Sección 1: Objeto

Este Estándar de Seguridad de la Información (o "Estándar") establece los requisitos de seguridad de la información de Eli Lilly and Company y sus Afiliados ("Lilly") para terceros/proveedores (cada uno, un "Tercero/Proveedor") con respecto a la confidencialidad, integridad y disponibilidad de la Información (definida a continuación). Cualquier obligación adicional de Terceros/Proveedores relacionada con la seguridad de la información en virtud de cualquier acuerdo con Lilly se suma a los requisitos de este Estándar de Seguridad de la Información.

Para mayor claridad, este Estándar de Seguridad de la Información se aplica a toda la Información manejada por un Tercero/Proveedor, incluido el manejo mediante: (i) creación; (ii) edición; (iii) gestión; (iv) procesamiento; (v) acceso; (vi) recibir; (vii) transferencia; (viii) destruir; (ix) almacenamiento; o (x) alojamiento, en cualquier formato, incluidos, entre otros: (a) sistemas; b) entornos en la nube; c) entornos de producción y no producción; (d) activos y dispositivos electrónicos (incluidos los proporcionados por la empresa y "traiga su propio dispositivo"); y e)versiones impresas.

Sección 2: Definiciones

Las definiciones que se presentan a continuación se refieren a los fines de esta Norma. Los términos en mayúsculas que no estén definidos tendrán el significado que se les atribuye en el Acuerdo.

"Información Confidencial" significa la Información considerada confidencial o de propiedad por una de las partes del Acuerdo (la "Parte Reveladora"), incluida la Información considerada confidencial o de propiedad exclusiva en virtud de las obligaciones de la Parte Reveladora para con otra Persona, que puede ser divulgada o adquirida por o en nombre de la otra parte (la "Parte Receptora") o que puede ser creada por la Parte Receptora que se basa en una divulgación de dicha Información recibida de la Parte Reveladora. A los efectos del Acuerdo, la Información Confidencial puede incluir cualquier información sobre el Acuerdo, incluida su existencia, planes y resultados de investigación y desarrollo; nuevos compuestos y procesos; procedimientos de evaluación (incluidas las pruebas clínicas y de campo); formulaciones de productos; métodos de fabricación; solicitudes a las autoridades gubernamentales; precios o costos; planes de construcción; estudios y planes de ventas, marketing y publicidad; listas de clientes; información y software informático; técnicas especiales exclusivas del negocio de Lilly; información sujeta a un derecho de privacidad, incluso en virtud de la Ley Aplicable; Secretos Comerciales; información que Lilly mantiene bajo un sistema de protección contra el acceso no autorizado; e información personal. El estado de la información como Información Confidencial no se ve afectado por los medios de adquisición o divulgación. Por ejemplo, la Información Confidencial puede adquirirse mediante comunicación escrita, oral o electrónica; directamente del Representante de la Parte Reveladora o contratista independiente, o indirectamente a través de uno o más intermediarios; o por observación visual. Del mismo modo, la adquisición o divulgación de información puede ser intencional o inadvertida sin afectar su estatus como Información Confidencial. Sin perjuicio de cualquier disposición en contrario en el Acuerdo, la Información Confidencial (que no sea Información Personal) no incluye ninguna información que:

(a) Es generalmente conocido por el público o se vuelve generalmente conocido por el público por medios distintos al incumplimiento por parte de la Parte Receptora de un deber contractual, legal o fiduciario de confidencialidad adeudado a la Parte Reveladora, sus Afiliados, sus Subcontratistas (si corresponde) o cualquiera de sus Representantes;

(b) La Parte Receptora lo poseía legalmente antes de adquirirlo como resultado del Acuerdo;

(c) Está o se pone a disposición de la Parte Receptora de forma no confidencial de una tercera persona que, según el conocimiento de la Parte Receptora después de la debida investigación, no está obligada por ningún deber contractual, legal o fiduciario de confidencialidad hacia la Parte Reveladora, sus Afiliados o los Representantes de la Parte Reveladora o sus Afiliados; o

(d) Es desarrollado íntegramente por Representantes de la Parte Receptora que no tienen acceso a la Información Confidencial de la Parte Reveladora.

a. **"Información personal"** se refiere a cualquier información, proporcionada por Lilly o recopilada por el Proveedor de Lilly, en relación con un Sujeto de datos, que pueda asociarse con un consumidor u hogar. La información personal puede estar en cualquier medio o formato, incluidos registros computarizados o electrónicos, así como archivos en papel. La información personal incluye, pero no se limita a: (i) un nombre o apellido o iniciales; (ii) un domicilio u otra dirección física; (iii) una dirección de correo electrónico u otra información de contacto en línea; (iv) un número de teléfono; (v) un número de seguro social, número de identificación fiscal, número de identificación individual u otro identificador emitido por el gobierno; (vi) una dirección de Protocolo de Internet ("IP") o nombre de host; (vii) un identificador persistente, como un número de cliente contenido en una "cookie" o un número de serie del procesador, que se combina con otros datos disponibles que identifican a un individuo; (viii) fechas de nacimiento o fechas de tratamiento; o

(ix) datos codificados que se derivan de la Información Personal. Además, en la medida en que se procese cualquier otra información, como, entre otros, información de formulario de informe de caso, códigos de identificación de ensayos clínicos, información de perfil personal, otros identificadores únicos o información biométrica, dicha información también se considerará Información personal. Para evitar dudas, la información personal que haya sido seudonimizada, lo que significa que la información no puede atribuirse a una persona física sin el uso de información adicional, también se considerará información personal.

b. **Información"** a los efectos del Estándar de Seguridad de la Información abarca tanto la Información Confidencial como la Información Personal que se utiliza con fines comerciales (en adelante, denominada de forma independiente y/o colectiva en el presente documento como "Información").

Sección 3: Políticas y Procedimientos de Seguridad de la Información:

1. El Tercero/Proveedor debe tener y cumplir con políticas, estándares y procedimientos de seguridad de la información documentados para establecer su entorno de control relacionado con la protección de la confidencialidad, integridad y disponibilidad de la Información. Las políticas y procedimientos deben ser revisados, actualizados y aprobados por la alta dirección anualmente.
2. Si el uso de dispositivos personales para acceder a la información o a los sistemas está permitido por un tercero/proveedor, se debe implementar una política de "traiga su propio dispositivo".

Sección 4: Gobernanza y formación:

1. El personal de terceros/proveedores debe completar la capacitación pertinente en seguridad de la información con requisitos de protección y manejo seguro de la información. Un resumen de la capacitación completada debe estar disponible a pedido.
2. El Tercero/Proveedor proporcionará un representante como único punto de contacto para todos los elementos relacionados con la seguridad de la información. Además, el Tercero/Proveedor tendrá asignado un representante que sea responsable de supervisar el cumplimiento de esta Norma de Seguridad de la Información.

Sección 5: Prácticas de seguridad de recursos humanos:

1. Las evaluaciones previas al empleo, incluidas las verificaciones de antecedentes penales (cuando lo permita la ley local), la revisión del currículum vitae o la hoja de vida, la revisión de las credenciales y la experiencia, y las entrevistas deben realizarse antes de la contratación.
2. Deben existir acuerdos de confidencialidad, no divulgación o equivalentes para todos los empleados. Los acuerdos incluyen, entre otros, los siguientes:
   a. Obligaciones de confidencialidad posteriores al empleo/contratación.
   b. Disposiciones que rigen el uso aceptable de los recursos electrónicos, incluido, entre otros, el uso de los recursos electrónicos de manera profesional, legal y ética.

3. Deben existir procesos para identificar y recopilar activos (físicos y electrónicos) de las personas al salir de la empresa o para aquellos que ya no requieren acceso.

Sección 6: Acceso a la información:

1. El Tercero/Proveedor debe tener, como mínimo, los siguientes controles de activación de la cuenta cuando el Tercero/Proveedor tenga Información que pertenezca a Lilly o que se le confíe que resida fuera del entorno de Lilly y/o cuando el Tercero/Proveedor tenga una conexión de acceso remoto al entorno de Lilly:
   a. Un proceso de aprobación formal para otorgar acceso basado en tener una necesidad empresarial para realizar tareas laborales (es decir, privilegio mínimo, es decir, el nivel de acceso necesario, pero no más).
   b. Segregación entre solicitud, aprobación y concesión de acceso.
   c. Las cuentas de usuario para el acceso a sistemas, servicios y aplicaciones deben asignarse a usuarios individuales y no compartirse.
   d. Las cuentas de usuario privilegiadas y/o administrativas deben ser diferentes a la cuenta de usuario estándar y tener ID de inicio de sesión de usuario únicos. Las cuentas privilegiadas (nivel elevado de acceso, que otorga poderes dentro de un sistema informático, que son significativamente mayores que los disponibles para el usuario común) deben restringirse y solo asignarse a los usuarios autorizados.
2. Los controles de contraseña deben ser implementados adecuadamente por el Tercero/Proveedor, incluidos los siguientes requisitos:
   a. Historial y caducidad periódica.
   b. Las contraseñas temporales se comunican de forma segura y se les pide que se cambien después del primer uso.
   c. Cambie las contraseñas inmediatamente cuando haya motivos para creer que una cuenta se ha visto comprometida.
   d. Las contraseñas de las cuentas de sistemas, servicios y aplicaciones compartidas deben cambiarse cuando alguien que conozca la contraseña abandone el Tercero/Proveedor o cambie a una posición diferente que ya no requiera el acceso.
   e. La identidad del usuario debe verificarse antes de restablecer una contraseña.
   f. Todas las contraseñas predeterminadas deben cambiarse de los valores predeterminados.
   g. Los requisitos de seguridad de las contraseñas deben cumplir con la longitud y la complejidad del estándar de seguridad común (e.g. ISO, NIST).
3. Se deben implementar los siguientes controles de desactivación para el Tercero/Proveedor:
   a. Un proceso formal para desactivar oportunamente las cuentas de los que se van y/o de los que ya no lo han hecho. a empresa debe tener acceso (por ejemplo, dentro de las 24 horas posteriores a la terminación).
   b. Proceso para garantizar la notificación a Lilly de cambios de personal de terceros/proveedores, dentro de las 24 horas, cuando dicho personal tenga cuentas o se le otorgue acceso a los sistemas de información de Lilly.
4. Los siguientes controles de acceso deben ser implementados por el Tercero/Proveedor:
   a. Las revisiones periódicas de acceso de todos los usuarios, cuentas del sistema, cuentas de prueba y cuentas genéricas deben realizarse y documentarse al menos una vez al año.
   b. Las cuentas de usuario deben bloquearse después de un número definido de intentos fallidos.
   c. Las cuentas sin actividad reciente (por ejemplo, los últimos 90 días, con la excepción de las que solo se utilizan para el procesamiento trimestral, semestral y anual) deben deshabilitarse.
   d. Los controles de sesión, incluido el bloqueo de cuentas y el tiempo de espera de sesión, deben estar en su lugar.

e. La autenticación multifactor (MFA) debe estar en su lugar para cualquier cuenta con privilegios y/o administrativa.
f. MFA debe estar en su lugar para cualquier aplicación que esté orientada a Internet.
g. MFA debe estar en su lugar para cualquier método de acceso remoto (por ejemplo, redes privadas virtuales, protocolos de escritorio remoto).

Sección 7: Seguridad de la red y del sistema:

1. El Tercero/Proveedor debe tener, como mínimo, los siguientes controles de seguridad de la red y del sistema cuando el Tercero/Proveedor tenga Información que pertenezca o se le confíe que resida fuera del entorno de Lilly y/o cuando el Tercero/Proveedor tenga una conexión de acceso remoto al entorno de Lilly:

   a. Estándares de endurecimiento para sistemas operativos, aplicaciones y dispositivos de red.
   b. Todos los sistemas deben ser parcheados para las actualizaciones del sistema operativo y de los componentes principales tras la publicación y evaluación de parches relacionados con la seguridad de acuerdo con los estándares de seguridad comunes (por ejemplo, ISO, NIST). Las vulnerabilidades de alto riesgo para las aplicaciones orientadas a Internet deben parchearse lo antes posible, pero no deben exceder los 30 días.
   c. Los sistemas deben mantenerse a niveles que permitan aplicar los últimos parches de seguridad/paquetes de servicio.

2. Controles de seguridad de la red:
   a. La información que pertenezca o se le confíe a Lilly no debe almacenarse en una zona desmilitarizada (DMZ).
   b. Las políticas de firewall deben implementarse en todas las interfaces de red que restrinjan el tráfico entrante y saliente en función de las necesidades.
   c. Se deben implementar sistemas de detección o prevención de intrusiones para detectar y responder al tráfico de red no autorizado o malicioso.
   d. Si existe un acuerdo de nivel de servicio de disponibilidad en un sistema o aplicación entre Lilly y un Tercero/Proveedor, se aplica la protección contra la Denegación de Acceso Distribuida (DDoS).

3. Controles de seguridad de los sistemas:
   a. Los dispositivos de punto final deben estar cifrados y protegidos con una contraseña.
   b. Los terminales móviles (smartphones, tabletas) deben protegerse mediante un sistema de gestión de dispositivos móviles.
   c. Los servidores y los endpoints deben estar protegidos mediante protección contra virus/malware que se mantenga actualizada.

Sección 8: Registro y monitoreo:

1. Las actividades de registro deben documentarse y realizarse de acuerdo con normas de seguridad comunes (por ejemplo, ISO, NIST). El monitoreo debe identificar mínimamente los eventos de ciberseguridad y verificar la efectividad de las medidas de protección.

Sección 9: Gestión de amenazas y vulnerabilidades:

1. El Tercero/Proveedor deberá contar con una evaluación continua de la vulnerabilidad y un proceso de corrección oportuno para la aplicación, el sistema operativo y otros componentes de la infraestructura. Además, los servicios y procesos se diseñarán para identificar, evaluar, mitigar y proteger contra vulnerabilidades y amenazas de seguridad nuevas y existentes, incluidos virus, bots y otros códigos maliciosos.
2. El Tercero/Proveedor debe contar con los siguientes controles:

a. Pruebas de penetración independientes anuales en sus redes y aplicaciones que manejan Información.
b. Se deben realizar análisis de vulnerabilidades trimestrales en sus plataformas y redes que manejan información para garantizar la alineación con los estándares de seguridad comunes específicamente relacionados con el endurecimiento del sistema.
c. Un programa de remediación basado en el riesgo para resolver oportunamente los hallazgos de las pruebas de penetración, los análisis de vulnerabilidades y las evaluaciones de cumplimiento.
d. Según sea necesario y según lo acordado mutuamente entre Lilly y el Tercero/Proveedor, el Tercero/Proveedor compartirá los resultados de las pruebas de penetración con Lilly.

Sección 10: Gestión del cambio:

1. El Tercero/Proveedor implementará una política de control de cambios documentada que incluya:
   a. Requisitos del plan de aprobación, clasificación, pruebas y respaldo.
   b. Segregación de funciones entre solicitud, aprobación e implementación.
   c. Gestión y revisión de cambios de emergencia dentro de un período de tiempo fijo (por ejemplo, 24 horas).

Sección 11: Gestión de activos:

1. El Tercero/Proveedor debe mantener un inventario de activos, incluidos los activos de sistema/dispositivo y software cuando el Tercero/Proveedor tenga Información que pertenezca o se le confíe que resida fuera del entorno de Lilly y/o cuando el Tercero/Proveedor tenga una conexión de acceso remoto al entorno de Lilly.
2. El Tercero/Proveedor debe contar con controles de eliminación de activos para garantizar que la información (impresa y electrónica) se elimine de acuerdo con los estándares de seguridad comunes (e.g. ISO, NIST) y los requisitos legales aplicables cuando ya no sea necesaria, y se debe mantener evidencia documentada de la eliminación adecuada.

Sección 12: Manejo de la información

1. El Tercero/Proveedor debe garantizar la separación física o lógica de la Información de otra información del cliente y de la propia información del Tercero/Proveedor cuando el Tercero/Proveedor tenga Información que pertenezca o se le confíe a Lilly que resida fuera del entorno de Lilly. Además, el Tercero/Proveedor debe ser capaz de producir una descripción del flujo de Información a través de sus entornos.
2. Los intercambios electrónicos de información entre Lilly y el Tercero/Proveedor (incluyendo correo electrónico, transferencia de archivos, conectividad remota, etc.) deben ser asegurados utilizando servicios mutuamente acordados.
3. Se utilizarán procesos y herramientas para prevenir, detectar y responder a la pérdida de información.
4. La información no debe almacenarse ni transferirse utilizando dispositivos de almacenamiento extraíbles sin la aprobación documentada a través del propietario del negocio de Lilly (obtenida a través del proceso de solicitud de almacenamiento extraíble de Lilly). Si se utilizan dichos dispositivos, toda la información almacenada en el dispositivo debe estar encriptada.

Sección 13: Encriptación

1. El cifrado es necesario para la información en tránsito cuando un tercero/proveedor tiene información que pertenece o se le confía a Lilly que reside fuera del entorno de Lilly.
2. Las claves de cifrado propiedad o administradas por el Tercero/Proveedor deben almacenarse en una ubicación segura separada de la ubicación donde se almacena la información con acceso administrado, junto con la capacidad de recuperación de claves demostrada.
3. Los procedimientos y prácticas de cifrado cumplirán las normas de seguridad comunes vigentes (e.g. ISO, NIST).

Sección 14: Seguridad física

1. Se establecerán y aplicarán controles físicos y de proceso para proteger las copias impresas y los sistemas de información (por ejemplo, hardware, software, documentación y datos) cuando el Tercero/Proveedor tenga Información que pertenezca o se le confíe que resida fuera del entorno de Lilly y/o cuando el Tercero/Proveedor tenga una conexión de acceso remoto al entorno de Lilly.
2. Los centros de datos deben estar bajo control físico, y el acceso debe gestionarse formalmente en función de las necesidades del negocio. Los centros de datos deben tener controles ambientales (temperatura, humedad, respaldo de energía) para evitar interrupciones o pérdidas.
3. Se requerirá una evaluación anual independiente de la seguridad física de las instalaciones para los Terceros/Proveedores que transmitan, almacenen o procesen Información.

Sección 15: Resiliencia / Continuidad del negocio / Copia de seguridad y recuperación de la información

1. Además de los requisitos del acuerdo para la continuidad de la actividad y la recuperación en caso de en caso de desastre o interrupción en línea con los requisitos comerciales contractuales y la criticidad de la Información, el Tercero/Proveedor se asegurará de que se implementen los siguientes controles.
   a. La energía redundante y la capacidad de procesamiento deben existir dentro de la instalación de procesamiento de datos principal.
   b. Asegurarse de que un sitio de procesamiento alternativo debe estar disponible para continuar con los procesos comerciales y recuperar la funcionalidad de Lilly dentro de la ventana de tiempo especificada del acuerdo, si corresponde.
   c. Se deben realizar pruebas anuales de resiliencia para demostrar la continuidad efectiva del negocio y la capacidad de recuperación.
   d. Los sistemas y datos aplicables deben ser respaldados regularmente en función de la criticidad. Las copias de seguridad deben probarse periódicamente para comprobar su viabilidad.
   e. Las cintas y/o transmisiones de copia de seguridad deben estar debidamente protegidas y separadas del almacenamiento primario.

Sección 16: Retención y destrucción de registros

1. El Tercero/Proveedor conservará la Información solo durante el tiempo especificado en el acuerdo aplicable, excepto en la medida en que la ley o los reglamentos aplicables exijan un período de retención más largo.
2. Al finalizar el contrato, el Tercero/Proveedor debe devolver, eliminar o destruir de forma segura la Información según las instrucciones de Lilly, excepto que pueden hacer y conservar una (1) copia según sea necesario de conformidad con la ley aplicable para su uso en sus archivos legales.
3. A petición de Lilly, el Tercero/Proveedor debe certificar que la Información ha sido destruida según las instrucciones.

Sección 17: Respuesta, gestión y presentación de informes a incidentes de seguridad de la información

1. El Tercero/Proveedor debe contar con procedimientos de gestión y respuesta a incidentes de seguridad (por ejemplo, exposición, infracción, robo, etc.) que permitan una detección, investigación, respuesta, mitigación y notificación razonables de eventos que impliquen una amenaza para la confidencialidad, integridad y/o disponibilidad de la Información cuando el Tercero/Proveedor tenga Información perteneciente a Lilly o confiada a ella que resida fuera del entorno de Lilly y/o cuando el Tercero/Proveedor tenga acceso remoto conexión con el entorno de Lilly. Los procedimientos de gestión y respuesta a incidentes deben documentarse, probarse y revisarse al menos una vez al año. Lilly tendrá la opción de revisar dichos procedimientos si así lo solicita.
2. El Tercero/Proveedor notificará a Lilly con prontitud, pero a más tardar 48 horas, de los incidentes de seguridad sospechados o conocidos que tengan un impacto potencial en la Información de Lilly.

Además, el Tercero/Proveedor deberá contar con un proceso documentado, con contactos definidos de Lilly y de Tercero/Proveedor, para garantizar el cumplimiento de este requisito de notificación.

3. El Tercero/Proveedor cooperará plenamente con Lilly para comprender la situación, la causa raíz y determinar las soluciones necesarias en caso de un incidente de seguridad real o sospechado.

Sección 18: Gestión de subcontratistas

1. Esta Norma de Seguridad de la Información se aplicará a todos los subcontratistas utilizados por el Tercero/Proveedor que manejen Información perteneciente a Lilly o confiada a ella que resida fuera del entorno de Lilly y/o cuando el Tercero/Proveedor tenga conexión de acceso remoto al entorno de Lilly. Es responsabilidad del Tercero/Proveedor asegurarse de que el Estándar de Seguridad de la Información sea comunicado y cumplido por cada subcontratista. Para evitar dudas, los subcontratistas incluyen, entre otros: terceros/proveedores de reprografía, terceros/proveedores de almacenamiento externo, desarrolladores de software, instalaciones de alojamiento en la nube e instalaciones de centros de datos.
2. Se deben ejecutar contratos formales entre el Tercero/Proveedor y los subcontratistas que describan los controles que se proporcionarán, incluidos los controles para mantener la confidencialidad, disponibilidad e integridad de la Información.
3. Se deben realizar evaluaciones iniciales y continuas para garantizar que los subcontratistas se adhieran a la Norma de Seguridad de la Información y que los incidentes y problemas de seguridad se gestionen adecuadamente.
4. Por lo general, Lilly autoriza a un Tercero/Proveedor a contratar subcontratistas que gestionarán la Información o tendrán acceso a los sistemas de Terceros/Proveedor o de Lilly en los que reside dicha Información, siempre que el Proveedor informe primero a Lilly de cualquier cambio previsto en relación con la adición o sustitución de subcontratistas y Lilly tendrá derecho a oponerse a dicho cambio y/o rescindir el acuerdo si las Partes no pueden alinearse con un Subcontratista.

Sección 19: Derechos de revisión de la seguridad de la información

1. El Tercero/Proveedor permitirá a Lilly y a sus agentes, auditores (internos y externos), reguladores y otros representantes inspeccionar, auditar, examinar y revisar las instalaciones, libros, sistemas, registros, listas de acceso, datos, prácticas y procedimientos del Tercero/Proveedor (y cualquier subcontratista que el Tercero/Proveedor pueda utilizar) para verificar la integridad de la Información y supervisar el cumplimiento de esta Norma de Seguridad de la Información.

Sección 20: Ciclo de vida del desarrollo del sistema

1. Estos requisitos son aplicables únicamente a los Terceros/Proveedores que construyen sistemas, software o aplicaciones para Lilly.
2. Metodología de ingeniería de desarrollo de software:
   a. Una metodología de desarrollo de sistemas definida debe implementarse formalmente con políticas, procedimientos y estándares comunicados y seguidos, y debe estar alineada con los estándares de la industria. Los estándares de programación deben desarrollarse y comunicarse a los miembros relevantes de la fuerza laboral. Los estándares incluyen especificaciones de arquitectura y diseño, revisión de lógica de negocios, adopción de algoritmos y bibliotecas seguros, eliminación de código de prueba y la corrección de fallas de seguridad comunes (por ejemplo, las diez principales vulnerabilidades de OWASP).
   b. Se deben realizar revisiones de código para confirmar el cumplimiento de los estándares de programación anteriores.
   c. El uso de datos de producción en entornos que no sean de producción solo debe realizarse cuando sea necesario y se deben implementar los mismos controles de seguridad que existen en el entorno de producción, o la información de producción utilizada en las pruebas debe estar suficientemente ofuscada.

d. El software que está disponible en el dominio público (por ejemplo, software de código abierto, shareware, freeware), si se utiliza, debe ser examinado adecuadamente para detectar riesgos potenciales, incluidos los riesgos legales potenciales (por ejemplo, violación de derechos de autor).

e. El software que está disponible en el dominio público (por ejemplo, software de código abierto, shareware, freeware), si se utiliza, debe incluir controles para garantizar que la introducción de este tipo de software no tenga a impacto negativo (por ejemplo, virus, troyanos, brechas de seguridad como "puerta trasera").

f. El código fuente debe mantenerse en una herramienta de control de versiones no pública aceptada por la industria, con controles estrictos relacionados con la extracción del código fuente. El Tercero/Proveedor debe tener sistemas de monitoreo que monitoreen los cambios en el código de entorno.

g. Gestione el ciclo de vida de la seguridad de todo el software desarrollado y adquirido internamente

3. Liberación de código:

a. El Tercero/Proveedor buscará la mejora continua en el modelo de desarrollo elegido.

b. El Tercero/Proveedor debe tener una política/procedimiento formal de gestión de cambios/versiones para las actualizaciones de software planificadas que demuestre que las versiones se planifican, gestionan, prueban, aprueban y comunican adecuadamente, y Lilly debe ser notificado con antelación de los cambios programados.

c. Los ciclos de gestión de cambios/liberaciones comienzan con la definición de requisitos. El impacto, la retroalimentación y la necesidad de Lilly deben tenerse en cuenta adecuadamente en los requisitos de los lanzamientos planificados.

d. Se deben realizar pruebas de regresión durante cada ciclo de lanzamiento. Las pruebas deben realizarse a varios niveles. (por ejemplo, unidad, integración y sistema, usuario). Las pruebas de usuario deben basarse en planes de prueba formales, realizados por partes independientes de quienes diseñan y desarrollan el sistema.

e. Las aprobaciones formales deben capturarse en cada etapa del ciclo de vida del desarrollo (requisitos, diseño, pruebas, aceptación del usuario, implementación de producción, etc.). Cuando se capturan las aprobaciones, debe quedar claro quién está aprobando, la fecha en que lo están aprobando y qué lo están aprobando.

f. Las versiones y los parches deben proporcionarse con instrucciones suficientes para su implementación y/o uso. Esto incluye aquellas soluciones en las que se proporciona a Lilly la versión o el parche para que se aplique, así como aquellas en las que se notifica a Lilly de un cambio que el Tercero/Proveedor ha aplicado en un entorno de Lilly.

g. Los diseños de sistemas deben crearse formalmente para ayudar a traducir los requisitos al código.

4. Cambios provisionales/correcciones de errores:

a. Debe existir un procedimiento formal para implementar cambios de emergencia/corrección de errores, incluidos aquellos para abordar las vulnerabilidades de seguridad, para confirmar que estos cambios se pueden realizar de manera oportuna y controlada.

b. Debe existir un proceso formal para comunicar los errores o defectos conocidos a Lilly.

c. Los cambios en la corrección de errores deben probarse formalmente y demostrar la documentación y las aprobaciones adecuadas. La aprobación debe ser otorgada por alguien que no sea la(s) persona(s) que realiza(n) el cambio.