MNEMO

Anexo 14

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO

Dentro de esta área se localizan los siguientes objetivos y principios, controles y posibles mediciones asociadas:

A8.33	Información utilizada en las pruebas
Objetivo	La información utilizada para las pruebas debería ser seleccionada, protegida y gestionada adecuadamente
Principios	Garantizar la pertinencia de las pruebas y la protección de la información operativa utilizada para las mismas. Se deberían diseñar controles apropiados en las propias aplicaciones, incluidas las desarrolladas por los propios usuarios, para asegurar el procesamiento correcto de la información. Estos controles deberían incluir la validación de los datos de entrada, el tratamiento interno y los datos de salida. Podrían ser requeridos controles adicionales para los sistemas que procesan o tienen algún efecto en activos de información de carácter sensible, valioso o crítico. Dichos controles deberían ser determinados en función de los requisitos de seguridad y la estimación del riesgo.
Información	Siempre que sea posible, utilice librerías y funciones estándar para necesidades corrientes como validación de datos de entrada, restricciones de rango y tipo, integridad referencial, etc. Para mayor confianza con datos vitales, construya e incorpore funciones adicionales de validación y chequeo cruzado (p. ej., sumas totalizadas de control). Desarrolle y use herramientas -y habilidades- de prueba automatizadas y manuales, para comprobar cuestiones habituales como desbordamientos de memoria, inyección SQL, etc. La información de las pruebas debe seleccionarse para garantizar la fiabilidad de los resultados de las pruebas y la confidencialidad de la información operativa pertinente. La información sensible

A8.33	Información utilizada en las pruebas
	(incluida la información de identificación personal) no debe copiarse en los entornos de desarrollo y pruebas (véase 8.31). Las pruebas del sistema y de aceptación pueden requerir volúmenes importantes de información de prueba que se acerquen lo más posible a la información operativa.
Medición	Porcentaje de sistemas para los cuales los controles de validación de datos se han (a) definido y (b) implementado y demostrado eficaces mediante pruebas.

A8.25	Ciclo de vida del desarrollo seguro
Objetivo	Deberían ser establecidas y aplicadas normas para el desarrollo seguro de software y sistemas
Principios	Garantizar que la seguridad de la información se diseñe e implemente dentro del ciclo de vida de desarrollo seguro de software y sistemas. 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.
Información	Incorpore la seguridad de la información al ciclo de vida de desarrollo de sistemas en todas sus fases, desde la concepción hasta la desaparición de un sistema, por medio de la inclusión de "recordatorios" sobre seguridad en los procedimientos y métodos de desarrollo, operaciones y gestión de cambios.

A8.25	Ciclo de vida del desarrollo seguro
	Trate el desarrollo e implementación de software como un proceso de cambio. Integre las mejoras de seguridad en las actividades de gestión de cambios (p. ej., documentación y formación procedimental para usuarios y administradores). El desarrollo seguro es un requisito para construir un servicio, una arquitectura, un software y un sistema seguros. Para lograrlo, deben tenerse en cuenta los siguientes aspectos a) la separación de los entornos de desarrollo, prueba y producción (véase 8.31) b) orientación sobre la seguridad en el ciclo de vida del desarrollo de software: 1) la seguridad en la metodología de desarrollo de software (véanse los apartados 8.28 y 8.27) 2) directrices de codificación segura para cada lenguaje de programación utilizado (véase 8.28) c) requisitos de seguridad en la fase de especificación y diseño (véase 5.8) d) los puntos de control de seguridad en los proyectos (véase 5.8) e) las pruebas de sistema y de seguridad, como las pruebas de regresión, el escaneo de código y las pruebas de penetración (véase 8.29); f) los repositorios seguros para el código fuente y la configuración (véase 8.4 y 8.9) g) seguridad en el control de versiones (véase 8.32); h) los conocimientos y la formación necesarios en materia de seguridad de las aplicaciones (véase el apartado 8.28) i) la capacidad de los desarrolladores para prevenir, encontrar y solucionar las vulnerabilidades (véase 8.28) j) requisitos de licencia y alternativas para garantizar soluciones rentables y evitar futuros j) los requisitos de licencia y las alternativas para garantizar soluciones rentables y evitar futuros problemas de licencia (véase 5.32).

A8.25	Ciclo de vida del desarrollo seguro
	Si el desarrollo se subcontrata, la organización debe obtener garantías de que el proveedor cumple con las normas de la organización para el desarrollo seguro (véase 8.30). El desarrollo también puede tener lugar dentro de las aplicaciones, como las aplicaciones ofimáticas, los scripts, los navegadores y las bases de datos.
Medición	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

A8.27	Principios de ingeniería y arquitectura de sistemas seguros
Objetivo	Los principios para la ingeniería de sistemas seguros deberían estar establecidos, documentados, mantenidos y aplicados a cualquier actividad de desarrollo de sistemas de información
Principios	Garantizar que los sistemas de información se diseñan, implementan y operan de forma segura dentro del ciclo de vida del desarrollo. 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.

A8.27	Principios de ingeniería y arquitectura de sistemas seguros
Información	Incorpore la seguridad de la información al ciclo de vida de desarrollo de sistemas en todas sus fases, desde la concepción hasta la desaparición de un sistema, por medio de la inclusión de "recordatorios" sobre seguridad en los procedimientos y métodos de desarrollo, operaciones y gestión de cambios. Trate el desarrollo e implementación de software como un proceso de cambio. Integre las mejoras de seguridad en las actividades de gestión de cambios (p. ej., documentación y formación procedimental para usuarios y administradores). Los principios de ingeniería de seguridad deben establecerse, documentarse y aplicarse a las actividades de ingeniería de los sistemas de información. La seguridad debe diseñarse en todas las capas de la arquitectura (negocio, datos, aplicaciones y tecnología). La nueva tecnología debe ser analizada para detectar los riesgos de seguridad y el diseño debe ser revisado contra los patrones de ataque conocidos. Los principios de la ingeniería de seguridad proporcionan orientación sobre las técnicas de autenticación de usuarios, el control de sesiones seguras y la validación y saneamiento de datos.
Medición	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.

A8.29	Pruebas de seguridad en desarrollo y su aceptación
Objetivo	Los procesos de pruebas de seguridad deberían estar definidas e implementadas en el ciclo de vida del desarrollo

A8.29	Pruebas de seguridad en desarrollo y su aceptación
Principios	Validar si se cumplen los requisitos de seguridad de la información cuando las aplicaciones o el código se despliegan en el entorno de producción. 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.
Información	Incorpore la seguridad de la información al ciclo de vida de desarrollo de sistemas en todas sus fases, desde la concepción hasta la desaparición de un sistema, por medio de la inclusión de "recordatorios" sobre seguridad en los procedimientos y métodos de desarrollo, operaciones y gestión de cambios. Trate el desarrollo e implementación de software como un proceso de cambio. Integre las mejoras de seguridad en las actividades de gestión de cambios (p. ej., documentación y formación procedimental para usuarios y administradores). Los nuevos sistemas de información, las actualizaciones y las nuevas versiones deben probarse y verificarse a fondo durante los procesos de desarrollo. Las pruebas de seguridad deben ser una parte integral de las pruebas de los sistemas o componentes. Las pruebas de seguridad deben realizarse en función de un conjunto de requisitos, que pueden expresarse como funcionales o no funcionales. Las pruebas de seguridad deben incluir la comprobación de a) las funciones de seguridad [por ejemplo, la autenticación de usuarios (véase 8.5), la restricción de acceso (véase 8.3) y el uso de criptografía (véase 8.24)]; b) la codificación segura (véase 8.28)

A8.29	Pruebas de seguridad en desarrollo y su aceptación
	c) las configuraciones seguras (véanse los apartados 8.9, 8.20 y 8.22), incluidas las de los sistemas operativos, los cortafuegos y otros componentes de seguridad. Las pruebas deben realizarse en un entorno de pruebas que se ajuste lo más posible al entorno de producción objetivo para garantizar que el sistema no introduce vulnerabilidades en el entorno de la organización y que las pruebas son fiables (véase 8.31).
Medición	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

A8.30	Desarrollo subcontratado
Objetivo	La organización debería dirigir, monitorear y revisar las actividades relacionadas con el desarrollo de sistemas subcontratados.
Principios	Garantizar la aplicación de las medidas de seguridad de la información requeridas por la organización en el desarrollo de sistemas subcontratados. 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.

A8.30	Desarrollo subcontratado
Información	Cuando se subcontrata el desarrollo de sistemas, la organización debe comunicar y acordar los requisitos y expectativas, y supervisar y revisar continuamente si la entrega del trabajo subcontratado cumple con estas expectativas. Los siguientes puntos deben ser considerados en toda la cadena de suministro externa de la organización: a) acuerdos de licencia, propiedad del código y derechos de propiedad intelectual relacionados con el contenido externalizado contenido subcontratado (véase 5.32); b) requisitos contractuales para el diseño seguro, la codificación y las prácticas de prueba (véanse los apartados 8.25 a 8.29) c) provisión del modelo de amenazas a considerar por los desarrolladores externos; d) pruebas de aceptación de la calidad y la precisión de los resultados (véase 8.29); e) suministro de pruebas de que se han establecido niveles mínimos aceptables de capacidades de seguridad y privacidad (por ejemplo, informes de garantía) f) presentación de pruebas de que se han realizado pruebas suficientes para evitar la presencia de contenido malicioso (tanto intencionado como no intencionado) en el momento de la entrega g) presentación de pruebas de que se han realizado pruebas suficientes para evitar la presencia de vulnerabilidades conocidas; h) acuerdos de custodia para el código fuente del software (por ejemplo, si el proveedor quiebra); i) derecho contractual a auditar los procesos y controles de desarrollo; j) requisitos de seguridad para el entorno de desarrollo (véase 8.31) k) consideración de la legislación aplicable (por ejemplo, sobre protección de datos personales). Puede encontrar más información sobre las relaciones con los proveedores en la serie ISO/IEC 27036.

A8.30	Desarrollo subcontratado
Medición	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

A8.31	Separación de entornos de desarrollo, prueba y producción
Objetivo	Los entornos de desarrollo, prueba y producción deberían estar separados y protegidos.
Principios	Proteger el entorno de producción y los datos del peligro que suponen las actividades de desarrollo y prueba. 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.
Información	Documente procedimientos, normas y directrices de seguridad de la información, además de roles y responsabilidades, identificadas en el manual de política de seguridad de la organización. Debe identificarse y aplicarse el nivel de separación entre los entornos de producción, pruebas y desarrollo que sea necesario para evitar problemas de producción.

A8.31	Separación de entornos de desarrollo, prueba y producción
	Una sola persona no debe tener la capacidad de realizar cambios tanto en el desarrollo como en la producción sin una revisión y aprobación previas. Esto puede lograrse, por ejemplo, mediante la segregación de los derechos de acceso o mediante reglas que se supervisen. En situaciones excepcionales, deben aplicarse medidas adicionales, como el registro detallado y la supervisión en tiempo real, para detectar los cambios no autorizados y actuar en consecuencia. En algunos casos, la distinción entre los entornos de desarrollo, prueba y producción puede difuminarse deliberadamente y las pruebas pueden llevarse a cabo en un entorno de desarrollo o mediante despliegues controlados a usuarios o servidores en vivo (por ejemplo, una pequeña población de usuarios piloto). En algunos casos, las pruebas del producto pueden realizarse mediante el uso en vivo del producto dentro de la organización. Además, para reducir el tiempo de inactividad de los despliegues en vivo, se puede dar soporte a dos entornos de producción idénticos en los que sólo uno esté en vivo en un momento dado. Son necesarios procesos de apoyo para el uso de datos de producción en entornos de desarrollo y pruebas (8.33). Las organizaciones también pueden tener en cuenta las orientaciones proporcionadas en esta sección para los entornos de formación cuando realicen la formación de los usuarios finales.
Medición	Métricas de madurez de procesos TI relativos a seguridad, tales como el semiperiodo de aplicación de parches de seguridad (tiempo que ha llevado parchear al menos la mitad de los sistemas vulnerables -esta medida evita la cola variable provocada por los pocos sistemas inevitables que permanecen sin parchear por no ser de uso diario, estar normalmente fuera de la oficina o cualquier otra razón-). Estado de la seguridad en sistemas en desarrollo", es decir, un informe sobre el estado actual de la seguridad en los procesos de

A8.31	Separación de entornos de desarrollo, prueba y producción
	desarrollo de software, con comentarios sobre incidentes recientes/actuales, vulnerabilidades actuales de seguridad conocidas y pronósticos sobre cualquier riesgo creciente, etc.

A8.32	Gestión del cambio
Objetivo	Los cambios en las instalaciones de procesamiento de la información y en los sistemas de información deberían estar sujetos a procedimientos de gestión del cambio
Principios	Para preservar la seguridad de la información al ejecutar cambios.
Información	Documente procedimientos, normas y directrices de seguridad de la información, además de roles y responsabilidades, identificadas en el manual de política de seguridad de la organización. La introducción de nuevos sistemas y de cambios importantes en los sistemas existentes debe seguir unas normas acordadas y un proceso formal de documentación, especificación, pruebas, control de calidad y aplicación gestionada. Deben establecerse responsabilidades y procedimientos de gestión para garantizar un control satisfactorio de todos los cambios. Los procedimientos de control de cambios deben documentarse y aplicarse para garantizar la confidencialidad, la integridad y la disponibilidad de la información en las instalaciones de procesamiento de la información y los sistemas de información, para todo el ciclo de vida de desarrollo del sistema, desde las primeras etapas de diseño hasta todos los esfuerzos de mantenimiento posteriores. Los cambios en el software pueden afectar al entorno de producción y viceversa.

A8.32	Gestión del cambio
	Las buenas prácticas incluyen la prueba de los componentes de las TIC en un entorno separado de los entornos de producción y desarrollo (véase 8.31). Esto proporciona un medio para tener control sobre el nuevo software y permite una protección adicional de la información operativa que se utiliza para las pruebas. Esto debería incluir parches, paquetes de servicio y otras actualizaciones. El entorno de producción incluye los sistemas operativos, las bases de datos y las plataformas de middleware. El control debe aplicarse a los cambios de aplicaciones e infraestructuras. Incorpore la seguridad de la información al ciclo de vida de desarrollo de sistemas en todas sus fases, desde la concepción hasta la desaparición de un sistema, por medio de la inclusión de "recordatorios" sobre seguridad en los procedimientos y métodos de desarrollo, operaciones y gestión de cambios. Trate el desarrollo e implementación de software como un proceso de cambio. Integre las mejoras de seguridad en las actividades de gestión de cambios (p. ej., documentación y formación procedimental para usuarios y administradores).
Medición	Métricas de madurez de procesos TI relativos a seguridad, tales como el semiperiodo de aplicación de parches de seguridad (tiempo que ha llevado parchear al menos la mitad de los sistemas vulnerables -esta medida evita la cola variable provocada por los pocos sistemas inevitables que permanecen sin parchear por no ser de uso diario, estar normalmente fuera de la oficina o cualquier otra razón-). 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