Requisitos de seguridad de la información

1. Introducción

El Proveedor y CWT han celebrado un contrato en virtud del cual el Proveedor ha aceptado proporcionar servicios y/o productos según los términos de dicho contrato (" **Acuerdo** "). El Proveedor acepta que cumplirá y hará que los Terceros que actúen en su nombre cumplan con los requisitos de seguridad de la información contenidos en este documento (" **Requisitos de Seguridad de la Información ")** y las medidas de seguridad de la información requeridas (" **Medidas de Seguridad Técnicas y Organizativas** "). Los Requisitos de Seguridad de la Información y las Medidas de Seguridad Técnicas y Organizativas se incorporan y forman parte del Acuerdo.

2. Definiciones

2.1 A menos que se establezca o amplíe lo contrario en el presente, los términos definidos tendrán el mismo significado que se establece en el Acuerdo. Los siguientes términos definidos se aplicarán a estos Requisitos de seguridad de la información. Si existe un conflicto entre la definición contenida en el Acuerdo y las del presente, prevalecerá la definición de este documento en lo que respecta a los requisitos de seguridad de la información.

"**Afiliados**", a menos que se defina de otro modo en el Acuerdo, significa, con referencia a una parte, cualquier empresa u otra entidad legal que, en la fecha de firma del Acuerdo, directa o indirectamente: (i) controle a una parte; o (ii) esté controlada por una parte; o (iii) esté controlada por una empresa o entidad que controle directa o indirectamente a una parte. A estos efectos, se entenderá por "control" el derecho a ejercer más del cincuenta por ciento (50%) del derecho de voto o similar; pero sólo mientras dicho control continúe existiendo.

"Empleado autorizado" se refiere a los empleados del Proveedor que tienen la necesidad de conocer o acceder de otro modo a Información confidencial e Información personal para permitir que el Proveedor cumpla con sus obligaciones en virtud del Acuerdo.

"**Parte Autorizada" o "Partes Autorizadas**" significa los (i) Empleados Autorizados del Proveedor; y (ii) Terceros que tienen la necesidad de conocer o acceder de otro modo a la Información personal y la Información confidencial para permitir que el Proveedor cumpla con sus obligaciones en virtud del Acuerdo, y que están sujetos por escrito a la confidencialidad y otras obligaciones suficientes para proteger la Información personal y la Información confidencial. de acuerdo con los términos y condiciones del Acuerdo y este documento.

"Información Confidencial" hace referencia a cualquier información comercialmente sensible, patentada o confidencial relacionada con (a) CWT, sus socios y sus Filiales; (b) un cliente de CWT y empleados, contratistas, subcontratistas o proveedores de clientes de CWT; (c) personal de CWT; (d) sus socios independientes y empresas conjuntas ; o (e) el contenido y/o propósito del Acuerdo, ya sea oral, por escrito o que por cualquier otro medio pueda directa o indirectamente llegar a manos del Proveedor o de las Partes Autorizadas como

resultado de o en relación con el Convenio. Para evitar dudas, todo Producto de Trabajo constituirá Información Confidencial.

“CWT” a menos que se defina de otra manera en el Acuerdo, significa la entidad de CWT descrita en el Acuerdo, así como sus Filiales.

" **Zona desmilitarizada** " o " **DMZ** " es una red o subred que se encuentra entre una red interna confiable, como una red de área local (LAN) privada corporativa, y una red externa no confiable, como la Internet pública. Una DMZ ayuda a evitar que los usuarios externos obtengan acceso directo a los sistemas internos y otros recursos.

El "Proceso de gestión de incidentes" es un proceso y procedimiento documentado y desarrollado por el proveedor que se debe seguir en caso de un ataque real o sospechado, una intrusión, un acceso no autorizado, una pérdida u otra violación que involucre la confidencialidad, disponibilidad o integridad. de Información Personal e Información Confidencial de CWT.

“Enmascarar” es el proceso de cubrir la información que se muestra en una pantalla.

“Dispositivos móviles y portátiles” se refiere a computadoras, dispositivos, medios y sistemas móviles y/o portátiles capaces de transportarse, moverse, transportarse o transportarse fácilmente que se utilizan en relación con el Acuerdo. Ejemplos de dichos dispositivos incluyen computadoras portátiles, tabletas, discos duros USB, dispositivos de memoria USB, asistentes digitales personales (PDA), teléfonos móviles o de datos y cualquier otro dispositivo inalámbrico, periférico o extraíble con la capacidad de almacenar información confidencial e información personal.

"Información personal", a menos que se defina de otra manera en el Acuerdo, significa como se define en el Reglamento (UE) 2016/679 y otras leyes globales aplicables de seguridad de la información, protección de datos y privacidad, significa cualquier información relacionada con una persona física identificada o identificable, que puede ser identificado directa o indirectamente, en particular por referencia a un número de identificación o a uno o más factores específicos de su identidad física, fisiológica, mental, económica, cultural o social. La Información personal es propiedad de CWT, no del Proveedor.

“Puerta de enlace de seguridad” hace referencia a un conjunto de mecanismos de control entre dos o más redes que tienen diferentes niveles de confianza que filtran y registran el tráfico que pasa o intenta pasar entre redes y los servidores administrativos y de gestión asociados. Los ejemplos de puertas de enlace de seguridad incluyen cortafuegos, servidores de administración de cortafuegos, cajas de salto, controladores de borde de sesión, servidores proxy y dispositivos de prevención de intrusiones.

"Autenticación fuerte" significa el uso de mecanismos de autenticación y metodologías de autenticación que requieren múltiples factores de autenticación, incluidos al menos dos de los siguientes: (1) Conocimiento: algo que el usuario sabe, por ejemplo, contraseña o número

de identificación personal, (2) Propiedad: algo el usuario tiene, por ejemplo, token, tarjeta inteligente, teléfono móvil y (3) Inherencia: algo que el usuario es, por ejemplo, huella digital.

"Cifrado fuerte" se refiere al uso de tecnologías de cifrado con longitudes de clave mínimas de 256 bits para el cifrado simétrico y 1024 bits para el cifrado asimétrico cuya fuerza proporciona una seguridad razonable de que protegerá la información cifrada del acceso no autorizado y es adecuada para proteger la confidencialidad. y privacidad de la información encriptada, y que incorpora una política documentada para la gestión de las claves de encriptación y los procesos asociados adecuados para proteger la confidencialidad y privacidad de las claves y contraseñas utilizadas como entradas al algoritmo de encriptación. Strong Encryption incluye, entre otros: SSL v3.0+/TLS v1.2, Protocolo de tunelización punto a punto (PPTP), AES 256, FIPS 140-2 (solo para el gobierno de los Estados Unidos), RSA 1024 bit, SHA1/SHA2 /SHA3, seguridad de protocolo de Internet (IPSEC), SFTP, SSH, Vormetric v4 o WPA2.

"Medidas de seguridad técnicas y organizativas" se refiere a cualquier actividad requerida en virtud de estos Requisitos de seguridad de la información. para acceder, administrar, transferir, procesar, almacenar, retener y destruir información o datos; para divulgar y notificar a las partes afectadas requeridas por el Acuerdo y por las leyes de protección de datos y privacidad de la información aplicables; y salvaguardar la información o los datos para garantizar la disponibilidad, integridad, confidencialidad y privacidad, o notificar a las personas sobre cualquier falla en la salvaguardia de dicha información o datos. Las medidas incluyen, entre otras, aquellas requeridas o interpretadas como requeridas bajo el Reglamento General de Protección de Datos (RGPD) de la UE, la Directiva de Servicios de Pago de la UE, la Ley de Privacidad del Consumidor de California, NYS DFS 23 NYCRR 500 , la Ley Gramm-Leach Bliley de los Estados Unidos (GLBA), la Ley de Portabilidad y Responsabilidad del Seguro Médico de los Estados Unidos (HIPAA), los requisitos de privacidad de datos de la UE/Suiza y cualquier otra ley internacional y de los EE. UU., interpretaciones legales oficiales o precedentes de casos relacionados con la información o los datos en virtud del Acuerdo .

"**Tercero"** o "**Terceros**" significa vendedor subcontratistas, consultores, personal temporal, contratistas o proveedores y/o agentes adicionales que actúan en nombre del Proveedor e incluye cualquier definición de Tercero según la legislación aplicable de la UE, los EE. UU. u otras leyes internacionales.

"**Proveedor**" significa la entidad contratante establecida en el Acuerdo junto con sus Afiliados y sus Terceros.

3 . <u>Organización de la Seguridad de la Información</u>

El proveedor deberá, como mínimo:

3.1 Asegúrese de que solo las Partes autorizadas tengan acceso a la Información personal y la Información confidencial.

3.2 Implementar Medidas de Seguridad Técnicas y Organizativas que no sean menos rigurosas que las mejores prácticas de seguridad de la información para proteger la integridad, disponibilidad y confidencialidad de la Información Confidencial, la Información Personal y otra información no pública y evitar el acceso, adquisición, divulgación, destrucción, alteración no autorizados., pérdida accidental, mal uso o daño de la Información Personal o Información Confidencial.

3.3 Establecer, implementar y mantener en consonancia con las mejores prácticas de la industria, políticas y un programa de medidas de seguridad organizativas, operativas, administrativas, físicas y técnicas y organizativas apropiadas para (1) evitar el acceso de partes no autorizadas a información personal e información confidencial en una manera no autorizada por el Acuerdo o estos Requisitos de seguridad de la información, y (2) cumplir con todas las leyes y reglamentos aplicables y los estándares de la industria aplicables.

3.4 Proporcionar a las partes autorizadas que tendrán acceso a la información personal y la información confidencial supervisión, orientación y capacitación sobre las medidas de seguridad técnicas y organizativas, incluida la capacitación que proporciona ejercicios prácticos que están alineados con los escenarios de amenazas actuales y brinda retroalimentación a quienes toman la capacitación. El Proveedor deberá proporcionar capacitación en Medidas de Seguridad Técnicas y Organizativas al momento de la contratación de un Empleado Autorizado y antes del acceso de una Parte Autorizada a la Información Confidencial y la Información Personal. Se proporcionará capacitación de actualización al menos una vez al año y tan pronto como sea posible después de cualquier cambio importante en las medidas de seguridad técnicas y organizativas del proveedor.

3.5 Brindar capacitación especializada específica para las Partes autorizadas con importantes funciones de seguridad, incluidas, entre otras, funciones de recursos humanos o tecnología de la información, y cualquier función de administrador de tecnología. Como mínimo, la capacitación especializada deberá incluir, según corresponda a la función, procedimientos de seguridad de la información, uso aceptable de los recursos de seguridad de la información, amenazas actuales a los sistemas de información, características de seguridad de sistemas específicos y procedimientos de acceso seguro.

3.6 Tomar medidas razonables para evitar el acceso no autorizado o la pérdida de Información personal e Información confidencial y los servicios, sistemas, dispositivos o medios que contienen esta información.

3.7 Emplear procesos y procedimientos de evaluación de riesgos para evaluar regularmente los sistemas utilizados para proporcionar servicios o productos a CWT. El Proveedor deberá remediar dichos riesgos tan pronto como sea razonablemente posible y de acuerdo con el nivel de riesgo para la Información personal y la Información confidencial dadas las amenazas conocidas en el momento de la identificación. Operar un proceso para permitir el reporte de riesgos o sospechas de incidentes al equipo de seguridad del Proveedor.

3.8 En la medida en que el Proveedor preste servicios de conformidad con el Acuerdo en las instalaciones de CWT o utilice servicios, sistemas, dispositivos o medios propiedad de CWT,

operados o administrados por este, el Proveedor deberá hacer que todas las Partes autorizadas cumplan con todas las políticas de CWT puestas a disposición del Proveedor, a su disposición. solicitud, que sean aplicables a dicho acceso. El Proveedor notificará de inmediato a CWT por escrito cuando una Parte autorizada ya no necesite acceder a la Información personal o a la Información confidencial para que el Proveedor proporcione productos o servicios a CWT, incluido, entre otros, cuando una Parte autorizada finalice o ya no esté realizando servicios bajo el Acuerdo.

3.9 Mantener registros de las partes autorizadas y los recursos de proveedores que acceden, transfieren, mantienen, almacenan o procesan información personal e información confidencial.

3.10 Realizar verificaciones exhaustivas de antecedentes de todas las Partes autorizadas antes de la contratación, en la medida permitida por la ley. La verificación integral de antecedentes de las personas incluirá, como mínimo, el historial de empleo anterior de la persona, antecedentes penales, historial crediticio, verificación de referencias y cualquier requisito adicional de verificación de antecedentes estándar de la industria.

3.11 Tener uno o más miembros del personal calificado designados con la responsabilidad de mantener su programa de seguridad de la información y deberán informar sobre su programa de seguridad de la información al menos una vez al año a la junta directiva del Proveedor o al órgano de gobierno equivalente. El proveedor se asegurará de que su personal de seguridad tenga la experiencia y capacitación necesarias y razonables en seguridad de la información, incluido el mantenimiento de conocimientos sobre amenazas cambiantes y contramedidas. Previa solicitud, el Proveedor proporcionará a CWT un punto de contacto para todos los elementos relacionados con la seguridad de la información.

3.12 Requerir compromisos contractuales de no divulgación o confidencialidad de las Partes autorizadas antes de proporcionarles acceso a Información personal e Información confidencial.

3.13 Garantizar que todas las Partes Autorizadas que puedan estar realizando trabajos en virtud del Acuerdo o que puedan tener acceso a Información Personal o Información Confidencial cumplan con estas Medidas de Seguridad Técnicas y Organizativas que se evidenciarán mediante un acuerdo por escrito no menos restrictivo que estos Requisitos de Seguridad de la Información.

4. Seguridad Física y Ambiental

El proveedor deberá, como mínimo:

4.1 Asegúrese de que todos los sistemas del Proveedor y otros recursos destinados a ser utilizados por múltiples usuarios estén ubicados en instalaciones físicas seguras con acceso limitado y restringido solo a personas autorizadas.

4.2 Supervisar y registrar, con fines de auditoría, acceso a las instalaciones físicas que contienen sistemas y otros recursos destinados a ser utilizados por múltiples usuarios utilizados en relación con el cumplimiento del Proveedor de sus obligaciones en virtud del Acuerdo.

4.3 Requerir que todas las partes autorizadas cumplan con una política de escritorio limpio y bloqueen las pantallas de las estaciones de trabajo antes de abandonar las áreas de trabajo.

4.4 Recoger todos los activos de la empresa al terminar el empleo o terminar el contrato.

4.5 Limite y controle el acceso físico a sus instalaciones de acuerdo con los siguientes requisitos:

a. Se registra el acceso de los visitantes, el cual se mantiene durante tres (3) meses, incluyendo el nombre del visitante, la empresa a la que representa y el nombre del empleado que autoriza el acceso físico. Los visitantes deben ser acompañados por un empleado del Proveedor en todo momento.
b. El acceso está restringido al personal apropiado, según la necesidad de saber.
c. Todos los empleados deben usar un gafete con el nombre provisto por la compañía y todos los visitantes o terceros deben usar un gafete de invitado/visitante provisto por la compañía.
d. El acceso se revoca inmediatamente después de la terminación del personal del Proveedor o Tercero, y todos los mecanismos físicos de acceso, como llaves, tarjetas de acceso, etc., se devuelven o deshabilitan.
e. El centro de datos o la sala de computadoras está bloqueado y el acceso está limitado solo a aquellos que necesitan acceso para realizar sus tareas laborales.
f. Donde lo permita la ley, use cámaras de video para monitorear el acceso físico individual a áreas sensibles y revise dichos datos con regularidad. Las secuencias de video deben almacenarse durante un mínimo de tres (3) meses.
g. El equipo utilizado para almacenar, procesar o transmitir información personal e información confidencial debe estar protegido físicamente, incluidos los puntos de acceso inalámbrico, las puertas de enlace, los dispositivos portátiles, el hardware de redes/comunicaciones y las líneas de telecomunicaciones.

4.6 Implementar controles para minimizar el riesgo y protegerse contra amenazas físicas.

4.7 Mantener todos los activos de hardware que procesan o manejan información personal e información confidencial de acuerdo con los requisitos de servicio recomendados por el fabricante.

4.8 Restrinja la sala de conferencias y otras redes de acceso público y los conectores de red de forma lógica y física desde la red interna del proveedor y restringida solo a usuarios autenticados o deshabilitada de forma predeterminada.

4.9 Proteja cualquier dispositivo que capture datos de tarjetas de pago a través de la interacción física directa contra la manipulación y la sustitución mediante la inspección periódica de las superficies del dispositivo para detectar la manipulación o la sustitución; proporcionar

capacitación para que el personal esté al tanto de intentos de manipulación o reemplazo de dispositivos.

4.10 Controle y separe los puntos de acceso, como las áreas de entrega y carga y otros puntos de todos los centros que acceden, administran, almacenan o procesan información personal e información confidencial.

4.11 Asegúrese de que los centros de datos del proveedor tengan dispositivos de calefacción, refrigeración, supresión de incendios, detección de agua y detección de calor/humo. Los centros de datos y las salas de computación de los proveedores deben estar libres de materiales combustibles (p. ej., cajas, papeles, etc.) o almacenarse en gabinetes metálicos.

5. Control de acceso

El proveedor deberá, como mínimo:

5.1 Tome todas las medidas razonables para evitar que cualquier persona que no sean las Partes autorizadas acceda a la Información personal y la Información confidencial de cualquier manera o para cualquier propósito no autorizado por CWT y el Acuerdo.

5.2 Separe la información de CWT de los datos de otros clientes del Proveedor o de las propias aplicaciones e información del Proveedor, ya sea mediante el uso de servidores separados físicamente o mediante el uso de controles de acceso lógico donde no se implemente la separación física de los servidores.

5.3 Identificar y solicitar a los propietarios apropiados que revisen y aprueben el acceso a los sistemas utilizados para acceder, procesar, administrar o almacenar Información personal e Información confidencial al menos trimestralmente para eliminar el acceso no autorizado; y mantener y rastrear las aprobaciones de acceso.

5.4 Eliminar el acceso a los sistemas que gestionan la Información personal y la Información confidencial dentro de las 24 horas posteriores a la terminación de la relación de la Parte autorizada con el Proveedor; y mantener procedimientos razonables para eliminar el acceso a dichos sistemas dentro de los tres días hábiles cuando ya no sea necesario o relevante para el desempeño de sus funciones. Todos los demás ID de usuario deben deshabilitarse o eliminarse después de 90 días calendario de inactividad.

5.5 Restrinja el acceso del administrador del sistema (también conocido como raíz, privilegiado o superusuario) a los sistemas operativos destinados a ser utilizados por múltiples usuarios solo a personas que requieran un acceso de alto nivel en el desempeño de sus trabajos. Utilice ID de administrador del sistema de pago con credenciales de inicio de sesión de usuario individuales y registros de actividad para administrar el acceso de alta seguridad y reducir el acceso de alto nivel a un número muy limitado de usuarios. Exigir a los administradores de aplicaciones, bases de datos, redes y sistemas que restrinjan el acceso de los usuarios solo a los comandos, datos, sistemas y otros recursos necesarios para que realicen las funciones

autorizadas. Las funciones administrativas del sistema y las listas de acceso deben revisarse al menos una vez al año.

5.6 Hacer cumplir la regla del privilegio mínimo (es decir, limitar el acceso solo a los comandos, la información, los sistemas y otros recursos necesarios para realizar las funciones autorizadas de acuerdo con la función de trabajo de uno).

5.7 Requerir autenticación sólida para todos los accesos administrativos que no sean de consola, cualquier acceso remoto y todos los accesos administrativos a entornos de nube.

5.8 Prohibir y emplear Medidas de Seguridad Técnicas y Organizativas para garantizar que la Información Personal no pueda copiar, mover o almacenar Información Personal en discos duros locales o cortar y pegar o imprimir Información Personal.

5.9 Active el uso de las capacidades de acceso remoto solo cuando sea necesario, controle mientras está en uso y desactívelo inmediatamente después del uso.

5.10 Requerir autenticación fuerte para conectarse a recursos internos del proveedor que contengan información personal e información confidencial.

6. <u>Identificación y autenticación</u>

El proveedor deberá, como mínimo:

6.1 Asigne identificaciones de usuario únicas a usuarios individuales y asigne mecanismos de autenticación a cada cuenta individual.

6.2 Utilizar un proceso documentado de gestión del ciclo de vida de ID de usuario que incluya, entre otros, procedimientos para la creación de cuentas aprobadas, la eliminación oportuna de cuentas y la modificación de cuentas (p. ej., cambios en los privilegios, intervalo de acceso, funciones/roles) para todo acceso a Información personal y Información confidencial y en todos los entornos (p. ej., producción, prueba, desarrollo, etc.). Dicho proceso deberá incluir la revisión de los privilegios de acceso y la validez de la cuenta que se realizará al menos trimestralmente.

6.3 Restrinja todo acceso a la información personal y la información confidencial a aquellos que utilicen una identificación de usuario y una contraseña válidas, y exija que las identificaciones de usuario únicas empleen uno de los siguientes: contraseña o frase de contraseña, autenticación de dos factores o un valor biométrico.

6.4 Requerir complejidad de contraseña y cumplir con los siguientes requisitos de construcción de contraseña: un mínimo de doce (12) caracteres de longitud para contraseñas del sistema y cuatro (4) caracteres para contraseñas de tabletas y teléfonos inteligentes. Las contraseñas del sistema deben contener tres (3) de los siguientes: mayúsculas, minúsculas, números o caracteres especiales. Las contraseñas tampoco deben ser iguales a la ID de usuario con la que están asociadas, contener una palabra del diccionario, números secuenciales o repetidos,

y no ser una de las últimas 24 contraseñas. Requerir el vencimiento de la contraseña a intervalos regulares que no excedan los noventa (90) días. Enmascare todas las contraseñas cuando se muestren.

6.5 Limite los intentos de inicio de sesión fallidos a no más de cinco (5) intentos de inicio de sesión fallidos dentro de las 24 horas y bloquee la cuenta de usuario al alcanzar ese límite en un estado persistente. El acceso a la cuenta de usuario puede reactivarse posteriormente a través de un proceso manual que requiere la verificación de la identidad del usuario.

6.6 Verifique la identidad del usuario y establezca un uso único y restablezca las contraseñas a un valor único para cada usuario. Cambie sistemáticamente después del primer uso.

6.7 Utilice un método seguro para el transporte de credenciales de autenticación (p. ej., contraseñas) y mecanismos de autenticación (p. ej., tokens o tarjetas inteligentes).

6.8 Restrinja la cuenta de servicio y las contraseñas de proxy a un mínimo de 20 caracteres, incluidos mayúsculas, minúsculas y caracteres numéricos, así como símbolos especiales. Cambie la cuenta de servicio y las contraseñas de proxy al menos una vez al año y después de la terminación del empleo de cualquier persona que tenga conocimiento de la contraseña.

6.9 Finalice las sesiones interactivas o active un protector de pantalla de bloqueo seguro que requiera autenticación, después de un período de inactividad que no exceda los quince (15) minutos.

6.10 Utilice un método de autenticación basado en la confidencialidad de la información personal y la información confidencial. Siempre que se almacenen las credenciales de autenticación, el Proveedor las protegerá mediante Cifrado fuerte.

6.11 Configure los sistemas para que se agoten automáticamente después de un período máximo de inactividad de la siguiente manera: servidor (15 minutos), estación de trabajo (15 minutos), dispositivo móvil (4 horas), protocolo de configuración dinámica de host (7 días), red privada virtual (24 horas).

7. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

El proveedor deberá, como mínimo:

7.1 Mostrar un banner de advertencia en las pantallas o páginas de inicio de sesión según lo especificado por escrito por CWT para productos o servicios de la marca CWT o para productos y software desarrollados para CWT.

7.2 Devuelva todos los dispositivos de acceso proporcionados o propiedad de CWT tan pronto como sea posible, pero en ningún caso más de quince (15) días después del primero de los siguientes:

a. expiración o terminación del Acuerdo;
b. la solicitud de CWT para la devolución de dicha propiedad; o
c. la fecha en que el Proveedor ya no necesita dichos dispositivos.

7.3 Emplear una metodología eficaz de gestión de aplicaciones que incorpore medidas de seguridad técnicas y organizativas en el proceso de desarrollo de software y garantizar que el proveedor implemente las medidas de seguridad técnicas y organizativas, representadas por las mejores prácticas de la industria, de manera oportuna.

7.4 Siga los procedimientos de desarrollo estándar de la industria, incluida la separación de acceso y código entre los entornos de producción y los que no son de producción y la segregación de funciones asociada entre dichos entornos.

7.5 Asegúrese de que los controles internos de seguridad de la información para el desarrollo de software se evalúen regularmente y reflejen las mejores prácticas de la industria, y revise e implemente estos controles de manera oportuna.

7.6 Administre la seguridad del proceso de desarrollo y asegúrese de que se implementen y sigan prácticas de codificación seguras, incluidos los controles criptográficos apropiados, las protecciones contra códigos maliciosos y un proceso de revisión por pares.

7.7 Realice pruebas de penetración en aplicaciones funcionalmente completas antes de lanzarlas a producción y posteriormente, al menos una vez al año y después de cualquier modificación significativa en el código fuente o la configuración que se alinee con OWASP, CERT, SANS Top 25 y PCI-DSS. Corrija cualquier vulnerabilidad explotable antes de la implementación en el entorno de producción.

7.8 Use datos anonimizados u ofuscados en entornos que no sean de producción. Nunca use datos de producción de texto sin formato en ningún entorno que no sea de producción, y nunca use información personal en entornos que no sean de producción por ningún motivo. Asegúrese de que todos los datos de prueba y las cuentas se eliminen antes del lanzamiento de producción.

7.9 Revise el código fuente abierto o gratuito aprobado por CWT, el software, las aplicaciones o los servicios en busca de fallas, errores, problemas de seguridad o incumplimiento de los términos de licencia de código abierto o gratuito. El Proveedor notificará a CWT antes de usar cualquier código fuente abierto o gratuito y, si CWT lo aprueba, proporcionará a CWT el nombre, la versión y la URL del código fuente abierto o gratuito. El Proveedor declara y garantiza que (a) cualquier código fuente abierto o gratuito que utilice en sus productos o servicios se licenciará bajo licencias de código fuente abierto o gratuito "permisivas" y no bajo licencias Restrictivas, Recíprocas, Hereditarias o Copyleft; (b) El proveedor tiene derecho a modificar, adaptar libremente el código fuente abierto o gratuito y combinar el código fuente abierto o gratuito o contener código fuente abierto o gratuito con código propietario sin imponer restricciones a dichas enmiendas, adaptaciones o combinaciones o código propietario que contenga código fuente abierto o gratuito y cómo se pueden otorgar licencias en adelante (colectivamente, " **trabajos derivados** ") y (c) dichos trabajos derivados no

estarán sujetos a ninguna licencia de código abierto o gratuito que requiera licenciar el trabajo derivado o ponerlo a disposición sin cargo a terceros bajo los términos de licencia de fuente abierta o libre.

7.10 No compartir ningún código creado en virtud del Acuerdo, independientemente de la etapa de desarrollo, en ningún entorno compartido o no privado, como un repositorio de código de acceso abierto, independientemente de la protección con contraseña.

8. Software e integridad de datos

El proveedor deberá, como mínimo:

8.1 En entornos donde el software antivirus está disponible comercialmente, tenga un software antivirus actual instalado y ejecutándose para buscar y eliminar rápidamente o poner en cuarentena virus y otro malware de cualquier sistema o dispositivo.

8.2 Separe la información y los recursos que no son de producción de la información y los recursos de producción.

8.3 Asegúrese de que los equipos utilicen un proceso de control de cambios documentado para todos los cambios del sistema, incluidos los procedimientos de restitución para todos los entornos de producción y los procesos de cambio de emergencia. Incluya pruebas, documentación y aprobaciones para todos los cambios del sistema y solicite la aprobación de la gerencia para cambios significativos en dichos procesos.

8.4 Cree y mantenga una zona PCI si el proveedor procesa o almacena datos del titular de la tarjeta.

8.5 Para las aplicaciones que utilizan una base de datos que permite modificaciones a la Información personal y la Información confidencial, habilite y mantenga las funciones de registro de auditoría de transacciones de la base de datos que conservan los registros de auditoría de transacciones de la base de datos durante un mínimo de un (1) año con tres meses inmediatamente disponibles para el análisis.

8.6 Revise el software para encontrar y remediar las vulnerabilidades de seguridad durante la implementación inicial y después de cualquier modificación y actualización significativa.

8.7 Realizar pruebas de garantía de calidad para los componentes de seguridad (p. ej., pruebas de las funciones de identificación, autenticación y autorización), así como cualquier otra actividad diseñada para validar la arquitectura de seguridad, durante la implementación inicial y tras cualquier modificación y actualización significativa.

9. Seguridad del sistema

El proveedor deberá, como mínimo:

9.1 Cree y actualice regularmente las versiones más recientes del flujo de datos y los diagramas del sistema utilizados para acceder, procesar, administrar o almacenar información personal e información confidencial.

9.2 Supervise activamente los recursos de la industria (p. ej., , www.cert.org y las listas de correo y los sitios web de los proveedores de software pertinentes) para recibir notificaciones oportunas de todas las alertas de seguridad correspondientes a los sistemas del proveedor y otros recursos de información.

9.3 Administre de manera efectiva las claves criptográficas al reducir el acceso a las claves por la menor cantidad de custodios necesarios, almacenar claves criptográficas secretas y privadas mediante el cifrado con una clave al menos tan sólida como la clave de cifrado de datos y almacenarlas por separado de la clave de cifrado de datos en un lugar seguro. dispositivo criptográfico, en el menor número de ubicaciones posibles. Cambie las claves criptográficas predeterminadas en la instalación y al menos cada dos años, y deseche las claves antiguas de forma segura.

9.4 Escanee los sistemas externos e internos y otros recursos de información, incluidos, entre otros, redes, servidores, aplicaciones y bases de datos, con el software de escaneo de vulnerabilidades de seguridad estándar de la industria aplicable para descubrir vulnerabilidades de seguridad, asegúrese de que dichos sistemas y otros recursos estén correctamente reforzado e identificar cualquier red inalámbrica no autorizada al menos trimestralmente y antes del lanzamiento para aplicaciones y para cambios y actualizaciones significativos dentro de los plazos resultantes de análisis de riesgo basados en políticas y estándares de TI razonables y generalmente aceptados.

9.5 Asegúrese de que todos los sistemas y otros recursos del proveedor estén y permanezcan reforzados, lo que incluye, entre otros, la eliminación o desactivación de la red no utilizada y otros servicios y productos (por ejemplo, finger, rlogin, ftp y Protocolo de control de transmisión/Protocolo de Internet simple (TCP/ servicios y productos IP) e instalar un firewall del sistema, envoltorios de Protocolo de control de transmisión (TCP) o tecnología similar.

9.6 Implementar uno o más Sistemas de detección de intrusiones (IDS), Sistemas de prevención de intrusiones (IPS) o Sistemas de detección y prevención de intrusiones (IDP) en un modo de operación activo que monitorea todo el tráfico que ingresa y sale de los sistemas y otros recursos en conjunto con el Acuerdo en entornos en los que dicha tecnología esté comercialmente disponible y en la medida de lo posible.

9.7 Mantener un proceso de clasificación de riesgos para los hallazgos de la evaluación de vulnerabilidades alineados con las mejores prácticas de la industria para remediar las vulnerabilidades de seguridad en cualquier sistema u otro recurso, incluidas, entre otras, aquellas descubiertas a través de publicaciones de la industria, escaneo de vulnerabilidades, escaneo de virus y revisión de registros de seguridad. , y aplique los parches de seguridad apropiados con prontitud con respecto a la probabilidad de que dicha vulnerabilidad pueda ser o esté en proceso de ser explotada. Los hallazgos y parches de la evaluación de vulnerabilidades críticas deben repararse inmediatamente después de su disponibilidad y, en

ningún caso, más de 7 días después del lanzamiento. Los resultados de la evaluación de alta vulnerabilidad y los parches deben repararse dentro de los 30 días posteriores al lanzamiento. Los hallazgos y parches de la evaluación de vulnerabilidades medias deben corregirse en un plazo de 90 días calendario. Los hallazgos y parches de la evaluación de vulnerabilidades bajas deben corregirse en un plazo de 120 días calendario.

9.8 Realice pruebas de penetración de red y segmentación interna y externamente al menos una vez al año y después de cualquier actualización o modificación significativa de la infraestructura o la aplicación.

9.9 Elimine o deshabilite el software no autorizado descubierto en los sistemas del Proveedor y emplee controles de malware estándar de la industria, incluida la instalación, actualización periódica y uso rutinario de productos de software antimalware en todos los servicios, sistemas y dispositivos que pueden usarse para acceder a Información personal y CWT. Información confidencial. Utilice un software antivirus confiable y con las mejores prácticas de la industria cuando sea posible y asegúrese de que dichas definiciones de virus permanezcan actualizadas.

9.10 Mantenga el software actualizado en todos los servicios, sistemas y dispositivos que puedan usarse para acceder a la Información personal y a la Información confidencial de CWT, incluido el mantenimiento adecuado de los sistemas operativos y la instalación exitosa de parches de seguridad razonablemente actualizados.

9.11 Asigne responsabilidades de administración de seguridad para configurar sistemas operativos host a personas específicas.

9.12 Cambie todos los nombres de cuenta predeterminados y/o las contraseñas predeterminadas.

10. Monitoreo

El proveedor deberá, como mínimo:

10.1 Conservar los datos de registro para la Información personal y la Información confidencial durante al menos 12 meses a partir de la fecha en que se crearon los datos de registro y poner el registro y dichos datos a disposición de CWT dentro de un plazo razonable y previa solicitud, a menos que se especifique en otra parte del Acuerdo. Los registros deben diseñarse para detectar y responder a incidentes e incluir, entre otros:

a. Todo acceso de usuario individual a Información personal e Información confidencial
b. Todas las acciones realizadas por aquellos con privilegios administrativos o de raíz
c. Acceso de todos los usuarios a los registros de auditoría
d. Intentos de acceso lógico no válidos
e. Uso y cambios en los mecanismos de identificación y autenticación

10.2 sistema principal de los terceros del proveedor para los sistemas que contengan información personal e información confidencial y contar con un programa formal de garantía de terceros para garantizar que los terceros o subcontratistas del proveedor cuenten con los controles y

certificaciones de seguridad apropiados Tener una evaluación de seguridad en la nube realizada si CWT los datos residen en un entorno de nube.

10.3 Restrinja el acceso a los registros de seguridad a personas autorizadas y proteja los registros de seguridad de modificaciones no autorizadas.

10.4 Implementar un mecanismo de detección de cambios (p. ej., monitoreo de integridad de archivos) para alertar al personal sobre la modificación no autorizada de archivos críticos del sistema, archivos de configuración o archivos de contenido; configurar el software para realizar comparaciones de archivos críticos semanalmente.

10.5 Revisar, al menos semanalmente, todos los registros de auditoría relacionados con la seguridad en los sistemas que contienen información personal e información confidencial para detectar anomalías y documentar y resolver todos los problemas de seguridad registrados de manera oportuna.

10.6 Revise diariamente todos los eventos de seguridad, los registros de los componentes del sistema que almacenan, procesan o transmiten datos del titular de la tarjeta, los registros de los componentes críticos del sistema y los registros de los servidores y los componentes del sistema que realizan funciones de seguridad.

11. <u>Pasarelas de seguridad</u>

El proveedor deberá, como mínimo:

11.1 Requerir autenticación sólida para el acceso administrativo y/o de gestión a Security Gateways, incluido, entre otros, cualquier acceso con el fin de revisar los archivos de registro.

11.2 Tener y utilizar controles, políticas, procesos y procedimientos documentados para garantizar que los usuarios no autorizados no tengan acceso administrativo o de gestión a los Security Gateways, y que los niveles de autorización de los usuarios para administrar y gestionar los Security Gateways sean adecuados.

11.3 Tenga controles estrictos sobre la seguridad del correo electrónico, como la configuración de los protocolos de autenticación DKIM y SPF que ayudan a validar que un mensaje de correo electrónico proviene de una fuente confiable y validada. Implementación de DMARC en los servidores de recepción de correo electrónico.

11.4 Al menos una vez cada seis (6) meses, asegúrese de que las configuraciones de Security Gateway estén reforzadas seleccionando una muestra de Security Gateways y verificando que cada conjunto de reglas predeterminado y conjunto de parámetros de configuración garantice lo siguiente:

una. El enrutamiento de origen del Protocolo de Internet (IP) está deshabilitado,
b. La dirección de loopback tiene prohibido ingresar a la red interna,
C. Se implementan filtros anti-spoofing,

d. Los paquetes de difusión no pueden ingresar a la red,
mi. Las redirecciones del Protocolo de mensajes de control de Internet (ICMP) están deshabilitadas,
F. Todos los conjuntos de reglas terminan con una declaración "DENY ALL", y
gramo. Cada regla es rastreable a una solicitud comercial específica.

11.5 Asegúrese de que se utilicen herramientas de monitoreo para validar que todos los aspectos de Security Gateways (por ejemplo, hardware, firmware y software) estén continuamente operativos.

Asegúrese de que todas las puertas de enlace de seguridad estén configuradas e implementadas de manera que todas las puertas de enlace de seguridad no operativas nieguen todo acceso.

11.6 Los paquetes entrantes de la red externa que no es de confianza deben terminar dentro de la zona desmilitarizada (" **DMZ** ") y no se les debe permitir que fluyan directamente a través de la red interna de confianza. Todos los paquetes entrantes que fluyen hacia la red interna confiable solo deben originarse dentro de la DMZ. La DMZ debe estar separada de la red externa que no es de confianza mediante el uso de un Security Gateway y debe estar separada de la red interna de confianza mediante el uso de:

una. otro Security Gateway, o
b. el mismo Security Gateway utilizado para separar la DMZ de la red externa no confiable, en cuyo caso el Security Gateway debe garantizar que los paquetes recibidos de la red externa no confiable se eliminen inmediatamente o, si no se eliminan, se enruten solo a la DMZ sin ningún otro procesamiento de dichos paquetes entrantes se realizaron de forma diferente a la posibilidad de escribir los paquetes en un registro.

Lo siguiente solo debe estar ubicado dentro de la red interna de confianza:

una. Cualquier Información personal e Información confidencial de CWT almacenada sin el uso de Strong Encryption,
b. La copia oficial del registro de información.
C. servidores de bases de datos,
d. Todos los registros exportados, y
mi. Todos los entornos utilizados para desarrollo, prueba, sandbox, producción y cualquier otro entorno similar; y todas las versiones del código fuente.

11.7 Las credenciales de autenticación que no estén protegidas por el uso de Strong Encryption no deben ubicarse dentro de la DMZ.

12. Seguridad de la red

El proveedor deberá, como mínimo:

12.1 A petición de CWT, proporcione a CWT un diagrama de red lógica que documente los sistemas y las conexiones a otros recursos, incluidos enrutadores, conmutadores, cortafuegos, sistemas IDS, topología de red, puntos de conexión externos, puertas de enlace, redes inalámbricas y cualquier otro dispositivo compatible con CWT.

12.2 Mantenga un proceso formal para aprobar, probar y documentar todas las conexiones de red y los cambios en las configuraciones del firewall y del enrutador. Configure cortafuegos para denegar y registrar paquetes sospechosos, y restrinja para permitir solo el tráfico apropiado y autorizado, denegando todo el resto del tráfico a través del cortafuegos. Revise las reglas del firewall cada seis meses.

12.3 Instale un firewall en cada conexión a Internet y entre cualquier DMZ y la zona de red interna. Cualquier sistema que almacene información personal debe residir en la zona de la red interna, separado de la DMZ y otras redes no confiables.

12.4 Supervise el firewall en el perímetro e internamente para controlar y proteger el flujo de tráfico de red que ingresa o sale del borde o límite, según sea necesario.

12.5 Instale tecnologías de detección de amenazas como Detección y respuesta de red (NDR), Detección y respuesta de punto final (EDR) y Detección y respuesta extendida (XDR) que ofrecen una solución integral para detectar y responder a varios ciberataques o ataques de ransomware.

12.6 Mantener un proceso documentado y controles implementados para detectar y manejar intentos no autorizados de acceder a Información personal e Información confidencial de CWT.

12.7 Al proporcionar servicios y productos basados en Internet a CWT, proteja la Información personal y la Información confidencial mediante la implementación de una red DMZ. Los servidores web que brindan servicio a CWT residirán en la DMZ. Cualquier sistema o recurso de información que almacene Información personal e Información confidencial (como servidores de aplicaciones y bases de datos) residirá en una red interna confiable. El proveedor utilizará DMZ para servicios y productos de Internet.

12.8 Restrinja el tráfico saliente no autorizado de aplicaciones que procesan, almacenan o transmiten información personal e información confidencial a direcciones IP dentro de la DMZ e Internet.

12.9 Al utilizar tecnologías de redes inalámbricas basadas en radiofrecuencia (RF) para realizar o respaldar servicios y productos para CWT, el Proveedor se asegurará de que toda la Información personal y la Información confidencial transmitida esté protegida mediante el uso de tecnologías de encriptación apropiadas suficientes para proteger la confidencialidad de la Información personal. e Información Confidencial; siempre que, sin embargo, en cualquier caso dicho cifrado utilice longitudes de clave no inferiores a 256 bits para el cifrado simétrico y 2048 bits para el cifrado asimétrico. Escanee, identifique y deshabilite periódicamente los puntos de acceso inalámbrico no autorizados.

12.10 Seguridad en la nube: cuando los datos de CWT residen en la nube o el proveedor utiliza un entorno de nube de terceros, incluidos, entre otros, Infraestructura como servicio (IaaS), Software como servicio (Saas) y Plataforma como servicio (PaaS), el proveedor debe implementar o evaluar la gestión de la postura de seguridad en la nube para descubrir y remediar automáticamente las amenazas, las configuraciones incorrectas, el uso indebido y las infracciones de cumplimiento en las nubes públicas.

13. Requisitos de conectividad

13.1 En el caso de que el Proveedor tenga, o se le proporcione, conectividad a la Información personal y a los recursos de Información confidencial de CWT junto con el Acuerdo, además de lo anterior, si el Proveedor tiene o se le proporciona conectividad al entorno de CWT, el Proveedor deberá, en un mínimo:

una. Utilice únicamente las instalaciones y metodologías de conexión acordadas mutuamente para interconectar el entorno de CWT con los recursos del Proveedor.

b. NO establecer interconexión con el entorno de CWT sin el consentimiento previo por escrito de CWT.

C. Proporcionar acceso a CWT a cualquier instalación del Proveedor aplicable durante el horario comercial normal para el mantenimiento y soporte de cualquier equipo (por ejemplo, enrutador) proporcionado por CWT en virtud del Acuerdo para la conectividad a los recursos de Información personal e Información confidencial.

d. Usar cualquier equipo proporcionado por CWT en virtud del Acuerdo para la conectividad con el entorno de CWT solo para el suministro de los servicios y productos o funciones explícitamente autorizados en el Acuerdo.

mi. Si la metodología de conectividad acordada requiere que el Proveedor implemente un Security Gateway, mantenga registros de todas las sesiones que utilicen dicho Security Gateway. Estos registros de sesión deben incluir información suficientemente detallada para identificar al usuario final o la aplicación, la dirección IP de origen, la dirección IP de destino, los puertos/protocolos de servicio utilizados y la duración del acceso. Estos registros de sesión deben conservarse durante un mínimo de seis (6) meses desde la creación de la sesión.

F. Permita que CWT recopile información relacionada con el acceso, incluido el acceso del proveedor, al entorno de CWT. CWT puede recopilar, conservar y analizar esta información para identificar posibles riesgos de seguridad sin previo aviso. Esta información puede incluir archivos de seguimiento, estadísticas, direcciones de red y los datos o pantallas reales a los que se accede o transfiere.

gramo. Suspender o terminar de inmediato cualquier interconexión al entorno de CWT si los Proveedores creen que ha habido una violación o un acceso no autorizado o siguiendo las instrucciones de CWT si CWT, a su entera discreción, cree que ha habido una violación de la seguridad o un acceso no autorizado o un uso indebido de las instalaciones de datos de CWT. o cualquier información, sistemas u otros recursos de CWT.

14. Dispositivos móviles y portátiles

El proveedor deberá, como mínimo:

14.1 No almacene información personal e información confidencial en dispositivos móviles y portátiles, a menos que esté completamente encriptada con un cifrado fuerte.

14.2 Utilice el cifrado fuerte para proteger la información personal y la información confidencial transmitida, utilizada o a la que se accede de forma remota mediante dispositivos móviles y portátiles con reconocimiento de red.

una. Cuando se utilizan Dispositivos móviles y portátiles compatibles con la red que no son computadoras portátiles para acceder y/o almacenar Información personal e Información confidencial, dichos dispositivos deben ser capaces de eliminar todas las copias almacenadas de Información personal e Información confidencial al recibir a través de la red una copia debidamente autenticada. dominio. (Nota: esta capacidad se suele denominar capacidad de "borrado remoto").

b. Tener políticas, procedimientos y estándares documentados para garantizar que la Parte autorizada que debe tener el control físico de un dispositivo móvil y portátil con reconocimiento de red que no sea una computadora portátil y que almacene Información personal e Información confidencial inicie de inmediato la eliminación de todos Información personal e información confidencial cuando el dispositivo se pierde o es robado.

C. Tenga políticas, procedimientos y estándares documentados para garantizar que los Dispositivos móviles y portátiles que no sean computadoras portátiles y que no sean compatibles con la red eliminen automáticamente todas las copias almacenadas de Información personal e Información confidencial después de intentos de inicio de sesión fallidos consecutivos.

14.3 Contar con políticas, procedimientos y estándares documentados que aseguren que cualquier dispositivo móvil y portátil utilizado para acceder y/o almacenar información personal e información confidencial:

una. Están en posesión física de las Partes autorizadas;

b. Están asegurados físicamente cuando no están en posesión física de las Partes autorizadas; o

C. Hacer que su almacenamiento de datos se elimine de manera rápida y segura cuando no esté en posesión física de una Parte autorizada, o físicamente protegido, o después de 10 intentos de acceso fallidos.

14.4 Antes de permitir el acceso a la Información personal y la Información confidencial almacenada en o mediante el uso de Dispositivos móviles y portátiles, el Proveedor deberá tener y utilizar un proceso para garantizar que:

una. El usuario es un Autorizado autorizado para dicho acceso; y

b. La identidad del usuario ha sido autenticada.

14.5 Implementar una política que prohíba el uso de Dispositivos móviles y portátiles que no sean administrados y/o administrados por el Proveedor o CWT para acceder y/o almacenar Información personal e Información confidencial.

14.6 Revisar, al menos una vez al año, el uso y los controles de todos los Dispositivos móviles y portátiles administrados o gestionados por el Proveedor para garantizar que los Dispositivos móviles y portátiles puedan cumplir con las Medidas de seguridad técnicas y organizativas aplicables.

15. <u>Seguridad en Tránsito</u>

El proveedor deberá, como mínimo:

15.1 Use Strong Encryption para la transferencia de información personal e información confidencial fuera de las redes controladas por CWT o controladas por proveedores o cuando transmita información personal e información confidencial a través de cualquier red que no sea de confianza.

15.2 Para los registros que contienen Información personal e Información confidencial en formato de papel, microfichas o medios electrónicos que se transferirán físicamente, transpórtelos por mensajería segura u otro método de entrega que pueda rastrearse, empaquetarse de manera segura y según las especificaciones del fabricante. Cualquier información personal e información confidencial debe transportarse en contenedores cerrados.

16. <u>Seguridad en reposo</u>

El proveedor deberá, como mínimo:

16.1 Utilice Cifrado Fuerte para proteger la Información Personal y la Información Confidencial cuando se almacene.

16.2 No almacenar Información personal o Información confidencial electrónicamente fuera del entorno de red del Proveedor (o de la propia red informática segura de CWT) a menos que el dispositivo de almacenamiento (p. ej., cinta de copia de seguridad, computadora portátil, tarjeta de memoria, disco de computadora, etc.) esté protegido por Strong Encryption.

16.3 No almacene información personal o información confidencial en medios extraíbles (p. ej., unidades flash USB, unidades de memoria flash, tarjetas de memoria, cintas, CD o discos duros externos), excepto: con fines de copia de seguridad, continuidad comercial, recuperación ante desastres e intercambio de datos, según lo permitido y requerido bajo contrato entre el Proveedor y CWT. Si se utilizan medios extraíbles para almacenar Información personal o Información confidencial según las excepciones indicadas en esta subsección, la información debe protegerse mediante Cifrado fuerte. La ejecución automática debe estar deshabilitada para medios extraíbles y dispositivos de almacenamiento.

16.4 Almacene y asegure adecuadamente los registros que contengan Información personal o Información confidencial en formato papel o microfichas en áreas cuyo acceso esté restringido al personal autorizado.

16.5 A menos que CWT indique lo contrario por escrito, al recopilar, generar o crear Información personal o Información confidencial en papel y medios de copia de seguridad para, a través o en nombre de CWT o bajo la marca CWT, asegúrese de que dicha información sea Información personal o Información confidencial. y, siempre que sea posible, etiquetar dicha información de CWT como "Confidencial". El Proveedor reconoce que la Información personal y la Información confidencial son y seguirán siendo propiedad de CWT, independientemente del etiquetado o la ausencia del mismo.

17. <u>Devolución, retención, destrucción y eliminación</u>

El proveedor deberá, como mínimo:

17.1 Sin cargo adicional para CWT, a solicitud de CWT o al finalizar el Acuerdo, proporcione copias de cualquier Información personal e Información confidencial a CWT dentro de los treinta (30) días calendario posteriores a dicha solicitud o finalización del Acuerdo. El Proveedor devolverá o, a elección de CWT, destruirá toda la Información confidencial y la Información personal de CWT, incluidas las copias de seguridad electrónicas, impresas y seguras, según lo dispuesto en el Acuerdo o, si no lo establece el Acuerdo, dentro de los noventa (90) días calendario. días después de lo que ocurra primero entre: (a) el vencimiento o la rescisión del Acuerdo, (b) la solicitud de CWT para la devolución de la Información personal y la Información confidencial, o (c) la fecha en que el Proveedor ya no necesita la Información personal y la Información confidencial para prestar los servicios. y productos en virtud del Acuerdo.

17.2 En el caso de que CWT apruebe la destrucción como alternativa a la devolución de la Información personal y la Información confidencial, certifique por escrito, por parte de un funcionario del Proveedor, que la destrucción hace que la Información personal y la Información confidencial no se puedan recuperar ni recuperar. El Proveedor destruirá por completo todas las copias de la Información personal y la Información confidencial en todas las ubicaciones y en todos los sistemas donde se almacene la Información personal y la Información confidencial, incluidas, entre otras, las Partes autorizadas previamente aprobadas. Dicha información se destruirá siguiendo un procedimiento estándar de la industria para la destrucción completa, como DOD 5220.22M o NIST Special Publication 800-88 o utilizando un producto de desmagnetización recomendado por el fabricante para el sistema afectado. Antes de dicha destrucción, el Proveedor deberá mantener todas las Medidas de Seguridad Técnicas y Organizativas aplicables para proteger la seguridad, privacidad y confidencialidad de la Información Personal y la Información Confidencial.

17.3 Deseche la información personal y la información confidencial de CWT de una manera que garantice que la información no se pueda reconstruir en un formato utilizable. Los papeles, diapositivas, microfilmes, microfichas y fotografías deben eliminarse mediante trituración cruzada o quema. Los materiales que contengan información personal e información

confidencial de CWT en espera de destrucción deben almacenarse en contenedores seguros y transportarse mediante un tercero seguro.

18. Respuesta y notificación de incidentes

El proveedor deberá, como mínimo:

18.1 Tener y utilizar un Proceso de Gestión de Incidentes y procedimientos relacionados y dotar de personal a dicho Proceso de Gestión de Incidentes y procedimientos con recursos especializados. Inmediatamente, y en ningún caso más de veinticuatro (24) horas, notifique a CWT en iRespond@mycwt.com cada vez que se sospeche o confirme un ataque, intrusión, acceso no autorizado, pérdida u otro incidente relacionado con la información de CWT sistemas u otros recursos.

18.2 Después de notificar a CWT, proporcionar a CWT actualizaciones de estado periódicas, incluidas, entre otras, las medidas tomadas para resolver dicho incidente, en intervalos o momentos acordados mutuamente durante la duración del incidente y tan pronto como sea razonablemente posible después del cierre del incidente. , proporcione a CWT un informe escrito que describa el incidente, las acciones tomadas por el Proveedor durante su respuesta y los planes del Proveedor para acciones futuras para evitar que ocurra un incidente similar.

18.3 No informar ni divulgar públicamente ninguna violación de la información, los sistemas u otros recursos de CWT sin notificar primero a CWT y trabajar directamente con CWT para notificar a los funcionarios gubernamentales regionales, nacionales, estatales o locales correspondientes o a los servicios de control de crédito, las personas afectadas por dicha violación. y cualquier medio de comunicación aplicable, según lo exija la ley.

18.4 Contar con un proceso para identificar rápidamente las violaciones de los controles de seguridad, incluidas las establecidas en estos Requisitos de seguridad de la información, por parte del personal del Proveedor o de Terceros. Los infractores identificados estarán sujetos a las medidas disciplinarias correspondientes conforme a las leyes aplicables. Sin perjuicio de lo anterior, los infractores quedarán bajo la autoridad del Vendedor o de sus Terceros. CWT no se considerará empleador del personal del Proveedor o de sus Terceros.

19. Gestión de la continuidad del negocio y recuperación ante desastres

El proveedor deberá, como mínimo:

19.1 Desarrolle, opere, administre y revise los planes de continuidad comercial para cada ubicación y los planes de recuperación ante desastres para cada tecnología central a fin de minimizar el impacto de CWT en el servicio o los productos del proveedor. Dichos planes incluirán: recursos designados específicos para las funciones de continuidad comercial y recuperación ante desastres, objetivos de tiempo de recuperación establecidos y objetivos de punto de recuperación, al menos una copia de seguridad diaria de datos y sistemas, almacenamiento externo de datos y copias de seguridad y registros de sistemas, registro planes de protección y contingencia acordes con los requisitos del Acuerdo, almacene dichos registros y planes de

forma segura fuera del sitio y asegúrese de que dichos planes estén disponibles para el Proveedor según sea necesario.

19.2 A solicitud de CWT, proporcionar a CWT un plan de continuidad comercial documentado que garantice que el Proveedor pueda cumplir con sus obligaciones contractuales en virtud del Acuerdo y este documento, incluidos los requisitos de cualquier declaración de trabajo o acuerdo de nivel de servicio aplicable. Dichos planes ejercerán la recuperación mientras protegen la integridad y confidencialidad de la Información personal y la Información confidencial.

19.3 Disponer de procedimientos documentados para la copia de seguridad y la recuperación seguras de la Información personal y la Información confidencial que incluirán, como mínimo, procedimientos para el transporte, el almacenamiento y la eliminación de las copias de seguridad de la Información personal y la Información confidencial y, a petición de CWT, proporcionar dichos procedimientos documentados a CWT.

19.4 Asegúrese de que se creen copias de seguridad de toda la información personal y la información confidencial almacenada o el software y las configuraciones de los sistemas utilizados por CWT al menos una vez a la semana.

19.5 Los planes de continuidad del negocio y recuperación ante desastres se actualizarán al menos una vez al año, o con la frecuencia que lo requieran los cambios significativos en el entorno empresarial y/o tecnológico.

19.6 Estos planes también se ejercerán de manera comprensible al menos una vez al año, o después de cualquier cambio material en los planes de continuidad del negocio o recuperación ante desastres a cargo y costo exclusivo del Proveedor. Dichos ejercicios garantizarán el funcionamiento adecuado de las tecnologías afectadas y el conocimiento interno de dichos planes.

19.7 Revise rápidamente su plan de continuidad comercial para abordar fuentes o escenarios de amenazas adicionales o emergentes y proporcione a CWT un resumen de alto nivel de los planes y las pruebas dentro de un período de tiempo razonable a pedido.

19.8 Asegúrese de que todos los proveedores o ubicaciones contratadas por proveedores que alberguen o procesen información personal e información confidencial de CWT sean monitoreados las 24 horas del día, los siete (7) días de la semana contra intrusiones, incendios, agua y otros peligros ambientales.

20. Cumplimiento y Acreditaciones

El proveedor deberá, como mínimo:

20.1 Conservar registros completos y precisos relacionados con el desempeño de sus obligaciones derivadas de estos Requisitos de seguridad de la información y el cumplimiento del Proveedor de los mismos en un formato que permita la evaluación o auditoría por un período no inferior

a tres (3) años o más, según sea necesario. de conformidad con una orden judicial o un procedimiento civil o reglamentario. Sin perjuicio de lo anterior, el Proveedor solo deberá mantener registros de seguridad durante un mínimo de un (1) año después de la ejecución continua del Acuerdo.

20.2 Permitir a CWT, sin costo adicional para CWT, con un aviso previo razonable, realizar evaluaciones de seguridad periódicas o auditorías de la Medida de seguridad técnica y organizativa utilizada por el Proveedor durante las cuales CWT proporcionará al Proveedor cuestionarios por escrito y solicitudes de documentación. Para todas las solicitudes, el Proveedor responderá con una respuesta por escrito y evidencia, si corresponde, de inmediato o de mutuo acuerdo. Ante la solicitud de CWT de una auditoría por parte de CWT, el Proveedor programará una auditoría de seguridad para que comience dentro de los diez (10) días hábiles a partir de dicha solicitud. CWT puede requerir acceso a instalaciones, sistemas, procesos o procedimientos para evaluar el entorno de control de seguridad del Proveedor.

20.3 A pedido de CWT, certificar que cumple con este documento junto con las certificaciones de respaldo para las versiones más recientes de PCI-DSS, ISO 27001/27002, SOC 2, Cyber Essentials o una evaluación similar para el Proveedor y para cualquier subcontratista o tercero. procesamiento, acceso, almacenamiento o gestión en nombre del Proveedor. Si el Proveedor no puede certificar el cumplimiento, deberá proporcionar un informe escrito que detalle dónde está fuera de cumplimiento y su plan de remediación para cumplir.

20.4 En el caso de que CWT, a su exclusivo criterio, considere que se ha producido una infracción de seguridad que no se informó a CWT de conformidad con este Acuerdo y el Proceso de gestión de incidentes del proveedor, programe la auditoría o evaluación para que comience dentro de las veinticuatro (24) horas. de la notificación de CWT que requiere una evaluación o auditoría.

20.5 Dentro de los treinta (30) días calendario posteriores a la recepción de los resultados de la evaluación o el informe de auditoría, proporcione a CWT un informe escrito que describa las acciones correctivas que el Proveedor ha implementado o propone implementar con el cronograma y el estado actual de cada acción correctiva. El Proveedor actualizará este informe a CWT cada treinta (30) días calendario informando el estado de todas las acciones correctivas hasta la fecha de implementación. El Proveedor implementará todas las acciones correctivas dentro de los noventa (90) días posteriores a la recepción del informe de evaluación o auditoría del Proveedor o dentro de un período de tiempo alternativo, siempre que las partes hayan acordado mutuamente por escrito dicho período de tiempo alternativo dentro de no más de treinta (30) días. días siguientes a la recepción por parte del Proveedor del informe de evaluación o auditoría.

20.6 Cumplimiento de PCI DSS: en la medida en que el Proveedor maneje números de cuenta de pago o cualquier otra información de pago relacionada, el Proveedor deberá cumplir actualmente con la versión más reciente de Payment Card Industry (PCI-DSS) para el alcance completo de los sistemas que manejan esta información y continuar tal cumplimiento. Si algún subcontratista o tercero está procesando, accediendo, almacenando o administrando

datos de tarjetas de crédito en nombre del Proveedor, el proveedor debe obtener un PCI AOC de dicho subcontratista o tercero y ponerlo a disposición de CWT cuando lo solicite. En caso de que el Proveedor no cumpla o ya no cumpla con PCI-DSS para cualquier parte del alcance total de los sistemas que manejan datos aplicables a PCI, el Proveedor notificará de inmediato a CWT, procederá de inmediato sin demora indebida para remediar dicho incumplimiento y proporcionará el estado regular de dicha remediación a CWT previa solicitud.

21. Estándares, Mejores Prácticas, Regulaciones y Leyes

En caso de que el Proveedor procese, acceda, visualice, almacene o administre Información personal o Información confidencial perteneciente al personal de CWT, socios, Afiliados, clientes de CWT; o empleados, contratistas, subcontratistas o proveedores de clientes de CWT; El Proveedor empleará Medidas de Seguridad Técnicas y Organizativas no menos estrictas que las requeridas por las pautas, regulaciones, directivas y leyes globales, regionales, nacionales, estatales y locales aplicables.

22. Modificación

CWT se reserva el derecho de actualizar o modificar estos Requisitos de seguridad de la información de vez en cuando mediante la publicación de la última versión en el sitio web de CWT. A menos que el Proveedor proporcione una notificación por escrito objetando dichas actualizaciones o modificaciones dentro de los treinta (30) días posteriores a la publicación, se considerará que el Proveedor las ha aceptado.

Versión 6.1
Fecha: abril de 2024