Spanish for Latin America

Requisitos de seguridad de la información del proveedor

1. Introducción

El Proveedor acuerda que su entidad y los terceros que actúen en su nombre para proporcionar servicios y productos a CWT cumplirán con los requisitos de seguridad de la información contenidos en este documento ("**Requisitos de seguridad de la información**"), los cuales establecen las medidas de seguridad de la información requeridas ("**Medidas de seguridad técnicas y de la organización**").

2. Definiciones

2.1 Salvo que se establezca algo distinto o se amplíen por la presente, los términos definidos tendrán el mismo significado que el establecido en el Acuerdo principal. Los siguientes términos definidos se aplican a estos Requisitos de seguridad de la información:

"**Afiliado**", salvo se defina de otra manera en el Acuerdo, hará referencia, respecto a una parte, a una compañía u otra entidad jurídica que: (i) controle directa o indirectamente a una parte; (ii) esté bajo el control directo o indirecto de una parte; o (iii) esté bajo el control directo o indirecto de una compañía o entidad que directa o indirectamente controle a una parte. A estos efectos, el "control" hace referencia al ejercicio de más del 50 % (cincuenta por ciento) de los votos o un derecho de titularidad similar, pero solo por el tiempo que dure dicho control.

"Acuerdo", salvo se defina de otra manera en los términos principales del acuerdo, hace referencia al contrato u otro documento legal celebrado por CWT y el Proveedor.

"Información confidencial" hace referencia a toda información sensible desde el punto de vista comercial, información patrimonial o de otra forma confidencial que se relacione con (a) CWT y sus Afiliados; (b) un cliente de CWT; (c) personal de CWT; (d) socios independientes y asociación en participación de CWT o (e) el contenido y/o el propósito del Acuerdo, ya sea oral, por escrito o que por cualquier otro medio pueda, directa o indirectamente, llegar a manos del Proveedor o del personal de un Proveedor, o del personal, representantes, contratistas o subcontratistas del Proveedor como resultado de este Acuerdo o en relación con él. A fin de evitar dudas, todo producto de trabajo constituye Información confidencial.

"CWT", salvo se defina de otra manera en el Acuerdo, hace referencia a la entidad CWT descrita en el Acuerdo, así como a sus Afiliados.

"**Red perimetral**" (o "**DMZ**", por su sigla en inglés) es una red o red secundaria que funciona entre una red interna de confianza, como la red de área local (LAN, por su sigla en inglés) privada de una compañía y una red externa que no es de confianza, como la Internet pública. Una DMZ ayuda a evitar que los usuarios externos puedan acceder directamente a los sistemas internos y a otros recursos.

"Proceso de gestión de incidentes" es un cauce procedimental debidamente documentado, desarrollado por el Proveedor, que se debe seguir en caso de ataque real o sospecha de ataque, invasión, acceso no autorizado, pérdida u otro supuesto de incumplimiento que se relacione con la confidencialidad, disponibilidad o integridad de la Información personal e Información confidencial.

"Enmascaramiento" es el proceso de cubrir la información que aparece en una pantalla.

"Dispositivos móviles y portátiles" hace referencia a las computadoras, dispositivos, medios o sistemas móviles y/o portátiles que se pueden llevar, mover, transportar o trasladar fácilmente y que se usan en relación con el Acuerdo. Entre los ejemplos de tales dispositivos se encuentran las computadoras tipo laptop, tabletas, discos duros USB, memoria extraíble USB, asistentes digitales personales (PDA, por su sigla en inglés), teléfonos móviles o de datos y cualquier otro dispositivo

periférico o inalámbrico con la capacidad de almacenar Información personal e Información confidencial.

“Información personal”, salvo se defina de otra manera en el Acuerdo, según la definición proporcionada en la Regulación 2016/679 (Unión Europea) y demás leyes vigentes sobre seguridad de la información global, protección de datos y privacidad, se hace referencia a la información relacionada con una persona natural, que puede ser identificada, directa o indirectamente, y en particular haciendo referencia a un número de identificación o a uno o más factores específicos a su identidad física, psicológica, mental, económica, cultural o social.

“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 las redes y los servidores administrativos y de gestión asociados. Entre los ejemplos de puertas de enlace de seguridad se incluyen los firewall, servidores de administración de firewall, hop boxes, controladores de borde de sesión, servidores proxy y dispositivos de prevención de intrusiones.

“Autenticación sólida” hace referencia al uso de mecanismos y metodologías de autenticación más sólidas que las contraseñas requeridas en el presente. Entre los ejemplos de mecanismos y metodologías de Autenticación sólida se incluyen los certificados digitales, autenticación en dos fases y contraseñas de un solo uso.

“Cifrado de alta seguridad” hace referencia a las tecnologías de cifrado con longitudes mínimas de claves de 256 bits para cifrado simétrico y 1024 bits para cifrado asimétrico cuya solidez proporcione una garantía razonable de protección de la información cifrada del acceso no autorizado y que incorporen una política documentada para el manejo de las claves de cifrado y los procesos asociados adecuados para proteger la confidencialidad y privacidad de las claves y contraseñas utilizadas como entradas para el algoritmo de cifrado. El cifrado de alta seguridad incluye, sin limitarse a ello: SSL v3.0+/TLS v1.0+, protocolo de túnel punto a punto (PPTP), AES 256, FIPS 140-2 (únicamente para el gobierno de Estados Unidos), RSA 1024 bits, SHA1/SHA2/SHA3, protocolo de seguridad de Internet (IPSEC), SFTP, SSH, Vormetric v4 o WPA2.

“Medidas de seguridad técnicas y de la organización” hacen referencia a las actividades requeridas en virtud de estos Requisitos de seguridad de la información a fin de acceder, manejar, transferir, procesar, almacenar, retener y destruir información o datos; divulgar y notificar a las partes afectadas requeridas conforme al acuerdo y en virtud de la legislación vigente sobre privacidad de la información y protección de los datos y proteger información o datos para asegurar la disponibilidad, integridad, confidencialidad y privacidad o notificar a las personas en el caso de imposibilidad de proteger dicha información o datos. Las medidas incluyen, entre otras, las requeridas, o las que se interpretan como requeridas, en virtud de las Directivas de la Unión Europea 94/46/CE y 2006/24/CE según se promulgaron por los países miembros, la Ley Gramm-Leach Bliley (GLBA, por su sigla en inglés) de Estados Unidos, la Ley de Portabilidad y Responsabilidad de Seguros Médicos (HIPAA, por su sigla en inglés) de Estados Unidos, los requisitos de privacidad de los datos de la UE/Suiza y cualquier otra ley internacional o estadounidense, interpretación jurídica oficial o precedente judicial relativo a la información o datos conforme al Acuerdo.

“**Tercero”**, salvo se defina de otra manera en el Acuerdo, hace referencia a los subcontratistas y a cada integrante del personal temporal, contratistas del Proveedor o proveedores adicionales y/o representantes que actúen en nombre del Proveedor, e incluye la definición de Tercero conforme a la legislación vigente en la UE, EE. UU. u otra ley internacional.

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

2.2 El Proveedor garantiza y declara que cumplirá con las siguientes Medidas de seguridad técnicas y de la organización en la medida en que sean aplicables para la prestación de los servicios establecidos en el Acuerdo:

3. Organización de la seguridad de la información

El Proveedor:

3.1 establecerá, implementará y mantendrá, en consonancia con las prácticas del sector, pero no menos que políticas razonables y un programa de Medidas de seguridad técnicas y de la organización a nivel interno, operativo, administrativo y físico para (1) prevenir los accesos a la Información personal e Información confidencial de forma no autorizada por el Acuerdo o estos Requisitos de seguridad de la información y (2) cumplir y satisfacer todas las normas correspondientes del sector. El Proveedor también se asegurará de que su personal de seguridad tenga la experiencia razonable y necesaria en seguridad de la información y de las redes.

3.2 Proporcionará un nivel adecuado de supervisión, orientación y capacitación sobre las Medidas de seguridad técnicas y de la organización al personal del Proveedor que necesite acceder a la Información personal e Información confidencial. El Proveedor también proporcionará capacitación sobre las Medidas de seguridad técnicas y de la organización al momento de la contratación y antes de acceder a la Información personal e Información confidencial. Se proporcionará capacitación de actualización al menos de forma anual y tan pronto como sea posible luego de un cambio importante en las Medidas de seguridad técnicas y de la organización.

3.3 El personal del Proveedor con tareas de seguridad significativas, que incluyan, entre otras, recursos humanos o funciones de tecnología de la información, y funciones de administrador de tecnología, también recibirán capacitación especializada específica a sus roles respectivos. La capacitación especializada incluirá, según corresponda al rol, procedimientos de seguridad de la información, uso aceptable de los recursos de seguridad de la información, amenazas actuales a los sistemas de información, funciones de seguridad de sistemas específicos y procedimientos de acceso seguro.

3.4 Tomará las medidas razonables para evitar el acceso físico o electrónico no autorizado o la pérdida de la Información personal e Información confidencial y los servicios, sistemas, dispositivos o medios que contengan esta información.

3.5 Utilizará procesos y procedimientos de evaluación de riesgos para evaluar periódicamente los sistemas usados para proporcionar los servicios o productos a CWT. El Proveedor también corregirá dichos riesgos tan pronto como sea razonablemente posible de acuerdo al nivel de riesgo establecido para las amenazas a la Información personal e Información confidencial conocidas al momento de la identificación. Pondrá en funcionamiento un proceso que permita al personal del Proveedor reportar los riesgos o incidentes sospechados al equipo de seguridad del Proveedor.

3.6 En la medida en que el Proveedor preste servicios, en virtud del Acuerdo, en las instalaciones de CWT, o usen los servicios, sistemas, dispositivos o medios que sean propiedad de CWT u operados o gestionados por CWT, el Proveedor cumplirá con todas las políticas de CWT que se pusieron a disposición del Proveedor que se aplican a dicho acceso. El Proveedor también notificará a CWT por escrito de manera oportuna cuando ya no se necesite dicho acceso, lo que incluye, sin limitarse a ello,

cuando un empleado, contratista, subcontratista o tercero del Proveedor ya no presta servicios en virtud del Acuerdo o cuando dejó de acceder a la Información personal e Información confidencial.

3.7 Cumplirá con los requisitos de verificación de antecedentes de CWT en la medida en que sea necesario y la ley lo permita y como de otro modo se establezca en una descripción del trabajo/orden de trabajo/orden de compra correspondiente.

4. Seguridad física y del entorno

El Proveedor:

4.1 Se asegurará de que los sistemas y demás recursos del Proveedor previstos para el uso de múltiples usuarios se encuentren en instalaciones físicas seguras con acceso limitado y restringido a las personas autorizadas únicamente.

4.2 Supervisará y registrará, a los efectos de una auditoría, el acceso a las instalaciones físicas que contengan los sistemas y otros recursos previstos para el uso de múltiples usuarios en relación con sus obligaciones en virtud del Acuerdo.

4.3 Se asegurará de que todo el personal del Proveedor firme un acuerdo de no divulgación o confidencialidad con el Proveedor antes de acceder a la Información personal e Información confidencial.

4.4 Exigirá que todo su personal se adhiera a una política de escritorio limpio y bloqueo de pantallas en las estaciones de trabajo antes de abandonar las áreas de trabajo.

4.5 Recolectará todos los bienes de la compañía al finalizar el empleo o contrato.

4.6 Limitará y supervisará el acceso físico a sus instalaciones de acuerdo con los siguientes requisitos:

a. El acceso de los visitantes se registra y el registro se guarda por tres (3) meses e incluye el nombre del visitante, la compañía que representa y el nombre del empleado que autoriza el acceso físico.
b. El acceso se restringe al personal apropiado de acuerdo a la necesidad de saber.
c. Todos los empleados deben usar una insignia de identificación proporcionada por la compañía.
d. El acceso se revocará de inmediato al momento de la finalización y todos los mecanismos de acceso físico, como son llaves, tarjetas de acceso, etc. se devolverán o inhabilitarán.
e. El centro de datos o sala de informática está bloqueado y el acceso se limita únicamente a quienes necesiten ingresar para desempeñar sus funciones laborales.
f. Donde esté permitido por la ley, utilizar cámaras de video para supervisar el acceso físico de las personas a las áreas sensibles y dicha información se revisa periódicamente. Las imágenes de video se almacenan por un mínimo de 3 (tres) meses.
g. El equipo usado para almacenar, procesar o transmitir Información personal e Información confidencial debe estar físicamente asegurado, lo que incluye los puntos de acceso inalámbrico, los dispositivos portátiles, el hardware de redes/comunicación y las líneas de telecomunicaciones.

4.7 Implementará controles a fin de reducir el riesgo y proteger contra las amenazas físicas.

4.8 Mantendrá el procesamiento del hardware y el manejo de la Información personal e Información confidencial de acuerdo con los requisitos de servicio técnico recomendados del proveedor de servicios.

4.9 Restringirá la sala de conferencias y otros conectores de red accesibles de forma pública lógicamente desde la red del Proveedor, la cual se restringirá únicamente a los usuarios autenticados o se deshabilitará de forma predeterminada.

4.10 Protegerá de la alteración o sustitución los dispositivos que registren datos de tarjetas de pago mediante la interacción física directa a través de la inspección periódica de las superficies del dispositivo a fin de detectar la alteración o sustitución, proporcionará capacitación para el personal a fin de tener conocimiento de los intentos de alteración o sustitución de los dispositivos.

4.11 Controlará y separará los puntos de acceso, tales como las áreas de entrega y carga y otros puntos de todos los centros que accedan, gestionen, almacenen o procesen Información personal e Información confidencial.

4.12 Debe contar con calefacción, aire acondicionado, extintores de incendios, dispositivos de detección de agua, calor y humo en los centros de datos.

5. Control del acceso

El Proveedor:

5.1 Tomará todas las medidas necesarias para evitar el acceso a la Información personal e Información confidencial en forma alguna o con un fin no autorizado por CWT y el Acuerdo. El Proveedor también limitará el acceso a la Información personal e Información confidencial al personal del Proveedor que (1) tenga la necesidad legítima de acceder a la Información personal e Información confidencial a fin de prestar servicios en virtud del Acuerdo y (2) haya acordado por escrito proteger la integridad, disponibilidad y confidencialidad de la Información personal e Información confidencial.

5.2 Mantendrá procedimientos razonables para poner fin al acceso a la Información personal e Información confidencial otorgado al personal del Proveedor cuando ya no sea necesario o relevante para el desempeño de sus funciones y antes de la finalización del empleo con el Proveedor o compromiso por parte de CWT.

5.3 Separará la información de CWT de las aplicaciones e información de otro cliente o del propio Proveedor, ya sea mediante el uso físico de servidores separados o de otra forma mediante el uso de controles de acceso lógico cuando no se implemente la separación física de los servidores.

5.4 Identificará y solicitará a los propietarios correspondientes que revisen y aprueben el acceso a los sistemas utilizados para acceder, procesar, gestionar o almacenar la Información personal e Información confidencial; y hará un seguimiento de las aprobaciones de acceso.

5.5 Eliminará el acceso a los sistemas que gestionen la Información personal e Información confidencial en un plazo de 24 horas luego de la finalización de la relación del Proveedor con un empleado, contratista, subcontratista o tercero; y eliminará el acceso a dichos sistemas en el plazo de 3 (tres) días hábiles cuando un empleado, contratista, subcontratista o tercero cambie las responsabilidades laborales dentro de la compañía. Todas las demás identificaciones de usuario serán deshabilitadas o eliminadas pasados 90 (noventa) días naturales de inactividad.

5.6 Revisará periódicamente y aprobará el acceso a los sistemas que manejen Información personal e Información confidencial al menos trimestralmente para eliminar el acceso no autorizado.

5.7 Limitará el acceso del administrador del sistema (también denominado usuario raíz, con privilegios o superusuario) o a los sistemas operativos previstos para el uso de múltiples usuarios únicamente a las personas que requieran dicho alto nivel de acceso en el desempeño de sus funciones. Utilizará identificaciones de verificación para las credenciales de inicio de sesión de los usuarios individuales y los registros de actividad a fin de administrar el acceso de alta seguridad cuando sea posible y de otra forma reducir el acceso de alto nivel a un número sumamente limitado de usuarios.

5.8 Exigirá que los administradores de sistemas, aplicaciones, bases de datos y redes restrinjan el acceso de los usuarios únicamente a los comandos, datos, sistemas y demás recursos necesarios para la realización de las funciones autorizadas.

5.9 Exigirá Autenticación sólida para el uso mediante acceso remoto.

5.10 Utilizará Medidas de seguridad técnica y de la organización a fin de garantizar que el personal del Proveedor que acceda a la Información personal e Información confidencial no puedan copiarla, trasladarla o almacenarla en discos duros ni que puedan cortar y pegar o imprimir dicha Información personal e Información confidencial. Hacerlo estará prohibido.

5.11 Activará el uso de las capacidades de acceso remoto solo cuando sea necesario, controlarlas mientras estén en uso e desactivarlas inmediatamente después de su uso.

5.12 Exigirá al menos una autenticación en dos fases para conectarse a los recursos internos del Proveedor que contengan Información personal e Información confidencial.

6. Identificación y autenticación

El Proveedor:

6.1 Asignará identificaciones de usuario exclusivas a los usuarios individuales y mecanismos de autenticación a cada cuenta individual.

6.2 Usará un proceso de administración del ciclo de vida de identificación de usuario documentado que incluya, entre otras cosas, procedimientos para la creación de cuentas aprobadas, eliminación oportuna de cuentas (p. ej., cambios en los privilegios, intervalo de acceso, funciones/roles) para todo el acceso a la Información personal e Información confidencial y en todos los entornos (p. ej., producción, prueba, desarrollo, etc.). Dicho proceso incluirá la revisión de los privilegios de acceso y la validez de la cuenta, lo que se llevará a cabo al menos de forma trimestral.

6.3 Implementará la regla de privilegios mínimos (es decir, limitará el acceso solo a los comandos, información, sistemas y otros recursos necesarios para llevar a cabo las funciones autorizadas de acuerdo con la función laboral de la persona).

6.4 Restringirá todo el acceso a la Información personal e Información confidencial a aquellos que usen una identificación de usuario y contraseña válida y exigirá que las identificaciones de usuario exclusivas empleen uno de los siguientes requisitos: contraseña o frase de contraseña, autenticación en dos fases o un valor biométrico.

6.5 Exigirá complejidad para las contraseñas y cumplirá con los siguientes requisitos de construcción de contraseñas: un mínimo de 8 (ocho) caracteres de longitud para las contraseñas del sistema y 4 (cuatro) caracteres para los códigos de acceso de tabletas y teléfonos inteligentes. Las contraseñas del sistema deben incluir 3 (tres) de los siguientes requisitos: mayúsculas, minúsculas, caracteres numéricos o especiales. Las contraseñas no deben ser iguales a la identificación de usuario a la que se

vinculan, contener una palabra de diccionario, números secuenciales o repetidos, ni ser una de las últimas cinco contraseñas. Exigirá el vencimiento de las contraseñas a intervalos periódicos que no superen los 90 (noventa) días. Enmascarará todas las contraseñas que aparezcan en pantalla.

6.6 Limitará la cantidad de intentos fallidos para iniciar sesión a no más de 5 (cinco) en un plazo de 24 horas y bloqueará la cuenta del usuario que llegue a ese límite de forma persistente. El acceso a la cuenta del usuario puede reactivarse posteriormente mediante un proceso manual que requiere la verificación de la identidad del usuario.

6.7 Verificará la identidad de los usuarios y establecerá contraseñas de restablecimiento de un solo uso para un valor único para cada usuario. Solicitará el cambio sistemáticamente después del primer uso.

6.8 Utilizará un método seguro para trasmitir credenciales de autenticación (p. ej., contraseñas) y mecanismos de autenticación (p. ej., tokens o tarjetas inteligentes).

6.9 Restringirá las contraseñas de cuenta de servicio y proxy a un mínimo de 12 caracteres que incluyan mayúsculas, minúsculas y caracteres numéricos, así como también símbolos especiales. Cambiará las contraseñas de las cuentas de servicio y proxy al menos de forma anual.

6.10 Finalizará las sesiones interactivas o activará protectores de pantalla seguros con bloqueo que requieran autenticación luego de un periodo de inactividad que no superará los 15 (quince) minutos.

6.11 Utilizará un método de autenticación basado en la sensibilidad de la información personal y la Información confidencial. Siempre que se almacenen credenciales de autenticación, el Proveedor las protegerá mediante Cifrado de alta seguridad. Requerirá la reautenticación después de 15 minutos de inactividad.

6.12 Configurará los sistemas para que expiren luego de un periodo máximo de inactividad: 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 los sistemas de información

El Proveedor:

7.1 En el caso de los productos o servicios de marca CWT o para los productos y software desarrollados para CWT, el Proveedor desplegará un cartel de advertencia en las pantallas o páginas de inicio de sesión según lo especificado por escrito por CWT.

7.2 Se asegurará de que todo el personal que realice tareas en virtud del Acuerdo cumpla con estas Medidas de seguridad técnicas y de la organización, lo cual se debe evidenciar mediante un acuerdo por escrito que no sea menos restrictivo que estos Requisitos de seguridad de la información.

7.3 Devolverá todos los dispositivos de acceso proporcionados por CWT o de su propiedad lo antes posible, pero en ningún caso pasados 15 (quince) días del primero de los siguientes:

(a) vencimiento o finalización del Acuerdo;
(b) la solicitud de CWT para la devolución de dicha propiedad;
(c) la fecha en la que el Proveedor deje de necesitar dichos dispositivos.

7.4 Empleará una metodología de administración de aplicaciones efectiva que incorpore Medidas de seguridad técnicas y de la organización en el proceso de desarrollo de software y garantizará la

implementación oportuna de las Medidas de seguridad técnicas y de la organización, según lo establecido en las políticas, normas y procedimientos de seguridad de la información o ciclo de vida de desarrollo de software de CWT.

7.5 Seguirá procedimientos estándares de desarrollo, incluida la separación del acceso y código entre los entornos de producción y los que no son de producción y la segregación asociada de tareas entre dichos entornos.

7.6 Garantizará que los controles de seguridad de la información interna para el desarrollo de software se evalúen periódicamente y reflejen las mejores prácticas del sector y revisará e implementará estos controles de manera oportuna.

7.7 Gestionará la seguridad del proceso de desarrollo y garantizará la implementación y seguimiento de prácticas de codificación seguras, lo que incluye controles criptográficos, protecciones contra códigos maliciosos y un proceso de evaluación por igual.

7.8 Realizará pruebas de penetración en aplicaciones de funcionalidad completa, antes de pasar a la producción y subsiguientemente, al menos una vez al año y luego de modificaciones importantes al código fuente o la configuración que se alinee con OWASP, CERT, SANS Top 25, y PCI-DSS. Solucionará las vulnerabilidades que puedan ser explotadas previo al lanzamiento del entorno de producción.

7.9 Utilizará datos anónimos o confusos en entornos que no sean de producción. Nunca utilizará datos de producción de texto sin formato en un entorno que no sea de producción y nunca utilizará Información personal e Información confidencial en entornos que no sean de producción, por ningún motivo. Se asegurará de que todos los datos y cuentas de prueba se eliminen antes del lanzamiento a producción.

7.10 Se asegurará de que el Proveedor que use códigos fuente libres, software, aplicaciones o servicios mantengan la debida diligencia en la revisión de dichos códigos en busca de fallas, errores o problemas de seguridad que puedan afectar a la integridad, disponibilidad o confidencialidad de los datos de CWT o los clientes de CWT. El Proveedor también notificará a CWT cuando utilice códigos de acceso abierto y proporcionará a CWT el nombre y la versión del código de acceso abierto.

7.11 Se asegurará de que, bajo ninguna circunstancia, el Proveedor comparta un código creado en virtud del Acuerdo, independientemente de la etapa de desarrollo, en un entorno compartido o que no sea privado, tal como un repositorio de códigos de acceso abierto, sin perjuicio de la protección con contraseña.

8. Integridad del software y los datos

El Proveedor:

8.1 En los entornos en los que haya software antivirus comercialmente disponible, instalará software antivirus actualizado y ejecutará escaneos de detección para eliminar y poner en cuarentena a virus y otros malwares de cualquier sistema o dispositivo.

8.2 Separará la información y los recursos que no sean de producción de la información y los recursos que sean de producción.

8.3 Se asegurará de que los equipos utilicen un proceso de control de cambios documentado, lo que incluye procedimientos de salida para todos los entornos de producción y procesos de cambios de emergencia. Incluirá pruebas, documentación y aprobaciones para todos los cambios del sistema y exigirá aprobación de administración para los cambios importantes en dichos procesos.

8.4 Creará y mantendrá una zona PCI (sigla en inglés para industria de las tarjetas de pago) si el Proveedor procesa o almacena datos de titulares de tarjetas.

8.5 Para las aplicaciones que utilicen bases de datos que permitan modificaciones de la Información personal e Información confidencial, habilitará y mantendrá funciones de registro de auditoría de transacciones de bases de datos y retendrá los registros de auditoría de transacciones de bases de datos por un mínimo de 6 (seis) meses.

8.6 Revisará el software a fin de encontrar y solucionar vulnerabilidades de seguridad durante la implementación inicial y al realizar modificaciones o actualizaciones significativas.

8.7 Llevará a cabo 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 o al realizar modificaciones o actualizaciones significativas.

9. Seguridad del sistema

El Proveedor:

9.1 Creará y actualizará periódicamente las versiones más recientes de los diagramas de flujos de datos y sistemas utilizados para acceder, procesar, administrar o almacenar la Información personal e Información confidencial.

9.2 Supervisará activamente los recursos del sector (p. ej.,, www.cert.org y los sitios web y listas de direcciones pertinentes del proveedor de software) para la notificación oportuna de todas las alertas de seguridad correspondientes que pertenezcan a los sistemas del Proveedor y otros recursos de información.

9.3 Manejará con eficacia las claves criptográficas al reducir el acceso a las claves por parte del menor número posible de administradores necesarios, almacenar claves criptográficas secretas y privadas al cifrar con una clave al menos tan sólida como la clave de cifrado de datos y almacenarla de forma separada de la clave de cifrado de datos en un dispositivo criptográfico seguro, en la menor cantidad de ubicaciones posibles. Cambiará las claves criptográficas predeterminadas al momento de la instalación y al menos cada dos años y eliminará de forma segura las claves antiguas.

9.4 Realizará un escaneo de los sistemas externos y demás recursos de información, lo que incluye, entre otras cosas, redes, servidores y aplicaciones, con software de escaneo de detección de vulnerabilidad de la seguridad estándar en el sector para descubrir vulnerabilidades de seguridad al menos de forma trimestral y antes del lanzamiento para las aplicaciones y para los cambios significativos y las actualizaciones en los plazos que resulten de los análisis de riesgo sobre la base de las políticas y normas de TI razonables y generalmente aceptadas.

9.5 Realizará un escaneo de los sistemas internos y demás recursos de información, lo que incluye, entre otras cosas, redes, servidores, aplicaciones y bases de datos, con software de escaneo de detección de vulnerabilidades de seguridad estándar en el sector para descubrir vulnerabilidades de seguridad, asegurar que dichos sistemas y demás recursos estén debidamente protegidos e identificar cualquier red inalámbrica no autorizada al menos de forma trimestral y antes del lanzamiento para las aplicaciones y para los cambios significativos y las actualizaciones en los plazos que resulten de los análisis de riesgo sobre la base de las políticas y normas de TI razonables y generalmente aceptadas.

9.6 Mantendrá un proceso de calificación de riesgos para las conclusiones de la evaluación de vulnerabilidad basado en las mejores prácticas de la industria y el impacto potencial. Todas las conclusiones de evaluación con una calificación CVSS de 4 o superior deben abordarse a través de un método formalizado para garantizar que se gestione la continuidad de la evaluación de riesgos.

9.7 Garantizará que todos los sistemas y demás recursos del Proveedor estén y permanezcan "protegidos", lo que incluye, entre otras cosas, retirar o deshabilitar redes no utilizadas y otros servicios y productos (p. ej., productos y servicios finger, rlogin, ftp y de protocolo de control de trasmisión/protocolo de Internet (TCP/IP, por sus siglas en inglés) simples) e instalar un firewall del sistema, contenedores del protocolo de control de transmisión (TCP, por su sigla en inglés) o una tecnología similar.

9.8 Desplegará uno o más sistemas de detección de intrusiones (IDS, por su sigla en inglés), sistemas de prevención de intrusiones (IPS, por su sigla en inglés) o sistemas de detección y prevención de intrusiones (IDP, por su sigla en inglés) en un modo de operación activo que controle todo el tráfico que entra y sale de los sistemas y demás recursos junto con el Acuerdo, en los entornos donde dicha tecnología esté disponible comercialmente y en la medida de lo posible.

9.9 Mantendrá un proceso de calificación de riesgos para solucionar las vulnerabilidades de seguridad en un sistema u otro recurso, lo que incluye, entre otras cosas, las descubiertas a través de publicaciones del sector, un escaneo de detección de vulnerabilidades, un escaneo de detección de virus y la revisión de los registros de seguridad y aplicará revisiones de seguridad apropiadas de forma inmediata con respecto a la probabilidad de que dicha vulnerabilidad pueda o esté en proceso de ser explotada. Las revisiones críticas con una calificación CVSS de 7.5 o superior deben instalarse de inmediato cuando estén disponibles y en ningún caso con posterioridad a un mes a partir de su lanzamiento. Las revisiones con una calificación CVSS de 4 o superior deben instalarse en el plazo de 90 días a partir del lanzamiento.

9.10 Llevará a cabo una prueba de penetración generalizada a nivel interno y externo al menos de forma anual y luego de una modificación o actualización importante de infraestructura o una aplicación.

9.11 Retirará o deshabilitará software descubierto en los sistemas del Proveedor y empleará controles de malware estándar del sector, incluida la instalación, actualización regular y uso periódico de productos de software contra el malware en todos los servicios, sistemas y dispositivos que pueden utilizarse para acceder a la Información personal e Información confidencial. Usará software antivirus fiable que sea la mejor práctica del sector cuando sea viable y se asegurará de que las definiciones de virus permanezcan actualizadas.

9.12 Mantendrá software actualizado en todos los servicios, sistemas y dispositivos que puedan utilizarse para acceder a la Información personal e Información confidencial, incluido el mantenimiento adecuado de los sistemas operativos y la instalación correcta de revisiones de seguridad razonablemente actualizadas.

9.13 Asignará responsabilidades de administración de seguridad para configurar los sistemas operativos host para personas específicas.

9.14 Cambiará todos los nombres de cuentas predeterminados y/o las contraseñas predeterminadas.

10. Supervisión

El Proveedor:

10.1 Retendrá los datos de registro para la Información personal e Información confidencial por al menos 12 meses y se asegurará de que dichos datos estén disponibles para CWT en un lapso razonable y previa solicitud, salvo lo especificado en otra sección del Acuerdo.

10.2 Registrará las actividades del sistema primario para los sistemas que contengan Información personal e Información confidencial.

10.3 Restringirá el acceso a los registros de seguridad a las personas autorizadas y protegerá los registros de seguridad de las modificaciones no autorizadas.

10.4 Implementará un mecanismo de detección de cambios (p. ej., control de la integridad de los archivos) a fin de alertar al personal de las modificaciones no autorizadas de los archivos críticos del sistema, los archivos de configuración o los archivos de contenido; configurará el software para que realice comparaciones de los archivos críticos de forma semanal.

10.5 Revisará, al menos semanalmente, todos los registros de seguridad y relacionados con la seguridad en los sistemas que contengan Información personal e Información confidencial en busca de errores y documentará y revisará todos los problemas de seguridad registrados de manera oportuna.

10.6 Revisará diariamente todos los eventos de seguridad, los registros de los componentes del sistema que almacenen, procesen o transmitan datos de titulares de tarjetas, registros de componentes críticos del sistema y registros de servidores y componentes del sistema que realicen funciones de seguridad sobre una base diaria.

11. Puertas de enlace de seguridad

El Proveedor:

11.1 Requerirá Autenticación sólida para el acceso administrativo y/o de gestión a las Puertas de enlace de seguridad, lo que incluye, entre otras cosas, el acceso a los efectos de revisar los archivos de registro.

11.2 Tendrá y usará controles documentados, políticas, procesos y procedimientos documentados para asegurar que los usuarios no autorizados no tengan acceso administrativo y/o de gestión a las Puertas de enlace de seguridad y que los niveles de autorización del usuario para administrar y gestionar las Puertas de enlace de seguridad sean apropiados.

11.3 Al menos una vez semestralmente, se asegurará de que las configuraciones de las Puertas de enlace de seguridad estén protegidas mediante la selección de Puertas de enlace de muestra y la verificación de que cada conjunto de reglas predeterminadas y de parámetros de configuración garantice lo siguiente:

a. El enrutamiento fuente del protocolo de Internet (IP) está deshabilitado.
b. La dirección de bucle invertido tiene prohibido ingresar en la red interna.
   Los filtros antisuplantación están implementados.
d. Los paquetes de difusión no tienen permitido ingresar a la red.
e. Los redireccionamientos del protocolo de mensajes de control de Internet (ICMP, por su sigla en inglés) están deshabilitados.
f. Todos los conjuntos de reglas finalizan con la declaración “DENY ALL” (denegar todo).
g. Cada regla se puede rastrear hasta una solicitud comercial específica.

11.4 Se asegurará de que se usen todas las herramientas de control para validar que todos los aspectos de las Puertas de enlace de seguridad (p. ej., hardware, firmware y software) estén continuamente en funcionamiento.

Se asegurará de que todas las Puertas de enlace de seguridad estén configuradas e implementadas de forma de que todas las Puertas de enlace no operacionales denieguen todo acceso.

11.5 Se asegurará de que todos los paquetes entrantes de la red externa que no son de confianza deben terminar dentro de la "Red perimetral" (o "**DMZ**", por su sigla en inglés) y no se debe permitir su ingreso directo a la red interna de confianza. Todos los paquetes entrantes que pasan a la red interna de confianza deben originarse únicamente dentro de la DMZ. La DMZ debe separarse de la red externa que no es de confianza mediante el uso de una puerta de enlace de seguridad, y de la red interna de confianza mediante el uso de uno de los siguientes procedimientos:

a. otra puerta de enlace de seguridad;
b. la misma puerta de enlace de seguridad que se usa para separar la DMZ de la red externa que no es de confianza, en cuyo caso la puerta de enlace de seguridad debe garantizar que los paquetes que se reciban de la red externa que no es de confianza se eliminen inmediatamente o, si no se eliminan, se dirijan únicamente a la DMZ sin más procesamiento de dichos paquetes entrantes que no sea la posibilidad de ingresar los paquetes en un registro.

Los siguientes elementos deben encontrarse únicamente dentro de la red interna de confianza:

a. Toda Información personal e Información confidencial almacenadas sin el uso de cifrado de alta seguridad,
b. La copia del registro oficial con la información a acceder a partir de solicitudes generadas en la red externa que no es de confianza,
c. La copia del registro oficial de información a ser modificada como resultado de solicitudes generadas en la red externa que no es de confianza,
d. Servidores de bases de datos,
e. Todos los registros exportados, y
f. Todos los entornos utilizados para el desarrollo, prueba, espacio aislado, producción y cualquier otro entorno de este tipo y todas las versiones de códigos fuente.

11.6 Las credenciales de autenticación no protegidas por el uso de cifrado de alta seguridad no deben encontrarse dentro de la DMZ.

12. Seguridad de la red

El Proveedor:

12.1 Previa solicitud de CWT, proporcionará a CWT un diagrama lógico de la red que documente los sistemas y conexiones a otros recursos, lo que incluye enrutadores, interruptores, firewalls, sistemas IDS, topología de red, puntos de conexión externa, redes inalámbricas y cualquier otro dispositivo de respaldo de CWT.

12.2 Mantendrá un proceso formal para aprobar, probar y documentar todas las conexiones de red y cambios a las configuraciones del firewall y enrutador. Configurará firewalls para denegar y registrar paquetes sospechosos y se limitará a permitir únicamente el tráfico apropiado y autorizado, denegando todo otro tráfico a través del firewall. Revisará las reglas de firewall cada seis meses.

12.3 Instalará un firewall en cada conexión a Internet y entre una red perimetral (DMZ) y la zona de red interna. Cualquier sistema que almacene Información personal e Información confidencial debe residir en la zona de red interna, segregado de la DMZ y otras redes que no son de confianza.

12.4 Controlará el firewall en el perímetro y a nivel interno para controlar y proteger el flujo de tráfico de la red que entre o salga del límite, según sea necesario.

12.5 Mantendrá un proceso y controles documentados implementados para detectar y manejar los intentos no autorizados para acceder a la Información personal e Información confidencial.

12.6 Cuando se proporcionen productos y servicios basados en Internet a CWT, protegerá la Información personal e Información confidencial mediante la implementación de una DMZ de red. Los servidores web que proporcionan servicio a CWT residirán en la DMZ. Cualquier sistema o recurso de información que almacene Información personal e Información confidencial (tal como los servidores de aplicaciones y bases de datos) residirá en una red interna de confianza. (Los servicios y productos de Internet deben usar DMZ).

12.7 Restringirá el tráfico de salida no autorizado de las aplicaciones que procesen, almacenen o transmitan Información personal e Información confidencial a las direcciones IP dentro de la DMZ e Internet.

12.8 Cuando utilice tecnologías de redes inalámbricas de radiofrecuencia (RF) para realizar servicios o productos o brindarles asistencia técnica para CWT, se asegurará de que toda la Información personal e Información confidencial que se transmita esté protegida mediante el uso de tecnologías de cifrado de alta seguridad apropiadas. Realizará escaneos, identificará y deshabilitará puntos de acceso inalámbrico no autorizados.

13. Requisitos de conectividad

El Proveedor:

13.1 En el caso de que el Proveedor tenga o se le proporcione conectividad a los recursos de Información personal e Información confidencial junto con el Acuerdo, el Proveedor:

a. Utilizará únicamente las instalaciones y metodologías de conexión mutuamente acordadas para interconectar los recursos de Información personal e Información confidencial con los recursos de información del Proveedor.
b. No establecerá una interconexión a los recursos de Información personal e Información confidencial de CWT sin el consentimiento previo de CWT.
c. Proporcionará acceso a CWT a las instalaciones de Proveedor correspondientes durante el horario comercial habitual para el mantenimiento y asistencia técnica de equipos (p. ej., enrutadores) proporcionados por CWT en virtud del Acuerdo para la conectividad de los recursos de Información personal e Información confidencial de CWT.
d. Utilizará todo equipo proporcionado por CWT en virtud del Acuerdo para la conectividad de los recursos de Información personal e Información confidencial solo para la prestación de dichos servicios y productos o funciones explícitamente autorizados en el Acuerdo.
e. Si la metodología de conectividad mutuamente acordada requiere que el Proveedor implemente una Puerta de enlace de seguridad, mantendrá registros de todas las sesiones que usen dicha Puerta de enlace de seguridad. Estos registros de sesión deberán incluir información suficientemente detallada para identificar el usuario final o la aplicación, la dirección IP de origen, la dirección IP de destino, los protocolos de puertos/servicio y la duración del acceso. Estos registros de sesión deben retenerse por un mínimo de 6 (seis) meses a partir de la creación de la sesión.

13.2 En el caso de que el Proveedor tenga o se le proporcione conectividad a los recursos de Información personal e Información confidencial junto con el Acuerdo, además de los otros derechos establecidos en el presente, permitirá a CWT:

a. Reunir información relativa al acceso, incluido el acceso del Proveedor, a los recursos de Información personal e Información confidencial. CWT podrá recolectar, retener y analizar esta información a fin de identificar los posibles riesgos de seguridad sin previo aviso. Esta información puede incluir archivos de rastreo, estadísticas, direcciones de red y los datos o pantallas reales a los que se accedieron o fueron transferidos.
b. Suspender o cancelar Inmediatamente la interconexión a los recursos de Información personal e Información confidencial si CWT, a su sola discreción, cree que hubo una violación a la seguridad o un acceso no autorizado o uso indebido de las instalaciones de información, sistemas u otros recursos de CWT.

14. Dispositivos móviles y portátiles

El Proveedor:

14.1 Utilizará Cifrado de alta seguridad para proteger toda la Información personal e Información confidencial almacenada en Dispositivos móviles y portátiles.

14.2 No almacenará Información personal e Información confidencial en dispositivos móviles o computadoras portátiles y no almacenará Información personal e Información confidencial en dispositivos extraíbles a menos que utilice Cifrado de alta seguridad.

14.3 Usará Cifrado de alta seguridad para proteger la Información personal e Información confidencial transmitida usando dispositivos móviles y portátiles o a la que se haya accedido de forma remota a través de estos dispositivos con conexión a red.

a. Cuando use dispositivos móviles y portátiles con conexión a red que no sean computadoras portátiles para acceder y almacenar Información personal e Información confidencial, dichos dispositivos deben ser capaces de eliminar la totalidad de las copias almacenadas de la Información personal e Información confidencial al recibir a través de la red un comando debidamente autenticado. (Importante: A menudo se hace referencia a dicha capacidad como “borrado remoto”).
b. Tendrá implementadas políticas, procedimientos y normas documentadas para garantizar que la persona autorizada que debe tener el control físico de un dispositivo móvil o portátil con conexión a red que no es una computadora portátil y que almacene Información personal e Información confidencial inicie de inmediato la eliminación de toda la Información personal e Información confidencial en caso de pérdida o robo del dispositivo.
c. Tendrá implementadas políticas, procedimientos y normas documentadas para garantizar que los dispositivos móviles y portátiles que no sean computadoras laptop y no tengan conexión de red eliminen automáticamente todas las copias almacenadas de la Información personal e Información confidencial después de intentos consecutivos de inicio de sesión fallidos.

14.4 Tendrá implementadas políticas, procedimientos y normas documentadas que aseguren que los dispositivos móviles y portátiles usados para acceder y/o almacenar Información personal e Información confidencial:

a. Estén en posesión física de personas autorizadas.
b. Estén físicamente protegidos cuando no estén en posesión física de personas autorizadas.

c. Puedan eliminar de forma rápida y segura el almacenamiento de datos cuando no estén en posesión física de personas autorizadas ni estén protegidos físicamente luego de 10 intentos de acceso fallidos.

14.5 Antes de permitir el acceso a la Información personal e Información confidencial almacenada en o a través del uso de los dispositivos móviles y portátiles, el Proveedor tendrá y utilizará un proceso para garantizar que:

a. El usuario tenga autorización para dicho acceso.
b. La identidad del usuario haya sido autenticada.

14.6 Implementará una política que prohíba el uso de dispositivos móviles y portátiles que no sean administrados y/o gestionados por el Proveedor o CWT para acceder y/o almacenar Información personal e Información confidencial.

14.7 Revisará, al menos de forma anual, el uso y los controles de todos los dispositivos móviles y portátiles administrados o gestionados por el Proveedor a fin de garantizar que estos dispositivos puedan cumplir con las Medidas de seguridad técnicas y de organización vigentes.

15. Seguridad en tránsito

El Proveedor:

15.1 Usará Cifrado de alta seguridad para la transferencia de la Información personal e Información confidencial fuera de las redes controladas por CWT o el Proveedor al transmitir Información personal e Información confidencial a través de una red que no sea de confianza.

15.2 Para los registros que contengan Información personal e Información confidencial en papel, microficha o medios electrónicos que se deban transferir de forma física deben transportarse mediante mensajería segura u otro medio de entrega que pueda rastrearse, embalarse de forma segura y de acuerdo con las especificaciones del fabricante. La Información personal e Información confidencial deben trasladarse en contenedores con bloqueo.

16. Seguridad de almacenamiento

El Proveedor:

16.1 Utilizará Cifrado de alta seguridad para proteger la Información personal e Información confidencial cuando se encuentren almacenados.

16.2 No almacenará Información personal e Información confidencial de forma electrónica fuera de su entorno de red (o la propia red informática segura de CWT) a menos que el dispositivo de almacenamiento (p. ej., grabación de respaldo, laptop, memoria extraíble, disco de computadora, etc.) esté protegido por Cifrado de alta seguridad.

16.3 No almacenará Información personal e Información confidencial en medios extraíbles (p. ej., unidad flash USB, thumb drive, memoria extraíble, cintas, CD o discos duros externos) excepto: (a) con fines de respaldo, continuidad, recuperación en casos de desastre e intercambio de datos, según lo permitido y requerido en virtud del contrato y (b) utilizando Cifrado de alta seguridad.

16.4 Almacenará y protegerá apropiadamente los registros que contengan Información personal e Información confidencial en formato impreso o microficha en las áreas donde el acceso se limite solo al personal autorizado.

16.5 A menos que CWT indique otra cosa por escrito, al recopilar, generar o crear Información personal e Información confidencial en formato impreso y medios de respaldo para, a través o en nombre de CWT o bajo la marca CWT, el Proveedor se asegurará de que dicha información sea Información personal e Información confidencial y, siempre que sea viable, etiquetará dicha información de CWT como "confidencial". El Proveedor acepta que la Información personal e Información confidencial seguirá siendo propiedad de CWT independientemente de si tiene el etiquetado o no.

17. Devolución, destrucción y desechado

El Proveedor:

17.1 Previa solicitud de CWT y sin cargo adicional alguno, el Proveedor proporcionará a CWT copias de la Información personal e Información confidencial en el plazo de treinta (30) días a partir de la solicitud. El Proveedor también devolverá o, según elija CWT, destruirá toda la Información personal e Información confidencial, incluidas las copias electrónicas o impresas según se disponga en el Acuerdo, o si no se dispone en el Acuerdo, dentro del plazo de noventa (90) días a partir de lo que ocurra primero: (a) el vencimiento o cancelación del Acuerdo, (b) la solicitud de CWT para la devolución de la Información personal e Información confidencial, o (c) la fecha en que el Proveedor ya no necesite la Información personal e Información confidencial para realizar los servicios o productos en virtud del Acuerdo.

17.2 En caso de que CWT apruebe la destrucción como alternativa a la devolución de la Información personal e Información confidencial, el Proveedor certificará por escrito que la destrucción dejará la Información personal e Información confidencial como irrecuperable. Destruirá totalmente todas las copias de la Información personal e Información confidencial de CWT en todas las ubicaciones y en todos los sistemas donde se almacene Información personal e Información confidencial, lo que incluye, entre otras cosas, Terceros del Proveedor previamente aprobados. Dicha información se destruirá siguiendo un procedimiento estándar del sector para la destrucción completa, tal como DOD 5220.22M o la Publicación especial de NIST 800-88 o usando un producto de desmagnetización recomendado por el fabricante para el sistema afectado. Antes de dicha destrucción, mantendrá todas las Medidas de seguridad técnicas y de la organización correspondientes a fin de proteger la seguridad, privacidad y confidencialidad de la Información personal e Información confidencial.

17.3 Desechará la Información personal e Información confidencial de una forma que asegure que dicha información no pueda ser reconstruida en un formato utilizable. Los papeles, diapositivas, microfilms, microfichas y fotografías deberán desecharse mediante trituradora o fuego. Los materiales que contengan Información personal e Información confidencial en espera de su destrucción deben almacenarse en contenedores seguros y transportarse a través de un tercero seguro.

18. Retención

El Proveedor:

18.1 Validará los requisitos de retención apropiados con los contactos de CWT antes de adquirir la Información personal e Información confidencial y de forma coherente con una descripción del trabajo u orden de compra.

18.2 Protegerá las copias de respaldo de la Información personal e Información confidencial creadas automáticamente por los servicios, sistemas, dispositivos o medios del Proveedor ("**Copias de archivo**"). Salvo se disponga lo contrario en el Acuerdo, en el plazo de 90 días calendario a partir del vencimiento o cancelación del Acuerdo o con anterioridad si CWT lo solicita de forma razonable, destruirá de forma segura todas las Copias de archivo de la Información personal e Información confidencial, siguiendo un procedimiento estándar del sector al menos tan restrictivo como DOD 5220.22M o la Publicación especial de NIST 800-88.

19. Respuesta y notificación en caso de incidentes

El Proveedor:

19.1 Tendrá y utilizará un Proceso de manejo de incidentes y procedimientos y personal relacionados, tales como procesos y procedimientos de manejo de incidentes con recursos especializados. Inmediatamente, y en ningún caso después de 24 (veinticuatro) horas, notificará a CWT en caso de ataque confirmado o sospechado, intrusión, acceso no autorizado, pérdida u otro incidente relacionado con la información, sistemas u otros recursos de CWT.

19.2 Luego de notificar a CWT, le proporcionará actualizaciones regulares, lo que incluye, entre otras cosas, las medidas tomadas para resolver el incidente, a intervalos o en plazos mutuamente acordados, por la duración del incidente y tan pronto como sea razonablemente posible después del cierre del incidente, proporcionará a CWT un informe escrito que describa el incidente, las medidas tomadas por el Proveedor durante la respuesta y sus planes para las medidas futuras a fin de evitar incidentes similares.

19.3 No divulgará públicamente la violación de la información de CWT, los sistemas u otros recursos sin notificar primero a CWT y trabajar directamente con CWT para notificar a los organismos gubernamentales locales, estatales, nacionales o regionales correspondientes o a los servicios de control de crédito, a las personas afectadas por la violación y a los medios de comunicación correspondientes, según lo exija la ley.

a. Habrá implementado un proceso para identificar rápidamente las violaciones a los controles de seguridad, incluidos los establecidos en estos Requisitos de seguridad de la información con el personal del Proveedor. El personal del Proveedor debidamente identificado estará sujeto a las medidas disciplinarias apropiadas en virtud de la legislación vigente. Sin perjuicio de lo anterior, el personal del Proveedor permanecerá bajo la autoridad del Proveedor. CWT no se considerará empleador del personal del Proveedor.

20. Gestión de la continuidad comercial y recuperación en casos de desastre

El Proveedor:

20.1 Desarrollará, operará, gestionará y revisará los planes de continuidad comercial y recuperación en casos de desastre para los servicios o productos del Proveedor a fin de minimizar el impacto para CWT. Dichos planes incluirán: recursos designados específicos para las funciones de continuidad comercial y recuperación en casos de desastre, objetivos de plazos establecidos para la recuperación y objetivos de puntos de recuperación, respaldo diario de datos y sistemas, almacenamiento fuera del sitio de los registros y medios de respaldo, planes de protección de los registros y contingencia relacionados con los requisitos del Acuerdo; almacenará dichos planes de forma segura fuera del sitio y garantizará que estén disponibles para el Proveedor cuando los necesite.

20.2 Previa solicitud de CWT, proporcionará a CWT un plan de continuidad comercial documentado que asegure que el Proveedor puede cumplir con sus obligaciones contractuales en virtud del Acuerdo, incluidos los requisitos de una descripción del trabajo o acuerdo de nivel de servicio aplicable. Dichos planes llevarán a cabo la recuperación mientras se protege la integridad y confidencialidad de la Información personal e Información confidencial.

20.3 Tendrá procedimientos documentados para el respaldo y recuperación seguros de la Información personal e Información confidencial que incluirán, como mínimo, procedimientos para el transporte, almacenamiento y desechado de las copias de respaldo de la Información personal e Información confidencial y, previa solicitud de CWT, entregará dichos procedimientos documentados a CWT.

20.4 Se asegurará de que los respaldos de toda la Información personal e Información confidencial almacenada o del software o configuraciones para los sistemas utilizados por CWT se creen al menos semanalmente.

20.5 De forma periódica, como mínimo anualmente, o con posterioridad a un cambio significativo en los planes de continuidad comercial o recuperación en casos de desastre, llevará a cabo dichos planes de forma integral por cuenta y cargo del Proveedor. Esto asegurará el funcionamiento adecuado de las tecnologías impactadas y el conocimiento interno de dichos planes.

20.6 Revisará de inmediato su plan de continuidad comercial para abordar las fuentes o situaciones de amenaza adicionales o emergentes y proporcionará a CWT un resumen de alto nivel de los planes y pruebas dentro de un plazo razonable, previa solicitud.

20.7 Se asegurará de que todas las ubicaciones del Proveedor o contratadas por el Proveedor que alojen o procesen Información personal e Información confidencial estén controladas las 24 horas del día, todos los días de la semana contra intrusiones, incendio, inundación y demás riesgos ambientales.

21. Cumplimiento y acreditaciones

El Proveedor:

21.1 Retendrá registros completos y precisos relativos al desempeño de sus obligaciones derivadas de estos Requisitos de seguridad de la información y el cumplimiento de estos por parte del Proveedor en un formato que permitirá la evaluación o auditoría por un período de no menos de 3 (tres) años, o más, según se requiera en virtud de una orden judicial o un procedimiento civil o normativo. Sin perjuicio de lo anterior, el Proveedor solo deberá mantener registros de seguridad por un mínimo de 6 (seis) meses luego del ejercicio continuado de este acuerdo.

21.2 CWT podrá, sin costo adicional alguno, y previa notificación con anticipación razonable, realizar evaluaciones o auditorías periódicas de las Medidas de seguridad técnicas y de la organización utilizadas por el Proveedor, durante las que proporcionará al Proveedor cuestionarios escritos y solicitudes de documentación. En el caso de todas las solicitudes, el Proveedor también responderá por escrito y con evidencia, si correspondiera, de forma inmediata o cuando lo acuerden mutuamente. Previa solicitud de auditoría por parte de CWT, el Proveedor coordinará una auditoría de seguridad que comenzará en el plazo de 10 (diez) días hábiles a partir de la solicitud. CWT puede requerir el acceso a las instalaciones, sistemas, procesos o procedimientos a fin de evaluar el entorno de control de la seguridad del Proveedor.

21.3 A solicitud de CWT, el Proveedor certificará que cumple con este documento junto con las certificaciones comprobantes para las versiones más recientes de PCI-DSS, ISO 27001/27002, SOC 2 o evaluaciones similares para el Proveedor. Si el Proveedor no puede certificar el cumplimiento, deberá

proporcionar un informe por escrito que detalle dónde está en incumplimiento y su plan de subsanación para poder estar en cumplimiento.

21.4 En caso de que CWT, a su entera discreción, considere que ha ocurrido una violación a la seguridad que no se ha denunciado a CWT de acuerdo con este documento y el Proceso de manejo de incidentes del Proveedor, el Proveedor coordinará que la auditoría o evaluación comience dentro del plazo de veinticuatro (24) horas de la solicitud de CWT para la realización de una evaluación o auditoría.

21.5 Dentro del plazo de 30 (treinta) días calendario posteriores a la recepción de los resultados de la evaluación o el informe de auditoría, el Proveedor proporcionará a CWT un informe por escrito que describa las medidas correctivas que haya implementado o proponga implementar junto con el cronograma y el estado actual de cada medida correctiva. Actualizará el informe para CWT cada 30 (treinta) días calendario respecto al estado de todas las medidas correctivas hasta la fecha de implementación. Implementará todas las medidas correctivas dentro de los 90 (noventa) días posteriores a la recepción del informe de evaluación o auditoría por parte del Proveedor o en el plazo de un período alternativo siempre que dicho periodo se haya acordado mutuamente por escrito por las partes en el plazo de no más de 30 (treinta) días a partir de la recepción del informe de evaluación o auditoría por parte del Proveedor.

21.6 Cumplirá, y seguirá cumpliendo, con los estándares de seguridad de la información gubernamentales y los requisitos de información vigentes y con ISO 27001/27002. En la medida en que el Proveedor maneje números de cuenta de pago u otra información de pago relacionada, el Proveedor cumplirá con la versión más reciente del Sector de tarjetas de pago (PCI-DSS) para el alcance total de los sistemas que manejen esta información y continuará en cumplimiento. En caso de que el Proveedor deje de cumplir con PCI-DSS en alguna parte del alcance total de los sistemas que manejan datos correspondientes de PCI, el Proveedor notificará de inmediato a CWT y procederá sin demora a remediar el incumplimiento y proporcionará una actualización periódica del estado de dicho remedio a solicitud de CWT.

22. Estándares, mejores prácticas, reglamentaciones y leyes

El Proveedor:

En caso de que el Proveedor procese, acceda, vea, almacene o maneje Información personal e Información confidencial relacionados con el personal, socios, Afiliados de CWT, clientes de CWT o empleados, contratistas o subcontratistas del cliente de CWT, el Proveedor empleará Medidas de seguridad técnicas y de la organización tan estrictas como se exija en las pautas, reglamentaciones, directivas y legislación local, estatal, nacional, regional o global vigentes.

23. Modificación

CWT se reserva el derecho a modificar estos Requisitos de seguridad de la información de tanto en tanto al publicar la última versión en el sitio web de CWT.

Versión 2.0

Fecha: 15 de Diciembre de 2017