ESTÁNDAR DE SEGURIDAD DE LA INFORMACIÓN ("ISS")

Esta Norma de Seguridad de la Información establece los requisitos de seguridad de la información de Eli Lilly and Company y sus filiales ("Lilly") frente a terceros/proveedores 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.

Como se menciona en el presente documento, el término "Información" abarca tanto la Información Confidencial como la Información Personal que se utiliza con fines comerciales (en lo sucesivo, denominada de forma independiente y/o colectiva en el presente documento como "Información"). Información personal se refiere a cualquier información tal y como se define en el Estándar de Privacidad de Proveedores ("SPS") de Lilly. Información confidencial se refiere a cualquier información confidencial o de propiedad exclusiva tal y como se define como tal (o con una designación similar) en cualquier contrato escrito entre el Tercero/Proveedor y Lilly.

Para mayor claridad, este Estándar de Seguridad de la Información se aplica a toda la Información procesada por un Tercero/Proveedor, incluido el procesamiento por: (i) creación; (ii) edición; (iii) gestión; (iv) procesamiento; (v) acceso; (vi) recepción; (vii) transferencia; (viii) destrucción; (ix) almacenamiento; y/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 Lilly y/o los propiedad del Tercero/Proveedor denominados "traiga su propio dispositivo"); y e) versiones impresas.

1. Políticas y procedimientos de seguridad de la información:

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 anualmente por la alta dirección.

Si Lilly permite el uso de dispositivos personales para acceder a información o sistemas al Tercero/Proveedor, el Tercero/Proveedor debe implementar una política de "traiga su propio dispositivo".

2. Gobernabilidad y Formación:

El personal del Tercero/Proveedor debe completar la capacitación pertinente en seguridad de la información con requisitos de protección y manejo seguro de la información. Un resumen de la formación completada debe ponerse a disposición de Lilly si así lo solicita.

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 un representante designado que será responsable de supervisar el cumplimiento de esta Norma de Seguridad de la Información.

3. Prácticas de seguridad de recursos humanos:

De acuerdo con el objeto del contrato, el Tercero/Proveedor se compromete a llevar a cabo una evaluación previa a la contratación, incluida la verificación de antecedentes penales (cuando lo permita la legislación local), la revisión del plan de estudios, la revisión de credenciales y experiencia, y la realización de una entrevista con el fin de asignar a los profesionales adecuados que trabajarán con la Información.

El Tercero/Proveedor se compromete a celebrar acuerdos de confidencialidad, no divulgación o equivalentes durante la duración del acuerdo mantenido con Lilly con todos los empleados del Tercero/Proveedor que manejen la Información de Lilly. Los acuerdos de confidencialidad deben incluir, entre otros:

A. Obligaciones de confidencialidad posteriores al empleo/contratación.
B. Disposiciones que rigen el uso aceptable de recursos electrónicos, incluido, entre otros, el uso de recursos electrónicos de manera profesional, legal y ética.

Deben existir procesos para identificar y recopilar activos (físicos y electrónicos) de las personas cuando abandonan el Tercero/Proveedor o de aquellos que ya no requieren acceso a la Información.

4. Acceso a la información:

El Tercero/Proveedor debe tener al menos los siguientes controles de activación de cuenta cuando tenga acceso a Información que pertenezca a Lilly o que Lilly le confíe y/o que esté almacenada 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 una necesidad comercial compatible con las funciones laborales realizadas por el personal del Tercero/Proveedor, es decir, privilegios mínimos de acceso a la información o nivel de acceso requerido, pero nunca mayor que el requerido.
B. Segregación entre solicitud, aprobación y concesión de acceso.
C. Las cuentas de usuario para acceder a sistemas, servicios y aplicaciones deben asignarse a usuarios individuales y no se pueden compartir.
D. Las cuentas de usuario con privilegios y/o administrativas deben ser diferentes de las cuentas de usuario estándar y tener identificadores de inicio de sesión de usuario únicos. Las cuentas privilegiadas (alto nivel de acceso, que otorga poderes dentro de un sistema informático, que son significativamente mayores que los disponibles para el usuario promedio) deben restringirse y asignarse solo a usuarios autorizados.

Los controles de contraseña deben ser implementados adecuadamente por el Tercero/Proveedor y deben incluir los siguientes requisitos:

A. Historial y caducidad periódica.
B. Las contraseñas temporales deben comunicarse de forma segura y con la obligación de cambiarlas después del primer uso.
C. Cambiar inmediatamente las contraseñas cuando haya motivos para creer que una cuenta se ha visto comprometida.
D. Las contraseñas de las cuentas compartidas de sistemas, servicios y aplicaciones deben cambiarse cuando el personal de terceros/proveedor que tiene acceso a la contraseña abandona el tercero/proveedor o se traslada a un puesto diferente que ya no requiere 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 el estándar de seguridad común (por ejemplo, ISO, NIST), la longitud y la complejidad.

El Tercero/Proveedor debe implementar los siguientes controles de exclusión:

A. Un proceso formal para desactivar a tiempo las cuentas de las personas que se desvinculan del Tercero/Proveedor y/o aquellas que ya no tienen una necesidad comercial de acceder (dentro de las veinticuatro horas posteriores a la terminación).
B. Proceso para garantizar la notificación a Lilly de cambios en el personal de Terceros/Proveedores dentro de las veinticuatro (24) horas cuando dichos empleados tengan cuentas o tengan acceso a la información o a los sistemas de información de Lilly.

Los siguientes controles de acceso deben ser implementados por el Tercero/Proveedor:

A. Se deben realizar y documentar revisiones periódicas, al menos una vez al año, del acceso de todos los usuarios, cuentas del sistema, cuentas de prueba y cuentas genéricas.
B. Las cuentas de usuario deben bloquearse después de un número determinado de intentos de acceso fallidos.
C. Las cuentas sin actividad reciente (por ejemplo, en los últimos noventa (90) días, con la excepción de las que se utilizan solo para el procesamiento trimestral, semestral y anual) deben desactivarse.
D. Los controles de sesión, incluido el bloqueo de cuentas y los tiempos de espera de sesión, deben estar en su lugar.
E. La autenticación multifactor (MFA) debe estar en su lugar para todas las cuentas con privilegios y/o administrativas.
F. MFA debe estar en su lugar para todas las aplicaciones orientadas a Internet.
G. La MFA debe estar en su lugar para cualquier método de acceso remoto (por ejemplo, redes privadas virtuales, protocolos de escritorio remoto).

5. Seguridad de redes y sistemas:

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

A. Estándares de protección para sistemas operativos, aplicaciones y dispositivos de red.
B. Todos los sistemas deben ser parchados para las actualizaciones del sistema operativo y de los componentes principales después de que se publique el parche relacionado con la seguridad y se evalúe 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 y no deben exceder los treinta (30) días.
C. Los sistemas deben mantenerse en niveles para permitir que se apliquen los parches de seguridad/Service Pack más recientes.

Para los controles de seguridad de red:

A. La información que Lilly posee o confía al Tercero/Proveedor 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 la necesidad.
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 el Tercero/Proveedor, se aplica la protección de denegación de acceso distribuida (DDoS).

Controles de seguridad del sistema:

A. Los dispositivos de punto final deben estar cifrados y protegidos con una contraseña.
B. Los terminales móviles (smartphones, tablets) deben estar protegidos mediante un sistema de gestión de dispositivos móviles.
C. Los servidores y los endpoints deben protegerse con una protección contra virus/malware que se mantenga actualizada.
D. Registro y monitoreo:Las actividades de registro deben documentarse y realizarse de acuerdo con estándares 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.

7. Gestión de amenazas y vulnerabilidades:

El Tercero/Proveedor llevará a cabo un proceso continuo de evaluación y corrección de vulnerabilidades de manera oportuna para las aplicaciones, el sistema operativo y otros componentes de la infraestructura. Además, los servicios y procesos deben diseñarse para identificar, evaluar, mitigar y proteger la información de amenazas y vulnerabilidades de seguridad nuevas y existentes, incluidos virus, botas y otros códigos maliciosos.

El Tercero/Proveedor debe contar con los siguientes controles:

A. Pruebas de penetración independientes anuales de sus redes y aplicaciones que manejan la información.
B. Se deben realizar análisis de vulnerabilidades trimestrales en las plataformas y redes que manejan la información para garantizar la alineación con los estándares de seguridad comunes específicamente relacionados con la protección del sistema.
C. Un programa de corrección basado en riesgos para resolver oportunamente los hallazgos de las pruebas de penetración, los análisis de vulnerabilidades y las evaluaciones de cumplimiento.
D. Según sea necesario, el Tercero/Proveedor trabajará para satisfacer las solicitudes de Lilly para realizar pruebas de penetración en la red.

8. Gestión del cambio:

El Tercero/Proveedor implementará una política de control de cambios documentada que incluirá:

A. Planifique los requisitos de aprobación, calificación, pruebas y retroceso.
B. Segregación de funciones entre solicitud, aprobación e implementación.Gestión y revisión de cambios de emergencia dentro de un período fijo (por ejemplo, 24 (veinticuatro) horas).

9. Gestión de activos:

El Tercero/Proveedor mantendrá un inventario de activos, incluidos los activos del sistema/dispositivo y software, cuando tenga acceso a Información que pertenezca o que Lilly le haya confiado al Tercero/Proveedor y/o que esté almacenada fuera del entorno de Lilly y/o cuando el Tercero/Proveedor tenga una conexión de acceso remoto al entorno de Lilly.

El Tercero/Proveedor deberá 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 (por ejemplo, ISO, NIST) y los requisitos legales aplicables cuando ya no sea necesaria, así como mantener evidencia documentada de la eliminación adecuada.

10. Tratamiento de la información:

El Tercero/Proveedor garantizará la separación física o lógica de la Información del resto de la información de Lilly, de la información de otros clientes y de la propia información del Tercero/Proveedor siempre que el Tercero/Proveedor tenga acceso a Información que pertenezca o que Lilly le haya confiado al Tercero/Proveedor y/o que esté almacenada fuera del entorno de Lilly y/o cuando el Tercero/Proveedor tenga una conexión de acceso remoto al entorno de Lilly. Además, el Tercero/Proveedor debe ser capaz de producir una descripción del flujo de Información en sus entornos.

Los intercambios electrónicos de información entre Lilly y el tercero/proveedor (incluyendo correo electrónico, transferencia de archivos, conectividad remota, etc.) se asegurarán mediante servicios escritos mutuamente acordados.

Se deben utilizar procesos y herramientas para prevenir, detectar y responder a la pérdida de información. La información no debe almacenarse ni transferirse utilizando dispositivos de almacenamiento extraíbles sin la aprobación documentada 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.

11. Encriptación:

El cifrado es necesario para la información en tránsito cuando el Tercero/Proveedor tiene acceso a Información propiedad de Lilly o confiada por Lilly al Tercero/Proveedor y/o que se almacena fuera del entorno de Lilly y/o cuando el Tercero/Proveedor tiene una conexión de acceso remoto al entorno de Lilly.

Las claves de cifrado que son propiedad o están gestionadas por el Tercero/Proveedor deben almacenarse en una ubicación segura separada de la ubicación donde se almacena la Información con acceso gestionado, junto con la capacidad de recuperación de claves demostrada.

Los procedimientos y prácticas de cifrado deben cumplir con los estándares de seguridad comunes actuales (por ejemplo, ISO, NIST).

12. Seguridad física:

Se deben establecer y aplicar 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 acceso a Información propiedad de Lilly o confiada por Lilly y/o que esté almacenada fuera del entorno de Lilly y/o cuando el Tercero/Proveedor tenga una conexión de acceso remoto al entorno de Lilly.

Los centros de datos deben estar bajo control físico, con un acceso gestionado formalmente en función de las necesidades empresariales del tercero/proveedor. Los Centros de Datos deben contar con controles ambientales (temperatura, humedad, respaldo de energía) para evitar interrupciones o pérdidas de Información.

Se requerirá una evaluación anual independiente de la seguridad física de la instalación si el Tercero/Proveedor transmite, almacena y/o procesa Información.

13. Resiliencia/Continuidad del negocio/Copia de seguridad y recuperación de la información:

Además de los requisitos establecidos en un acuerdo celebrado entre Lilly y el Tercero/Proveedor para la continuidad del negocio y la recuperación ante desastres, de acuerdo con los requisitos comerciales contractuales y la criticidad de la Información, el Tercero/Proveedor debe asegurarse de que se implementan los siguientes controles.

a) La energía redundante y la capacidad de procesamiento deben existir dentro de la instalación de procesamiento de datos principal.
b) Asegúrese de que debe haber una ubicación de procesamiento alternativa disponible para continuar con los procesos comerciales y recuperar la funcionalidad de Lilly dentro de la ventana de tiempo especificada por el contrato, si corresponde.
c) Deben implementarse pruebas anuales de resiliencia para demostrar la continuidad efectiva del negocio y la capacidad de recuperación.
d) Se debe realizar una copia de seguridad periódica de los sistemas y datos aplicables en función de la criticidad. La viabilidad de las copias de seguridad debe probarse periódicamente.
e) Las cintas y/o transmisiones de copia de seguridad deben estar adecuadamente protegidas y separadas del almacenamiento primario.

14. Retención y destrucción de registros:

El Tercero/Proveedor conservará la Información solo durante el tiempo especificado en el acuerdo con Lilly, a menos que las leyes o reglamentos aplicables exijan un período de retención más largo.
Tras la terminación del contrato con Lilly, por cualquier motivo, el Tercero/Proveedor está obligado a devolver, eliminar o destruir la Información de forma segura, según las instrucciones del contrato, cuando corresponda o proporcionada por Lilly.

A petición de Lilly, el Tercero/Proveedor debe emitir un certificado que atestigüe que la Información ha sido destruida según las instrucciones de Lilly.

15. Respuesta, gestión e informes de incidentes de seguridad de la información:

El Tercero/Proveedor deberá contar con procedimientos de gestión y respuesta a incidentes de seguridad (por ejemplo, exposición, violación, robo, etc.) que permitan la detección, investigación, respuesta, mitigación y notificación razonables de eventos que impliquen una amenaza a la confidencialidad, integridad y/o disponibilidad de la Información siempre que el Tercero/Proveedor tenga acceso a Información que pertenezca o sea confiada por Lilly al Tercero/Proveedor y/o que esté almacenada fuera del Lilly y/o cuando el Tercero/Proveedor tenga una conexión de acceso remoto al 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.

El Tercero/Proveedor debe notificar a Lilly dentro de las veinticuatro (24) horas del evento de incidentes de seguridad sospechados o conocidos que tengan un impacto potencial en la Información. Además, el Tercero/Proveedor debe tener un proceso documentado, con contactos definidos de Lilly y de Tercero/Proveedor, para garantizar el cumplimiento de este requisito de notificación.

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.

16. Gestión de subcontratistas:

Esta Norma de Seguridad de la Información se aplica a todos los subcontratistas utilizados por el Tercero/Proveedor que gestionan Información propiedad de Lilly o confiada a ella que se almacena fuera del entorno de Lilly y/o en los que el Tercero/Proveedor tiene una 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 que tenga acceso a la Información. Para evitar dudas, los subcontratistas incluyen, entre otros, proveedores de reprografía/proveedores de terceros, proveedores de almacenamiento externo/de terceros, desarrolladores de software, instalaciones de alojamiento en la nube e instalaciones de centros de datos.

Se celebrarán contratos formales entre Terceros/Proveedores y subcontratistas, en los que se describirán los controles que se proporcionarán, incluidos los controles para mantener la confidencialidad, disponibilidad e integridad de la Información.

El Tercero/Proveedor debe realizar evaluaciones iniciales y continuas para garantizar que los subcontratistas se adhieran al Estándar de Seguridad de la Información y que los incidentes y problemas de seguridad se gestionen adecuadamente.

El Tercero/Proveedor debe informar a Lilly y obtener una aprobación por escrito antes de autorizar el acceso a la Información de Lilly por parte de los subcontratistas.

17. Derechos de análisis de seguridad de la información:

El Tercero/Proveedor permitirá a Lilly y a sus agentes, auditores (internos y/o externos) y/o cualquier otro representante inspeccionar, auditar, examinar y revisar las instalaciones, libros, sistemas, registros, listas de acceso, datos, prácticas y procedimientos del Tercero/Proveedor y de 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.

18. Ciclo de vida de desarrollo del sistema:

Los requisitos que se indican a continuación solo se aplicarán en el caso de que el Tercero/Proveedor desarrolle software o aplicaciones para Lilly.

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. Las normas de programacion deben desarrollarse y comunicarse a los miembros pertinentes de la fuerza laboral. Los estándares incluyen especificaciones de arquitectura y diseño, revisión de la lógica empresarial, adopción de algoritmos y bibliotecas seguros, eliminación de código de prueba y corrección de fallas de seguridad comunes (por ejemplo, las diez principales vulnerabilidades de OWASP).
B. Se deben realizar revisiones del 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 debe realizarse solo cuando sea necesario y, de manera similar, se deben implementar controles de seguridad 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 debidamente examinado para detectar riesgos potenciales, incluidos los riesgos legales potenciales (por ejemplo, infracción 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 un impacto negativo (por ejemplo, virus, troyanos, violaciones de seguridad como "puerta trasera").
F. código fuente debe mantenerse en una herramienta de control de versiones no pública aceptada por la industria, con controles estrictos relacionados con la verificación 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 seguridad de todo el software desarrollado y adquirido internamente

Liberación de código:

A. El Tercero/Proveedor debe buscar 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 planificar actualizaciones de software que demuestren que las versiones se planifican, gestionan, prueban, aprueban y comunican correctamente, Lilly será notificado con antelación de los cambios programados.
C. Los ciclos de gestión de cambios/liberaciones comienzan con la definición de los requisitos. El impacto, la retroalimentación y la necesidad de Lilly deben tenerse en cuenta adecuadamente en los requisitos de los lanzamientos planificados.
D. Las pruebas de regresión deben realizarse durante cada ciclo de versión. La prueba debe realizarse a varios niveles. (por ejemplo, unidad, integración y sistema, usuario). Las pruebas de usuario deben basarse en planes de prueba formales, llevados a cabo por partes independientes para 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 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 Lilly recibe la versión o el parche para aplicar, así como aquellas en las que Lilly recibe una notificación de un cambio que el Tercero/Proveedor ha aplicado a un entorno de Lilly.
G. Los diseños de sistemas deben crearse formalmente para ayudar a traducir los requisitos en código.

Cambios provisionales/correcciones de errores:

A. Debe existir un procedimiento formal para implementar cambios de emergencia o corrección de errores, incluidos los destinados a tratar las vulnerabilidades de seguridad, para confirmar que estos cambios se pueden realizar de manera oportuna pero controlada.
B. Debe existir un proceso formal para informar a Lilly de los errores o defectos conocidos.
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 persona que realiza el cambio.