REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN (ISR) DE TERCEROS

Propósito. Este ISR establece los requisitos de seguridad de información de Chubb con respecto a los Datos de Chubb y formará parte del acuerdo maestro de Chubb ("Acuerdo") aplicable que regirá los servicios ("Servicios") que proporcionará usted ("Proveedor") de conformidad con dicho Acuerdo. Durante el cumplimiento de los Servicios, el Proveedor deberá cumplir con todas las disposiciones de este ISR y hará que cumplan con todas estas todos los Subproveedores a quienes el Proveedor pueda proporcionar acceso a los datos, revelar datos de Chubb o autorizar a recopilar dichos datos en su nombre, tal como se permite en el Acuerdo. El Proveedor y Chubb se denominarán en adelante colectivamente "las Partes" o, individualmente, "Parte".

1. Definiciones

1.1 "Datos de Chubb" significa (a) datos o información propiedad de Chubb o provista por cualquier tercero (incluido el Proveedor), sus afiliados o cualquiera de sus proveedores o clientes, a los que el Proveedor obtiene acceso (ya sea con anterioridad o posterioridad a la fecha de entrada en vigencia del Acuerdo) en conexión con la negociación o la ejecución del Acuerdo, o con el cumplimiento de las obligaciones del Proveedor bajo el Acuerdo, incluida la Información de identificación personal, así como todos los datos e información: (i) relacionados con empresas, clientes, asegurados, reclamantes, socios comerciales, personal, operaciones, instalaciones, productos, tarifas, cumplimiento normativo, competidores, mercados de consumo, activos, gastos, fusiones, adquisiciones, desinversiones, facturaciones, recaudaciones y finanzas de Chubb y sus afiliados, los clientes y proveedores de ambos; o (ii) creados, generados, recopilados o procesados por el Proveedor durante el cumplimiento de sus obligaciones bajo el Acuerdo, incluido el procesamiento de datos de entrada y salida, mediciones de nivel de servicio, información de activos, informes, acuerdos de servicio y de productos con terceros; y (b) todos los derivados de cualquiera de los anteriores.

1.2 "Incumplimiento" significa (i) uso, pérdida o divulgación no autorizados, o acceso no autorizado a los Datos de Chubb y los sistemas que los contienen y/o (ii) incumplimiento de los Servicios de acuerdo con las Mejores prácticas de seguridad de la información.

1.3 "**Mejores prácticas de seguridad de la información**" significa (i) las mejores prácticas de privacidad y seguridad de la información coherentes con marcos de seguridad de la información reconocidos (como ISO 27001, NIST Cybersecurity Framework), (ii) los requisitos de seguridad, las normas, las obligaciones, las especificaciones y los procedimientos de informes de sucesos establecidos en este ISR o en el Acuerdo (ya que se pueden modificar de vez en cuando); y (iii) cualquier otro requisito, norma, obligación, especificación o procedimiento de informe de eventos requerido por cualquier Ley.

1.4 "Leyes" significa toda ley, estatuto, decreto, norma y reglamento internacional, federal, estatal, provincial, regional, territorial y local aplicable, todo decreto, requisito de supervisión, directriz, circular, opinión y carta interpretativa ejecutivos y todo otro comunicado de cualquier Gobierno o autoridad, departamento o agencia de este, incluidas las Leyes de privacidad.

1.5 "Información de identificación personal (PII)" se refiere a cualquier Dato de Chubb que contenga un identificador único o más, a partir de los que se pueda determinar la identidad de la persona o acceder a ella, como el nombre completo, el número de identificación nacional, el número de seguro social, el número de pasaporte, la licencia para conducir o cualquier otro número de identificación emitido por el Gobierno, la tarjeta de crédito, la tarjeta de débito o información de la cuenta financiera, la fecha de nacimiento, el nombre de soltera de la madre, la información médica o del seguro de salud, los registros biométricos, los archivos de firma digital, la información de inicio de sesión de la cuenta (por ejemplo, una combinación de identificación de usuario o dirección de correo electrónico con una contraseña u otra información que brinde acceso a una cuenta) y cualquier otra información protegida por las Leyes de privacidad.

1.6 "Leyes de privacidad" significa toda ley, reglamento o norma internacional, federal, estatal, provincial o local aplicable relacionada con la privacidad de datos, seguridad de la información, información personal de identificación, robo de identidad, notificación de violación de datos, flujo transfronterizo de datos o protección de datos.

1.7 "Subproveedor" significa, de forma colectiva e individual, cualquier tercero, incluidos, entre otros, cualquier subcontratista, proveedor de servicios *offshore*, agente, subcontratista o similar, que procesa o almacena los Datos de Chubb, que tiene acceso a estos, o que recopila datos en nombre de Chubb (sujeto a la aprobación escrita previa de Chubb).

2. Protección de datos

2.1 Restricción de datos. El Proveedor se compromete y concuerda con lo siguiente: (a) no venderá, cederá, licitará ni comercializará Datos de Chubb a terceros sin el previo consentimiento por escrito de Chubb; y (b) no hará uso de los Datos de Chubb para sus propios fines o en beneficio de cualquier persona o cualquier otra entidad que no sea Chubb, y dichos datos solo serán utilizados y divulgados para cumplir con las obligaciones del Proveedor con respecto a los Servicios.

2.2 Remediación. Si los controles de seguridad física y de datos del Proveedor no son adecuados para proteger los Datos de Chubb, las partes discutirán un plan de remediación, si corresponde, o, en caso de que la remediación no sea factible, Chubb puede rescindir cualquiera o todos los Servicios y los acuerdos aplicables con cinco (5) días hábiles de aviso por escrito al Proveedor sin responsabilidad por dicha rescisión.

3. Corrección y reconstrucción. El Proveedor desarrollará y mantendrá procedimientos para la reconstrucción de los Datos perdidos de Chubb y, sin costo para Chubb, deberá corregir cualquier error, destrucción, pérdida o alteración de cualquier Dato de Chubb causado por el Proveedor o el Subproveedor.

4. Procesamiento de datos

4.1 Cada Parte deberá cumplir con todas las Leyes de privacidad en relación con el cumplimiento de sus obligaciones y el ejercicio de sus derechos bajo este Acuerdo. El Proveedor cooperará según lo

solicite Chubb en relación con cualquier presentación, divulgación o registro requerido por las autoridades de protección de datos en relación con la provisión o recepción de los Servicios.

4.2 Si el Proveedor o Subproveedor procesa PII en nombre de Chubb en conexión con este Acuerdo, el Proveedor deberá asegurar lo siguiente, o asegurar que el Subproveedor lo realice: (i) procesar dicha PII solo de acuerdo con las instrucciones de Chubb y, en particular, no procesar dicha PII excepto para proporcionar los Servicios; (ii) disponer en todo momento de salvaguardias administrativas, técnicas y físicas adecuadas para proteger las PII contra la destrucción accidental o ilícita, la pérdida accidental, la alteración, la divulgación no autorizada o el acceso a las PII (en particular cuando el procesamiento implica la transmisión de datos a través de una red, entre otros) y todas las demás formas ilegales y no autorizadas de procesamiento; (iii) tratar la PII como confidencial, no revelar dicha PII a ninguna persona, excepto con el previo consentimiento por escrito de Chubb, y limitar el acceso a dicha PII a los empleados del Proveedor o Subproveedor que necesiten acceso para proporcionar los Servicios; (iv) informar sin demora a Chubb acerca de cualquier acceso no autorizado o procesamiento ilegal de PII de los que tenga conocimiento; (v) cuando los Datos de Chubb ya no sean necesarios para la provisión de los Servicios ni se requiera retenerlos, borrar de forma inmediata y segura los Datos de Chubb de manera que la información sea irrecuperable y enviarle a Chubb una certificación que constate que se ha efectuado la eliminación o, a criterio de Chubb, devolver los Datos de Chubb a Chubb; y (vi) no comprometer a Chubb con la violación de cualquier Ley de privacidad por cualquier acto u omisión.

4.3 En la medida en que el Proveedor procese o almacene cualquier información de tarjeta de pago de conformidad con los Servicios, el Proveedor deberá cumplir con (i) cualquier estándar emitido por el Consejo de normas de seguridad de la Industria de tarjetas de pago (PCI), incluida la Norma de seguridad de datos de la Industria de tarjetas de pago y la Norma de seguridad de datos de Aplicaciones de pago; (ii) cualquier ley o reglamento operativo de las tarjetas VISA, MasterCard y cualquier otra red de tarjetas de crédito; y (iii) cualquier Ley aplicable a los datos del titular de la tarjeta, ya que (i) - (iii) pueden ser modificados o revisados cada cierto tiempo.

5. Procedimientos de salvaguardia de datos

5.1 Durante el plazo del Acuerdo y siempre que los Datos de Chubb estén en posesión o bajo el control del Proveedor, el Proveedor establecerá y mantendrá un programa integral de seguridad de datos por escrito que incluya políticas administrativas, técnicas y físicas, procedimientos y salvaguardias para la protección de Datos de Chubb. El programa de seguridad de datos del Proveedor debe estar diseñado específicamente para lo siguiente: (1) garantizar la seguridad, integridad, disponibilidad y confidencialidad de los Datos de Chubb; (2) proteger la seguridad o integridad de los Datos de Chubb contra cualquier amenaza o peligro previsto; y (3) proteger contra la destrucción, la pérdida, el acceso no autorizado o la alteración de los Datos de Chubb. Las políticas y los procedimientos del Proveedor tendrán las siguientes características: (i) no serán menos rigurosos que aquellos mantenidos por el Proveedor para su propia información de naturaleza similar; (ii) no serán menos rigurosos que las mejores prácticas de la industria para ubicaciones similares a la ubicación de servicio aplicable en este Acuerdo; (iii) serán adecuadas para cumplir con los requisitos de las Leyes. Chubb tendrá derecho a auditar el programa de seguridad de datos del Proveedor y los controles, incluso a través de inspecciones en el sitio, con un aviso anticipado razonable por escrito al Proveedor (sin costo adicional para Chubb). Además, el Proveedor cooperará con Chubb para

realizar evaluaciones del control de seguridad a través de cuestionarios, correos electrónicos, llamadas telefónicas o reuniones en línea (incluido el acceso a las políticas, los procedimientos y otra documentación relevante del Proveedor y el acceso al personal del Proveedor, según sea razonablemente necesario para facilitar tales evaluaciones). Durante dicha evaluación, el Proveedor deberá proporcionarle a Chubb copias de cualquier informe de auditoría independiente (correspondientes a los productos o servicios que se brindan a Chubb de conformidad con este Acuerdo) que se hayan preparado para el Proveedor, como un informe SOC 2 Tipo II o una certificación ISO 27001:2013. Si Chubb, a su discreción razonable, descubre algún problema o deficiencia con los controles de seguridad del Proveedor, el Proveedor deberá presentarle un plan de remediación a Chubb dentro de los treinta (30) días siguientes a la finalización de dicha evaluación y el Proveedor deberá remediar cada uno de esos problemas de manera oportuna, de acuerdo con un programa de remediación acordado mutuamente por las partes.

5.2 Si los servicios proporcionados por el Proveedor requieren acceso a los sistemas de Chubb, no se copiará ni extraerá ningún dato de dichos sistemas sin el consentimiento previo por escrito del gerente de Seguridad de la información de Chubb. Como parte de los Servicios, el Proveedor llevará a cabo evaluaciones de vulnerabilidad y amenazas, por sí mismo y mediante un tercero independiente, al menos una vez al año, para identificar amenazas o vulnerabilidades que puedan comprometer la seguridad, confidencialidad, disponibilidad o integridad de los Datos de Chubb, y monitoreará, probará y actualizará su programa de seguridad de datos para asegurar su efectividad y cumplimiento con este Acuerdo. El Proveedor documentará y mantendrá un plan de respuesta ante incidentes de seguridad que contemple amenazas a la confidencialidad, la integridad y la disponibilidad de los Datos de Chubb, y se involucrará en ejercicios periódicos de preparación para incidentes. Si el Proveedor descubriera cualquier acceso accidental o intencional, le informaran de dicho acceso o sospechara acerca de una violación de la seguridad de los Datos de Chubb o de cualquier uso o divulgación ilegal o no autorizada de los Datos de Chubb, deberá realizar lo siguiente: (a) notificar de inmediato al gerente de Seguridad de información de Chubb al correo electrónico tpsecuritynotice@chubb.com, en ningún caso pasadas veinticuatro (24) horas desde el descubrimiento del acceso o la sospecha de violación de la seguridad de los Datos de Chubb; (b) asegurar inmediatamente los sistemas afectados para prevenir más ingresos; (c) investigar y remediar los efectos de tal acceso o sospecha de acceso a los Datos de Chubb, realizar un análisis de la causa principal y proporcionar un resumen ejecutivo de dicho análisis a Chubb bajo petición.

5.3 El Proveedor reconoce que las Leyes de privacidad incluyen ciertos estatutos o regulaciones de notificación de violación de seguridad que obligan a los propietarios y licenciatarios de PII a notificar el acceso o el uso no autorizado de dicha información (las "Leyes de violación de seguridad"). Si el Proveedor tiene conocimiento de cualquier circunstancia que pueda desencadenar las obligaciones de cualquiera de las Partes bajo las Leyes de violación de seguridad, deberá notificarlo por escrito a Chubb y deberá cooperar plenamente con Chubb para permitir que Chubb cumpla con sus obligaciones bajo las Leyes de violación de Seguridad. Chubb tendrá el derecho exclusivo de emitir los avisos requeridos bajo cualquier Ley de violación de seguridad. Si el Proveedor está obligado por cualquier Ley de violación de seguridad a dar cualquier aviso a cualquier persona que no sea Chubb, el Proveedor cooperará con Chubb en el desarrollo y la entrega de dicha notificación, y Chubb tendrá el derecho final de aprobación sobre el contenido de dicha notificación (sujeto a la ley aplicable). El Proveedor asumirá todos los costos relacionados con cualquier violación que involucre los Datos de Chubb, excepto que tal violación sea causada directamente por las acciones de Chubb en incumplimiento de las obligaciones expresas de Chubb bajo este ISR. Cada Parte

proporcionará toda asistencia, cooperación y apoyo que la otra Parte pueda razonablemente solicitar en la investigación de cualquier incidente de seguridad, acceso, intento de fraude u otro desastre.

6. Prácticas de seguridad. El Proveedor proporcionará todos los Servicios de acuerdo con las Mejores prácticas de seguridad de la información. Sin tener en cuenta ninguna disposición establecida que sea contraria a este documento, el Proveedor acuerda por este medio implementar y mantener, como mínimo, los siguientes controles de seguridad:

6.1 Controles de red

(a) Mantener un firewall en cada conexión a Internet, entre cualquier DMZ y la red interna, las conexiones a las redes públicas deben usar la Traducción de direcciones de red (o equivalente) y asegurarse de que las reglas de alto riesgo se revisen anualmente.
(b) Separar lógica o físicamente, en la medida de lo técnicamente factible, todos los Datos de Chubb respecto de aquellos de cualquier otro cliente del Proveedor y restringir el acceso en cualquier entorno compartido a los empleados del Proveedor o Subproveedor que realice los servicios.
(c) Separar lógica o físicamente los entornos de producción de los entornos que no son de producción (por ejemplo, desarrollo, prueba, control de calidad), se debe implementar el filtrado de contenido web, bloquear sitios de Internet inapropiados y mantener/revisar anualmente.
(d) Solo permitir que los dispositivos autorizados se conecten a la red interna.

6.2 Parámetros predeterminados

(a) Cambiar las contraseñas y las configuraciones predeterminadas, si corresponde, en los dispositivos suministrados por el proveedor antes de conectarlos a la red.
(b) Habilitar solo los puertos, servicios y protocolos necesarios y seguros, según sea necesario para el funcionamiento de un sistema en particular.
(c) Actualizar y mantener las configuraciones del sistema de manera coherente con las prácticas de la industria y los estándares de fortalecimiento del sistema del Proveedor.

6.3 Datos almacenados

(a) Mantener y seguir procesos para la eliminación o la destrucción seguras de medios electrónicos e impresos cuando ya no sean necesarios.
(b) Crear un *hash* y/o cifrar contraseñas donde sea que se almacenen mediante un sistema de criptografía o un sistema de bóveda de contraseñas de acuerdo con las Mejores prácticas de seguridad de la información.
(c) Prohibir el almacenamiento de PII en entornos que no sean de producción, a menos que se haya implementado un cifrado anónimo o de capa de aplicación.

6.4 Cifrado

(a) Se prohíbe el uso de criptografía obsoleta.
(b) Los datos y las contraseñas de Chubb se cifrarán en tránsito y en reposo, incluido el almacenamiento en medios extraíbles (como cintas de respaldo, computadoras portátiles, unidades USB).
(c) Asegurarse de que las redes inalámbricas corporativas se implementen con protocolos estándar de la industria utilizando algoritmos de cifrado sólidos para la autenticación y la transmisión.

6.5 Gestión de vulnerabilidades

(a) Instalar y mantener software antivirus/malware en los sistemas informáticos de acuerdo con las Mejores prácticas de seguridad de la información.
(b) Asegurar que todos los mecanismos antivirus/malware (por ejemplo, las firmas de virus) estén actualizados, se estén ejecutando activamente y mantengan los registros de auditoría durante al menos 90 días.
(c) Un programa de gestión de vulnerabilidades debe documentarse y gestionarse de acuerdo con las Mejores prácticas de seguridad de la información y garantizar la corrección oportuna de las vulnerabilidades priorizadas. El programa de gestión de vulnerabilidades debe incluir lo siguiente:
    (1) Desarrollar aplicaciones basadas en pautas de codificación segura, según OWASP.
    (2) Realizar un análisis de código estático y resolver para evitar vulnerabilidades de codificación comunes, según OWASP y Enumeración de debilidades comunes (por ejemplo, según la lista de OWASP) en el desarrollo de software.
    (3) Realizar escaneos de vulnerabilidades en todos los dispositivos conectados a la red interna.
    (4) Realizar análisis de vulnerabilidades de aplicaciones a través de herramientas o métodos de evaluación de seguridad manuales y/o automatizados, al menos una vez al año y antes del lanzamiento de nuevas versiones o después de cualquier cambio significativo.
    (5) Remediar o mitigar todas las vulnerabilidades críticas o de alto riesgo confirmadas dentro de los treinta (30) días posteriores al descubrimiento.

6.6 Control de acceso

(a) Restringir las cuentas de usuario mantenidas por el Proveedor para acceder solo a la información mínima necesaria para realizar las responsabilidades laborales.
(b) Requerir autenticación multifactor según las Mejores prácticas de seguridad de la información para el acceso remoto a las redes internas del Proveedor desde redes externas y para el acceso a la aplicación del proveedor.
(c) Evaluar el acceso de los usuarios a los sistemas del Proveedor al menos semestralmente para corroborar su acceso y uso apropiados, y revocar de inmediato el acceso a los usuarios que ya no formen parte del equipo.
(d) Los servicios que requieren que el personal de Chubb acceda a la red o la aplicación del Proveedor (o viceversa) requieren el uso de federación si no se utiliza VDI o Escritorio como servicio (DaaS).
(e) Notificar de inmediato a Chubb acerca de cualquier usuario del Proveedor con acceso a los sistemas de Chubb que (i) ya no forme parte del equipo o (ii) ya no cuente con un justificativo empresarial para acceder a los sistemas de Chubb, o (iii) una cuenta esté comprometida.
(f) Prácticas de contraseña: (i) no use cuentas y contraseñas grupales, compartidas o genéricas, (ii) gestione las contraseñas de acuerdo con las Mejores prácticas de seguridad de la información o una longitud mínima de 8 caracteres con una combinación de al menos 3 de las 4 categorías: caracteres en mayúsculas, caracteres en minúsculas, caracteres especiales y números, (iii) las contraseñas de las cuentas de usuario deben caducar cada 90 días y no deben repetir ninguna de las últimas doce

(12) contraseñas para el ID de usuario asociado, y (iv) contraseñas no seguras conocidas (por ejemplo, Pas$word1).

(g) Bloquee las ID de usuario durante un período de espera mínimo de 30 minutos después de no más de 6 intentos fallidos o pida que un administrador desbloquee las ID bloqueadas.

6.7 Supervisión

(a) Implementar el registro de eventos para los componentes del sistema necesarios para reconstruir eventos y así detectar o responder a problemas de seguridad.

(b) Configurar la hora del sistema de manera que sea precisa, coherente entre los sistemas y basada en fuentes de tiempo aceptadas por la industria.

(c) Debe existir un proceso de respuesta a incidentes de seguridad que sea proporcional a los riesgos asociados con la violación de datos, la corrupción de datos o la interrupción del negocio. Esto debe incluir una solución de Incidente de seguridad y gestión de eventos (SIEM) o un servicio administrado de terceros que correlacione los registros entre los sistemas, detecte actividades anómalas, garantice una respuesta adecuada y tenga un proceso establecido para ajustar las reglas para identificar nuevas amenazas de seguridad cibernética.

(d) Asegurar los registros de auditoría para que no puedan ser alterados ni modificados, y retener los datos transmitidos durante un año

(e) Utilizar sistemas de detección de intrusos o sistemas de prevención de intrusos para supervisar todo el tráfico en el perímetro de la red.

6.8 Controles físicos y ambientales

(a) Implementar y mantener controles de acceso físico, incluidos controles que restrinjan el acceso a las instalaciones al personal autorizado, que limiten el acceso a áreas confidenciales (por ejemplo, centro de datos) basado en las responsabilidades laborales, y requerir protocolos apropiados de escolta de visitantes.

(b) Utilizar cámaras de CCTV o de vigilancia en todos los puntos de entrada y salida de las instalaciones que almacenan y procesan datos de Chubb y que tienen acceso a estos. También se deben utilizar cámaras dentro y fuera de las salas de datos donde se almacenan los servidores que contienen datos de Chubb. Los registros de video de CCTV deben conservarse durante 90 días.

(c) Implementar y mantener controles ambientales, incluida la detección y supresión de incendios adecuadas, fuente de alimentación redundante, respaldo de batería, detección de agua, HVAC, sistemas de control de humedad cuando corresponda.

(d) Implementar y mantener programas de eliminación de residuos que incluyan la eliminación segura de residuos confidenciales. Los residuos confidenciales se definen como documentos, dispositivos de almacenamiento electrónico y cualquier material descartado que contenga o pueda divulgar Datos de Chubb.

7. **Trabajo remoto.** En la medida en que un empleado del Proveedor o Subproveedor esté trabajando de forma remota, es decir, trabajando en un lugar que no sea el lugar de trabajo de su empleador (incluido el trabajo desde casa) ("Trabajo remoto"), el Proveedor se asegurará de que cada empleado cumpla con los siguientes requisitos:

7.1 Requisitos técnicos. Todo el equipo utilizado en un acuerdo de Trabajo remoto debe ser emitido y gestionado por el Proveedor y cumplir con las siguientes especificaciones técnicas mínimas:

(a) Un sistema antivirus monitoreado y gestionado por el Proveedor y actualizado de acuerdo con las Mejores prácticas de seguridad de la información.
(b) Un disco duro cifrado.
(c) No se permiten derechos de administrador local.
(d) No se deben utilizar medios extraíbles (como unidades USB).
(e) El software y la configuración de los sistemas deben ser actuales y estar actualizados.
(f) Toda la conectividad a Chubb debe realizarse mediante las capacidades de la Interfaz de escritorio virtual (VDI) de Chubb y requiere autenticación multifactor ("MFA"). Cualquier alternativa a esta conectividad debe enviarse a Chubb por escrito con anticipación para su aprobación a exclusivo criterio de Chubb.

7.2 Dispositivo personal. Si no tiene a su disposición un dispositivo proporcionado y gestionado por el Proveedor, se puede usar un dispositivo personal ("BYOD"), pero primero debe conectarse a la red del Proveedor a través de VPN mediante MFA, y, solo luego, conectarse al VDI de Chubb. Si se utiliza un dispositivo BYOD, aún le corresponde al Proveedor garantizar que los datos y los entornos de Chubb estén protegidos. Bajo ninguna circunstancia los dispositivos BYOD pueden conectarse directamente al VDI de Chubb.

7.3 Procedimientos de trabajo remoto. El Proveedor certifica que los siguientes requisitos de Trabajo remoto han sido o serán comunicados a los empleados del Proveedor antes de que participen en el Trabajo remoto:

(a) Usar filtros de privacidad sobre las pantallas (cuando estén disponibles).
(b) Almacenar los dispositivos cuando no estén en uso en un lugar seguro (preferiblemente bajo llave).
(c) Evitar colocar los monitores donde puedan ser vistos por personas no autorizadas.
(d) No compartir contraseñas ni escribir contraseñas en papel.
(e) La información sensible no debe ser fotografiada o tomada en forma escrita.
(f) No modificar ni intentar modificar ninguna configuración de seguridad en un dispositivo BYOD

8. General

8.1 Administración de la seguridad. El Proveedor proveerá (o hará proveer) entrenamiento de concientización de seguridad a todos los empleados y Subproveedores que usen o tengan acceso a los Datos de Chubb. La capacitación debe estar diseñada para educarlos en el mantenimiento de la confidencialidad, la integridad y la disponibilidad de información personal y corporativa confidencial, y debe dictarse al momento de la contratación no menos de una vez al año. El administrador de Seguridad del Proveedor debe mantener la responsabilidad exclusiva de proporcionar el acceso a los sistemas que contienen Datos de Chubb, o el uso de estos sistemas, a todos los empleados del Proveedor y Subproveedor, y de proporcionar un proceso mediante el que se creen y eliminen las cuentas administrativas específicas del Proveedor de manera segura y oportuna. El Proveedor aplicará los principios de acceso a la Seguridad: segregación de deberes, necesidad de saber y privilegios mínimos.

8.2 Subproveedores. El Proveedor impondrá requisitos contractuales escritos equivalentes a aquellos relacionados con la privacidad y la seguridad de los datos en este ISR a cualquier Subproveedor

antes de que dicho Subproveedor obtenga acceso a los Datos de Chubb. Chubb tendrá el derecho de revisar y aprobar previamente a cualquier Subproveedor. Cualquier acto u omisión por parte de cualquier Subproveedor que corresponda a un incumplimiento de este ISR si fuese cometido por el Proveedor, será considerado como un incumplimiento del Proveedor, y el Proveedor será el responsable. El Proveedor será totalmente responsable de todos los Subproveedores utilizados por el Proveedor en el desempeño de cualquier Servicio.

Por el PROVEEDOR:	**Por Chubb [entidad aplicable]**
_____	_____
NOMBRE: _____	**NOMBRE:** _____
CARGO: _____	**CARGO:** _____
FECHA: _____	**FECHA:** _____