridad y Protección de Datos. 2. En la medida en que las actividades del Vendedor en conexión con el Contrato involucren una solución móvil o basada en la web: (a) el Vendedor deberá realizar evaluaciones de seguridad (incluyendo pruebas de desempeño) de dicha solución móvil o basada en la web no menos frecuentemente que anualmente y discutir los resultados con el Comprador a solicitud; y (b) el Comprador puede realizar sus propias evaluaciones de seguridad de dicha solución móvil o basada en la web en coordinación con el Vendedor. 3. El Vendedor proporcionará al Comprador, o menos frecuentemente que cada trimestre (o tal otro periodo como el Comprador pueda acordar), con visiones generales integrales y fácilmente comprensibles relacionadas con: (a) los permisos de acceso de todas las personas con acceso a la Información del Comprador; y (b) rastros de auditoría de todas las personas con acceso a la Información del Comprador. 4. El Vendedor deberá, dentro de un periodo razonable, notificar al Comprador si el Vendedor enfrenta un evento de seguridad que afecte negativamente la confidencialidad o integridad de la Información del Comprador.
Continuidad del Servicio:	El Vendedor deberá: 1. detectar, rastrear, escalar y resolver cualquier incidente, falla, evento de seguridad u otro riesgo operacional real (o potencial) de manera oportuna; 2. probar, aprobar y desplegar cambios al Sistema del Vendedor de manera controlada solo con mínima interrupción para el Comprador; 3. planear, implementar y probar regularmente las medidas organizacionales y técnicas adecuadas necesarias para mantener o recuperar rápidamente los servicios que se prestan al Comprador en caso de cualquier evento disruptivo previsto; y 4. asegurar que cualquier ubicación stand-by o alternativa utilizada para efectos de la continuidad de los servicios del Vendedor se encuentre sujeta a controles de seguridad de la información al menos equivalentes a aquellos vigentes en las instalaciones de donde el Vendedor usualmente opera los procesos reubicados.