ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Requisitos de seguridad de los sistemas de información

Tiene como objetivo el asegurar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas.

Análisis y especificación de los requisitos de seguridad de la información

Los requisitos relacionados con la seguridad de la información deberían ser incluidos en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes.

Los requisitos de seguridad de la información deberían identificarse utilizando varios métodos, tales como derivar los requisitos de cumplimiento a partir de las políticas y regulaciones, modelado de amenazas, revisiones de incidentes o el uso de umbrales de vulnerabilidad. Los resultados de la identificación deberían documentarse y revisarse por todas las partes interesadas.

Los requisitos de seguridad de la información y los controles deberían reflejar el valor de negocio de la información involucrada y el potencial impacto negativo de negocio, que podría ser resultado de la falta de seguridad adecuada.

Los requisitos de identificación y gestión de la seguridad de la información y los procesos asociados deberían integrarse en las etapas tempranas de proyectos de sistema de información. La consideración temprana de los requisitos de seguridad de la información, por ejemplo, en la etapa de diseño, puede dar lugar a soluciones más efectivas y eficientes de costos.

Los requisitos de seguridad de la información deberían considerar también:

a) el nivel de confianza requerido para la identidad declarada de los usuarios, a fin de obtener los requisitos de autenticación de los usuarios;

b) la provisión de acceso y de procesos de autorización, para los usuarios de negocios, así como para los usuarios privilegiados o técnicos;

c) informar a los usuarios y operadores de sus deberes y responsabilidades;

d) las necesidades de protección requeridas de los activos involucrados, en particular considerando la disponibilidad, la confidencialidad y la integridad;

e) los requisitos derivados de los procesos de negocio, tales como el registro de transacciones y seguimiento, requisitos de no-repudio;

f) los requisitos exigidos por otros controles de seguridad, por ejemplo, interfaces para el registro y la supervisión o los sistemas de detección de fugas de datos.

Si se adquieren productos, debería seguirse un proceso de prueba y adquisición formal. Los contratos con el proveedor deberían incluir los requisitos de seguridad identificados. Cuando la funcionalidad de seguridad en un producto propuesto no satisface el requisito especificado, entonces el riesgo presentado y los controles asociados deberían reconsiderarse antes de la compra del producto.

Deberían evaluarse e implantarse las directrices disponibles para la configuración de seguridad del producto alineada con el paquete final de software/servicios de ese sistema.

Deberían definirse los criterios para la aceptación de productos, por ejemplo, en términos de su funcionalidad, los cuales darán certeza de que se cumplan los requisitos de seguridad identificados. Los productos deberían evaluarse de acuerdo con estos criterios antes de la adquisición. La funcionalidad adicional debería ser revisada para asegurarse de que no presenten riesgos inaceptables adicionales.

Asegurar los servicios de aplicaciones en las redes públicas
La información involucrada en los servicios de aplicaciones que pasan a través de redes públicas, debe ser protegida de la actividad fraudulenta, de la disputa contractual y de la divulgación y modificación no autorizada.

Las consideraciones de seguridad de la información para los servicios de aplicación que pasan a través de las redes públicas deberían incluir lo siguiente:

a) el nivel de confianza que cada parte requiere en la identidad declarada de cada uno, por ejemplo, a través de la autenticación;

b) los procesos de autorización asociados con quién puede aprobar el contenido, emitir o firmar los documentos transaccionales clave;

c) asegurarse de que los socios que se comunican estén plenamente informados de sus autorizaciones para la prestación o utilización de los servicios;

d) determinar y cumplir los requisitos de confidencialidad, integridad, prueba de envío y recepción de documentos clave y el no repudio de los contratos, por ejemplo, asociados con los procesos de licitación y contratos;

e) el nivel de confianza requerido en la integridad de los documentos clave;

f) los requisitos de protección de la información confidencial;

g) la confidencialidad y la integridad de las transacciones de pedidos, la información de pago, detalles de la dirección de entrega y la confirmación de recibos;

h) el grado de verificación adecuado para verificar la información de pago suministrada por el cliente;

i) la selección del formulario de liquidación de pago más adecuado para evitar el fraude;

j) el nivel de protección requerido para mantener la confidencialidad y la integridad de la información del pedido;

k) la prevención de la pérdida o duplicación de la información de transacción;

l) la responsabilidad asociada con cualquier transacción fraudulenta;

m) los requisitos del seguro.

Muchas de las consideraciones anteriores pueden ser abordadas mediante la aplicación de controles criptográficos, teniendo en cuenta el cumplimiento de los requisitos legales.

Los acuerdos de servicios de aplicaciones entre socios deberían estar respaldados por un acuerdo documentado que compromete a ambas partes a los términos acordados de servicios, incluyendo los detalles de la autorización

Deberían considerarse los requisitos de resiliencia frente a los ataques, dentro de los que se pueden incluir requisitos para la protección de los servidores de aplicación involucrados o para asegurar la disponibilidad de las interconexiones de red necesarias para prestar el servicio.

Protección de las transacciones de servicios de aplicación
La información involucrada en las transacciones de servicios de aplicación debería ser protegida para prevenir la transmisión incompleta, el mal enrutamiento y la alteración, la divulgación, la duplicación o la reproducción no autorizada del mensaje.

Las consideraciones de seguridad de la información para las transacciones de servicio de aplicación deberían incluir lo siguiente:

a) el empleo de firmas digitales por cada una de las partes implicadas en la transacción;

b) todos los aspectos de la transacción, es decir asegurarse de que:

   1) la información secreta de autenticación del usuario de todas las partes sea válida y verificada;

   2) la transacción permanezca confidencial;

   3) la privacidad asociada con todas las partes implicadas sea conservada;

c) el canal de comunicación entre todas las partes implicadas sea cifrado;

d) los protocolos utilizados para comunicarse entre todas las partes implicadas estén asegurados;

e) asegurarse de que el almacenamiento de los detalles de transacción sea localizado fuera de cualquier ambiente público accesible, por ejemplo, en una plataforma de almacenamiento que exista en la Intranet de la organización y no conservado y expuesto en un medio de almacenamiento directamente accesible desde Internet;

f) cuando se emplea una autoridad confiable (por ejemplo, para propósitos de emitir y mantener firmas digitales y/o certificados digitales) la seguridad se integra e incorpora a través de todo el proceso completo de gestión del certificado / firma.

Seguridad en los procesos de desarrollo y soporte

Tiene como objetivo el asegurar que la seguridad de la información sea diseñada e implementada dentro del ciclo de vida del desarrollo de sistemas de información.

Política de desarrollo seguro
Las reglas para el desarrollo de software y sistemas se deberían establecer y aplicar a los desarrollos dentro de la organización.

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

El desarrollo seguro es un requisito para construir un servicio, una arquitectura, un software y un sistema seguro. Dentro de una política de desarrollo seguro, los siguientes aspectos deberían someterse a consideración:

a) la seguridad del ambiente de desarrollo;

b) la orientación sobre la seguridad en el ciclo de vida del desarrollo de software:

   1) seguridad en la metodología de desarrollo de software;

   2) fijar las directrices de codificación para cada lenguaje de programación utilizado;

c) los requisitos de seguridad en la etapa de diseño;

d) los controles de seguridad dentro de los hitos del proyecto;

e) los repositorios seguros;

f) la seguridad en el control de la versión;

g) el conocimiento requerido de la seguridad de aplicaciones;

h) la capacidad del desarrollador de evitar, encontrar y corregir vulnerabilidades.

Las técnicas seguras de programación deberían utilizarse tanto para los nuevos desarrollos como en escenarios de reutilización de código, donde las normas aplicables al desarrollo pueden no ser conocidas o no fueron coherentes con las mejores prácticas actuales. Las normas de codificación segura deberían considerarse y cuando corresponda, utilizarse. Los desarrolladores deberían capacitarse en su uso y deberían verificar su utilización en las pruebas y en la revisión de código.

Si el desarrollo es subcontratado, la organización debería obtener garantías de que la parte externa cumpla con estas reglas de desarrollo seguro.
Información adicional

El desarrollo también puede tener lugar dentro de las aplicaciones, tales como las aplicaciones de oficina, secuencia de comandos (scripting), navegadores y bases de datos.

Procedimiento de control de cambios del sistema
Los cambios en los sistemas dentro del ciclo de vida de desarrollo deberían ser contralados mediante el uso de procedimientos formales de control de cambios.

Para garantizar la integridad del sistema, aplicaciones y productos, deberían documentarse y hacerse cumplir los procedimientos formales de control de cambios, desde las etapas tempranas de diseño a través de todas las tareas de mantenimiento posteriores. La introducción de nuevos sistemas y cambios importantes a sistemas existentes debería seguir un proceso formal de documentación, especificación, pruebas, control de calidad, y gestión de implementación.

Este proceso debería incluir una evaluación de riesgo, el análisis de los impactos de los cambios, y la especificación de los controles de seguridad necesarios. Este proceso también debería asegurar que los procedimientos existentes de seguridad y control no sean comprometidos, que

a los programadores de apoyo se les da el acceso sólo a aquellas partes del sistema necesario para su trabajo y que se tenga un acuerdo formal y aprobación para cualquier cambio.

De ser practicable, los procedimientos de control de cambio de aplicación y operacionales deberían integrarse. Los procedimientos de control de cambio deberían incluir, pero no limitarse a:

a) el mantenimiento de un registro de niveles de autorización acordados;

b) asegurar que los cambios sean enviados por usuarios autorizados;

c) la revisión de los controles y procedimientos de integridad para asegurarse de que no sean comprometidos por los cambios;

d) identificar todo el software, la información, entidades de base de datos, y el hardware que requieran enmienda;

e) identificar y verificar el código crítico de seguridad para reducir al mínimo la posibilidad de las debilidades de seguridad conocidas;

f) obtener la aprobación formal para propuestas detalladas antes de que comience el trabajo;

g) asegurarse de que los usuarios autorizados acepten los cambios antes de la implementación;

h) asegurarse de que al terminar cada cambio la documentación de sistema sea actualizada y que la documentación antigua sea archivada o eliminada;

i) el mantenimiento de una versión controlada de todas las actualizaciones de software;

j) el mantenimiento de una pista de auditoría de todos los requerimientos de cambio;

k) asegurarse de que la documentación de operaciones y los procedimientos de usuario sean cambiados según sea necesario para que permanezcan actualizados;

l) asegurarse de que la implementación de cambios ocurra en el momento adecuado y no interfiera los procesos de negocio implicados.

Revisión técnica de las aplicaciones después de realizar cambios de plataforma de operación

Cuando se cambian las plataformas de operación, las aplicaciones críticas de negocio deberían ser revisadas y probadas para asegurar que no hay impacto negativo en las operaciones de la organización o de la seguridad.

Este proceso debería cubrir:

a) la revisión de los controles de aplicación y procedimientos de integridad para asegurarse de que éstos no hayan sido comprometidos por los cambios en la plataforma operativa;

b) asegurarse de que la notificación de cambios a la plataforma operativa sea provista a tiempo para permitir pruebas y revisiones apropiadas antes de que sean implementados;

c) asegurarse de que los cambios apropiados sean aplicados en los planes de continuidad de negocio.

Restricciones en los cambios a los paquetes de software
Las modificaciones a los paquetes de software deberían desalentarse, limitándose a modificaciones necesarias y todos los cambios deberían ser estrictamente controlados.

En la medida de lo posible, y practicable, los paquetes de software, suministrados por vendedores, deberían utilizarse sin modificación. Cuando un paquete de software necesite ser modificado los siguientes puntos deberían considerarse:

a) el riesgo de comprometer los procesos de control y de integridad incorporados;

b) si se requiere consentimiento del vendedor;

c) la posibilidad de obtener por parte del vendedor los cambios requeridos como actualizaciones estándar del programa;

d) el impacto, si la organización se hace responsable por el futuro mantenimiento del software como consecuencia de los cambios;

e) la compatibilidad con otro software en uso.

Si los cambios son necesarios, el software original sería ser conservado y los cambios ser aplicados a una copia claramente identificada. Un proceso de gestión de actualización de software debería ponerse en práctica para asegurarse de que los parches más recientes aprobados y las actualizaciones de aplicación sean instalados para todo el software autorizado. Todos los cambios deberían ser totalmente probados y documentados, de modo que ellos puedan volverse a aplicar, si fuera necesario a futuras actualizaciones de software. De ser requerido, las modificaciones deberían probarse y validarse por un equipo de evaluación independiente.

Principios de ingeniería de sistemas seguros
Principios de ingeniería de sistemas seguros deberían ser establecidos, documentados, mantenidos y aplicados a todos los esfuerzos de implementación de sistemas de información.

Los procedimientos de la ingeniería de sistemas de información seguros basados en los principios de ingeniería de seguridad, deberían establecerse, documentarse y aplicarse a las actividades internas de ingeniería de sistemas de información. La seguridad debería diseñarse en todas las capas de arquitectura (negocios, datos, aplicaciones y tecnología) equilibrando la necesidad de seguridad de la información con la necesidad de la accesibilidad. Debería analizarse la nueva tecnología para los riesgos de seguridad y el diseño debería revisarse contra patrones de ataque conocidos.

Estos principios y procedimientos de ingeniería establecidos deberían revisarse regularmente, para asegurarse de que estén contribuyendo eficazmente a mejorar normas de seguridad dentro del proceso de ingeniería. Estos también deberían revisarse periódicamente para asegurarse de que permanezcan actualizados en cuanto a la lucha contra las nuevas amenazas potenciales y que sigan siendo aplicables a los avances en las tecnologías y soluciones a ser aplicadas.

Los principios establecidos de ingeniería de la seguridad deberían aplicarse, cuando corresponda, por medio de contratos, a los sistemas de información subcontratados, así como de otros acuerdos vinculantes entre la organización y el proveedor que contrata la organización. La organización debería confirmar que el rigor de los principios de ingeniería de seguridad de los proveedores sea comparable con el propio.

Ambiente de desarrollo seguro
Las organizaciones deberían establecer y proteger adecuadamente los ambientes de desarrollo seguros para el desarrollo del sistema y los esfuerzos de integración de sistemas que cubren todo el ciclo de vida de desarrollo del sistema.

Un ambiente de desarrollo seguro incluye personas, procesos y tecnología asociados con el desarrollo y la integración de los sistemas.

Las organizaciones deberían evaluar los riesgos asociados con los esfuerzos de desarrollo de sistemas individuales y establecer ambientes de desarrollo seguro para esfuerzos de desarrollo de sistemas específicos, considerando:

a) sensibilidad de los datos a ser procesados, almacenados y transmitidos por el sistema;

b) requisitos externos e internos aplicables, por ejemplo, de reglamentos o políticas;

c) los controles de seguridad ya implementados por la organización que apoyan el desarrollo del sistema;

d) la confiabilidad del personal que trabaja en el ambiente;

e) el grado de contratación externa asociado con el desarrollo del sistema;

f) la necesidad de separación entre los diferentes ambientes de desarrollo;

g) el control de acceso al ambiente de desarrollo;

h) seguimiento al cambio en el ambiente y al código ahí almacenado;

i) los respaldos sean almacenados en ubicaciones seguras fuera de las instalaciones;

j) el control sobre el movimiento de los datos desde y hacia este ambiente.

Una vez que el nivel de protección es determinado para un ambiente de desarrollo específico, las organizaciones deberían documentar los procesos correspondientes de los procedimientos de desarrollo seguro y proporcionarlos a todas las personas que los necesiten.

Desarrollo contratado externamente
La organización debería supervisar y dar seguimiento a las actividades de desarrollo de sistemas contratadas externamente.

Cuando el desarrollo del sistema es contratado externamente, deberían considerarse los siguientes puntos en toda la cadena de suministro externa de la organización:

a) los acuerdos de licencias, la propiedad del código y los derechos de propiedad intelectual relacionado con el contenido contratado externamente;

b) los requisitos contractuales para el diseño, la codificación y las prácticas de pruebas seguros;

c) el suministro al desarrollador externo del modelo de amenazas aprobado;

d) las pruebas de aceptación para la calidad y precisión de los entregables;

e) la provisión de evidencias de que se utilizaron umbrales de seguridad para establecer los niveles mínimos aceptables de seguridad y calidad de la privacidad;

f) la provisión de evidencias de que se han revisado suficientes pruebas para proteger contra la presencia de contenido malicioso intencional y no intencional en la entrega;

g) la provisión de evidencias de que se han aplicado suficientes pruebas para protegerse contra la presencia de vulnerabilidades conocidas;

h) los acuerdos de custodia, por ejemplo, si el código fuente ya no está disponible por más tiempo;

i) el derecho contractual de auditar procesos y controles de desarrollo;

j) la documentación efectiva del ambiente construido utilizado para crear los entregables;

k) la organización sigue siendo responsable de cumplir con las leyes aplicables y la verificación de la eficacia del control.

Pruebas de seguridad de sistemas
Las pruebas de funcionalidad de la seguridad se deberían llevar a cabo durante el desarrollo.

Los sistemas nuevos y actualizados requieren pruebas exhaustivas y verificación durante los procesos de desarrollo, incluyendo la preparación de un calendario detallado de actividades y las entradas de pruebas y las salidas esperadas bajo un rango de condiciones.

En cuanto a los desarrollos internos, tales pruebas deberían realizarse inicialmente por parte del equipo de desarrollo. Deberían realizarse pruebas de aceptación independientes (tanto para el desarrollo interno, como para el contratado externamente) para asegurarse de que el sistema funciona tal y como se esperaba. El alcance de las pruebas debería ser proporcional a la importancia y naturaleza del sistema.

Pruebas de aceptación del sistema
Programas de pruebas de aceptación y los criterios relacionados deberían ser establecidos para los nuevos sistemas de información, las actualizaciones y las nuevas versiones.

Las pruebas de aceptación del sistema deberían incluir las pruebas de los requisitos de seguridad de la información y la adhesión a las prácticas de desarrollo de sistemas seguros. Las pruebas también deberían ser llevadas a cabo en los componentes recibidos y sistemas integrados. Las organizaciones pueden aprovechar las herramientas automatizadas, tales como las herramientas

de análisis de códigos o escáneres de vulnerabilidad, y deberían verificar la corrección de los defectos relacionados con la seguridad.

Las pruebas deberían realizarse en un ambiente de prueba realista para asegurarse de que el sistema no va a presentar vulnerabilidades en el ambiente de la organización y que las pruebas sean fiables.

Datos de prueba

Tiene como objetivo el asegurar la protección de los datos utilizados para la prueba.

Protección de los datos de prueba

Los datos de prueba deberían ser cuidadosamente seleccionados, protegidos y controlados.

Debería evitarse el uso de los datos de producción que contengan información personal identificable o cualquier otra información confidencial para fines de prueba. Si se utiliza información personal identificable o cualquier otra información confidencial para propósitos de hacer pruebas, todos los detalles y el contenido sensible deberían protegerse por eliminación o modificación.

Las directrices siguientes deberían aplicarse para proteger datos de producción cuando son utilizados con propósitos de pruebas:

a) los procedimientos de control de acceso, que se aplican a sistemas de aplicaciones en producción, deberían aplicarse también a los sistemas de prueba de aplicaciones;

b) debería autorizarse por separado, cada vez que se copie la información de producción a un ambiente de prueba;

c) debería borrarse la información de producción de un sistema de prueba de aplicación inmediatamente después de que las pruebas sean completadas;

d) la copia y uso de la información en producción debería registrarse en bitácora para proporcionar una pista de auditoría.