ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

INTRODUCCIÓN Y ANTECEDENTES

Los sistemas de información incluyen sistemas operativos, infraestructura, aplicaciones del negocio, productos de vitrina, servicios y aplicaciones desarrolladas para usuarios. El diseño y la implementación del sistema de información que da soporte a los procesos del negocio pueden ser cruciales para la seguridad. Se deberían identificar y acordar los requisitos de seguridad antes del desarrollo y / o la implementación de los sistemas de información.

Todos los requisitos de seguridad se deberían identificar en la fase de requisitos de un proyecto y se deberían justificar, acordar y documentar como parte de todo el caso del negocio para un sistema de información.

Se deberían validar los datos de entrada a las aplicaciones para asegurar que dichos datos son correctos y apropiados.

OBJETIVOS

El objetivo es evitar errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones.

Se deberían diseñar controles apropiados en las aplicaciones, incluyendo las aplicaciones desarrolladas por el usuario para garantizar el procesamiento correcto. Estos controles deberían incluir la validación de los datos de entrada, del procesamiento interno y de los datos de salida.

Garantizar que la seguridad es parte integral de los sistemas de información.

Requisitos de seguridad de los sistemas.

Dentro de los sistemas de información se incluyen los sistemas operativos, infraestructuras, aplicaciones de negocio, aplicaciones estándar o de uso generalizado, servicios y aplicaciones desarrolladas por los usuarios.

El diseño e implantación de los sistemas de información que sustentan los procesos de negocio pueden ser cruciales para la seguridad. Los requisitos de seguridad deberían ser identificados y consensuados previamente al desarrollo y/o implantación de los sistemas de información.

Todos los requisitos de seguridad deberían identificarse en la fase de recogida de requisitos de un proyecto y ser justificados, aceptados y documentados como parte del proceso completo para un sistema de información.

Análisis y especificación de los requisitos de seguridad

Las demandas de nuevos sistemas de información para el negocio o mejoras de los sistemas ya existentes deberían especificar los requisitos de los controles de seguridad.

Posibles Soluciones a este control:

Applipedia	Base de datos proporcionada en abierto por Palo Alto Network Research y su equipo de investigación para que aprender más sobre el nivel de riesgo de las aplicaciones que utilizan la red. El equipo de investigación continuamente actualiza las aplicaciones (mediante una tecnología pendiente de patente) el tráfico de la clasificación, con aplicaciones nuevas y emergentes a una tasa promedio de cuatro por semana. La base de datos identifica cada aplicación además de ofrecer una descripción de la aplicación, los puertos que utiliza, características de comportamiento, entre otros.
CSIRT Comunitat Valenciana	Informes sobre realizados por CSIRT-CV con guías para la configuración segura de servicios como Dropbox o dispositivos móviles entre otros.
ENISA	El presente documento en español permite realizar una evaluación informada de los riesgos y ventajas para la seguridad que presenta el uso de la computación en nube, y ofrece orientaciones sobre protección para los usuarios actuales y futuros de la computación en nube.
FFIEC	Guía del FFIEC (Federal Financial Institutions Examination Council), en inglés, sobre cómo implantar un proceso de desarrollo y adquisición de TI eficaz en una organización. La acompaña una lista de verificación -checklist-, útil para auditar dicho proceso.

ISO	ISO/IEC 21827 es la norma, en inglés, que especifica el "Systems Security Engineering - Capability Maturity Model", que describe las características esenciales del proceso de ingeniería de seguridad en una organización. ISO/IEC 21827 no prescribe un proceso o secuencia particular, sino que recoge las prácticas generales del sector.
Métrica 3	La metodología MÉTRICA Versión 3 ofrece a las organizaciones un instrumento útil para la sistematización de las actividades que dan soporte al ciclo de vida del software. Está promovida por el Gobierno español.
NIST	El documento publicado resume la justificación de un Protocolo de Uso (EUP) de la Historia Clínica Electrónica (EHR) y describe los procedimientos para la evaluación del diseño y pruebas de rendimiento de los usuarios de estos sistemas.
OWASP	La guía de desarrollo de OWASP (Open Web Application Security Project) ayuda a crear aplicaciones web seguras. Disponible también en español.

Seguridad de las comunicaciones en servicios accesibles por redes públicas.

El diseño e implantación de los sistemas de información que sustentan los procesos de negocio pueden ser cruciales para la seguridad. Los requisitos de seguridad deberían ser identificados y consensuados previamente al desarrollo y/o implantación de los sistemas de información.

Todos los requisitos de seguridad deberían identificarse en la fase de recogida de requisitos de un proyecto y ser justificados, aceptados y documentados como parte del proceso completo para un sistema de información.

Trabaje estrechamente con las unidades de negocio para desarrollar un negocio electronico seguro, incorporando requisitos de seguridad de la información en los proyectos, y con ello en los sistemas de comercio electrónico, desde el principio (también en cualquier cambio/actualización posterior).

Análisis y especificación de los requisitos de seguridad: Los requisitos relacionados con la seguridad de la información se deberían incluir en los requisitos para los nuevos sistemas o en las mejoras a los sistemas de información ya existentes.

Seguridad de las comunicaciones en servicios accesibles por redes públicas: La información de los servicios de aplicación que pasan a través de redes públicas se deberían proteger contra actividades fraudulentas, de disputa de contratos y/o de modificación no autorizada.

Protección de las transacciones por redes telemáticas: La información en transacciones de servicios de aplicación se debería proteger para evitar la transmisión y enrutamiento incorrecto y la alteración, divulgación y/o duplicación no autorizada de mensajes o su reproducción.

Seguridad en los procesos de desarrollo y soporte

Se deberían controlar estrictamente los entornos de desarrollo de proyectos y de soporte.

Los directivos responsables de los sistemas de aplicaciones deberían ser también responsables de la seguridad del proyecto o del entorno de soporte. Ellos deberían garantizar que todas las propuestas de cambio en los sistemas son revisadas para verificar que no comprometen la seguridad del sistema o del entorno operativo.

"Estado de la seguridad en sistemas en desarrollo", es decir, un informe sobre el estado actual de la seguridad en los procesos de desarrollo de software, con comentarios sobre incidentes recientes/actuales, vulnerabilidades actuales de seguridad conocidas y pronósticos sobre cualquier riesgo creciente, etc.

* Procedimientos de control de cambios

Se debería controlar la implantación de cambios mediante la aplicación de procedimientos formales de control de cambios.

OCS Inventory NG	OCS Inventory es una herramienta gratuita de creación automática de inventarios de HW, escaneo de red y distribución de paquetes de software.
Genos Open Source	GMF es una implementación de las recomendaciones ITIL (IT Infrastructure Library) para la gestión de servicios de TI (IT Service Management o ITSM). GMF es un producto de software libre distribuido bajo licencia GPL e incluye módulos de gestión de incidencias (Trouble Ticketing), gestión de inventario, gestión del cambio (Change Management), SLA y reporting.
Distribución de SW	Diversas herramientas de pago de distribución de paquetes de software en una red: Altiris, Enteo NetInstall, Microsoft System Center Configuration Manager.

Revisión técnica de los cambios en el sistema operativo

Se deberían revisar y probar las aplicaciones críticas de negocio cuando se realicen cambios en el sistema operativo, con objeto de garantizar que no existen impactos adversos para las actividades o seguridad de la Organización

Restricciones en los cambios a los paquetes de software

Se debería desaconsejar la modificación de los paquetes de software, restringiéndose a lo imprescindible y todos los cambios deberían ser estrictamente controlados.

Pruebas de funcionalidad durante el desarrollo de los sistemas.

Se deberían seleccionar, proteger y controlar cuidadosamente los datos utilizados para las pruebas.

Durante la fase de construcción del sistema, el Equipo de Proyecto realizará pruebas que verifiquen que el código está libre de errores.

Pruebas unitarias. Conjunto de pruebas que comprueban el correcto funcionamiento de cada componente de código por separado. Esto sirve para asegurar que cada uno de los módulos funcione correctamente por separado. Posteriormente, con las pruebas de integración, se podrá asegurar el correcto funcionamiento del sistema o subsistema en cuestión. Para la ejecución de las pruebas unitarias se deberá utilizar una herramienta que automatice el proceso, por ejemplo, JUnit. Se propone la siguiente plantilla como ayuda a la definición de las pruebas unitarias.
Pruebas de integración. Conjunto de pruebas que verifican la correcta integración entre todos los componentes/módulos del sistema. La necesidad de realizar las pruebas de integración viene dada por el hecho de que los módulos que forman un programa suelen fallar cuando trabajan de forma conjunta, aunque previamente se haya demostrado que funcionan correctamente de manera individual. Por ello se deberán realizar este tipo de pruebas, las cuáles asegurarán que los módulos que están relacionados se ejecutan correctamente. Con el uso de estas pruebas, se conseguirá formar el producto global a medida que se comprueba como los distintos componentes interaccionan y se comunican libres de errores. Para automatizar las pruebas de integración se pueden emplear las mismas herramientas que para las pruebas unitarias (por ejemplo, JUnit), pero los casos de pruebas por regla general serán más largos y la verificación de resultados puede requerir más de una comprobación. Se propone la siguiente plantilla como ayuda a la definición de las pruebas de integración.
Pruebas de código estático. Son verificaciones de código estático que todo programador debe realizar en su código para evitar errores de compilación, ejecución durante las fases posteriores. Un alto porcentaje de las pruebas se podrán automatizar en herramientas.

Datos de prueba

El objetivo es asegurar la protección de los datos usados para pruebas.

Protección de datos de prueba.

Datos de ensayo: seleccionados, protegidos y controlados cuidadosamente.
Evitar usar información confidencial para pruebas.
Los sistemas de aplicación de pruebas deben contar con controles de acceso.
La información operacional del ambiente de pruebas debe borrase después de las pruebas.