MNEMO

Anexo 12

SEGURIDAD EN LAS OPERACIONES

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

A5.37	Procedimientos operativos documentados
Objetivo	Los procedimientos operativos para las instalaciones de procesamiento de información deben documentarse y ponerse a disposición del personal que los necesite.
Principios	Garantizar el funcionamiento correcto y seguro de las instalaciones de tratamiento de la información. Se deberían establecer responsabilidades y procedimientos para la gestión y operación de todos los recursos para el tratamiento de la información. Esto incluye el desarrollo de instrucciones apropiadas de operación y de procedimientos de respuesta ante incidencias. Se implantará la segregación de tareas, cuando sea adecuado, para reducir el riesgo de un mal uso del sistema deliberado o por negligencia. Se realizarán las proyecciones a futuro de la infraestructura actual con el fin de garantizar su rendimiento y disponibilidad. Es importante hacer una distinción entre los equipos de desarrollo, pruebas y operación con el fin de reducir riesgos en cuanto a acceso no autorizado o cambios no autorizados en los ambientes de producción. Se debe contemplar el control de cambios en general sobre procesos de negocio, instalaciones y sistemas específicos
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.

A5.37	Procedimientos operativos documentados
	Deben prepararse procedimientos documentados para las actividades operativas de la organización asociadas a la seguridad de la información, por ejemplo a) cuando la actividad debe ser realizada de la misma manera por muchas personas; b) cuando la actividad se realiza con poca frecuencia y cuando la próxima vez que se realice es probable que se haya olvidado el procedimiento c) cuando la actividad es nueva y presenta un riesgo si no se realiza correctamente d) antes de traspasar la actividad a personal nuevo. Los procedimientos operativos documentados deben ser revisados y actualizados cuando sea necesario. Los cambios en los procedimientos operativos documentados deben ser autorizados. Siempre que sea técnicamente posible, los sistemas de información deben gestionarse de forma coherente, utilizando los mismos procedimientos, herramientas y utilidades.
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-).

A8.6	Gestión de la capacidad
Objetivo	El uso de los recursos debería ser monitoreado y ajustado en función de las necesidades de capacidad actuales y previstas
Principios	Garantizar la capacidad necesaria de instalaciones de procesamiento de información, recursos humanos, oficinas y otras instalaciones. Se deberían establecer responsabilidades y procedimientos para la gestión y operación de todos los recursos para el tratamiento de la información. Esto incluye el desarrollo de instrucciones apropiadas de operación y de procedimientos de respuesta ante incidencias. Se implantará la segregación de tareas, cuando sea adecuado, para reducir el riesgo de un mal uso del sistema deliberado o por negligencia. Se realizarán las proyecciones a futuro de la infraestructura actual con el fin de garantizar su rendimiento y disponibilidad. Es importante hacer una distinción entre los equipos de desarrollo, pruebas y operación con el fin de reducir riesgos en cuanto a acceso no autorizado o cambios no autorizados en los ambientes de producción. Se debe contemplar el control de cambios en general sobre procesos de negocio, instalaciones y sistemas específicos.
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. El ajuste y la supervisión del sistema deben aplicarse para garantizar y, cuando sea necesario, mejorar la disponibilidad y la eficiencia de los sistemas. La organización debe realizar pruebas de estrés de los sistemas y servicios para confirmar que se dispone de suficiente capacidad del sistema para satisfacer los requisitos de rendimiento máximo.

A8.6	Gestión de la capacidad
	Deben establecerse controles de detección para indicar los problemas a tiempo. Las proyecciones de las futuras necesidades de capacidad deben tener en cuenta las nuevas necesidades de la empresa y del sistema, así como las tendencias actuales y previstas en las capacidades de procesamiento de la información de la organización. Hay que prestar especial atención a los recursos con largos plazos de adquisición o costes elevados. Por lo tanto, los gestores y los propietarios de servicios o productos deben supervisar la utilización de los recursos clave del sistema. Los gestores deben utilizar la información sobre la capacidad para identificar y evitar las posibles limitaciones de recursos y la dependencia del personal clave que puedan suponer una amenaza para la seguridad del sistema o los servicios, y planificar las medidas adecuadas. Para más detalles sobre la elasticidad y la escalabilidad de la computación en nube, véase ISO/IEC TS 23167.
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-).

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. 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

A8.31	Separación de entornos de desarrollo, prueba y producción
	(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 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. 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.

A8.32	Gestión del cambio
	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.

A8.7	Protección contra malware
Objetivo	La protección contra los programas maliciosos debería ser implementada y complementada con una adecuada concienciación de los usuarios.
Principios	Garantizar la protección de la información y otros activos asociados contra el malware. Se requieren ciertas precauciones para prevenir y detectar la introducción de código malicioso y códigos móviles no autorizados. El software y los recursos de tratamiento de información son vulnerables a la introducción de software malicioso como virus informáticos, gusanos de la red, caballos de Troya y bombas lógicas. Los usuarios deberían conocer los peligros que puede ocasionar el software malicioso o no autorizado y los administradores deberían introducir controles y medidas especiales para detectar o evitar su introducción.
Información	Combine controles tecnológicos (p. ej., software antivirus) con medidas no técnicas (educación, concienciación y formación). ¡No sirve de mucho tener el mejor software antivirus del mercado si los empleados siguen abriendo e-mails de remitentes desconocidos o descargando ficheros de sitios no confiables. No siempre es posible instalar un software que proteja contra el malware en algunos sistemas (por ejemplo, algunos sistemas de control industrial). Algunas formas de malware infectan los sistemas operativos y el firmware de los ordenadores de tal manera que los controles comunes de malware no pueden limpiar el sistema y es necesario volver a crear una imagen completa del software del sistema operativo y, a veces, del firmware del ordenador para volver a un estado seguro.
Medición	Tendencia en el número de virus, gusanos, troyanos o spam detectados y bloqueados. Número y costes acumulados de incidentes por software malicioso.

A8.13	Respaldo de la información
Objetivo	Las copias de seguridad de la información, de los programas informáticos y de los sistemas deberían ser mantenidos y probados periódicamente de acuerdo con la política específica acordada sobre copias de seguridad
Principios	Para permitir la recuperación de la pérdida de datos o sistemas. Se deberían establecer procedimientos rutinarios para conseguir la estrategia aceptada de para realizar copias de seguridad y probar su puntual recuperación.
Información	Implante procedimientos de backup y recuperación que satisfagan no sólo requisitos contractuales sino también requisitos de negocio "internos" de la organización. Básese en la evaluación de riesgos realizada para determinar cuáles son los activos de información más importantes y use esta información para crear su estrategia de backup y recuperación. Hay que decidir y establecer el tipo de almacenamiento, soporte a utilizar, aplicación de backup, frecuencia de copia y prueba de los soportes. Cifre copias de seguridad y archivos que contengan datos sensibles o valiosos (en realidad, serán prácticamente todos porque, si no, ¿para qué hacer copias de seguridad?). Las medidas de respaldo para los sistemas y servicios individuales deben probarse regularmente para garantizar que cumplen los objetivos de los planes de respuesta a incidentes y de continuidad del negocio (véase 5.30). Esto debe combinarse con una prueba de los procedimientos de restauración y cotejarse con el tiempo de restauración requerido por el plan de continuidad del negocio. En el caso de los sistemas y servicios críticos, las medidas de copia de seguridad deben cubrir toda la información de los sistemas, las aplicaciones y los datos necesarios para recuperar el sistema completo en caso de desastre.

A8.13	Respaldo de la información
	Cuando la organización utilice un servicio en la nube, deben realizarse copias de seguridad de la información, las aplicaciones y los sistemas de la organización en el entorno del servicio en la nube. La organización debe determinar si se cumplen los requisitos de copia de seguridad, y cómo, cuándo se utiliza el servicio de copia de seguridad de la información proporcionado como parte del servicio en la nube. Debe determinarse el período de conservación de la información empresarial esencial, teniendo en cuenta cualquier requisito de conservación de copias de archivo. La organización debe considerar la eliminación de la información (véase 8.10) en los medios de almacenamiento utilizados para las copias de seguridad una vez que el período de retención de la información haya expirado y debe tener en cuenta la legislación y la normativa.
Medición	Porcentaje de operaciones de backup exitosas. Porcentaje de recuperaciones de prueba exitosas. Tiempo medio transcurrido desde la recogida de los soportes de backup de su almacenamiento fuera de las instalaciones hasta la recuperación exitosa de los datos en todas ubicaciones principales. Porcentaje de backups y archivos con datos sensibles o valiosos que están encriptados

A8.15	Inicio de sesión
Objetivo	Los registros grabados de actividades, excepciones, fallas y cualquier otro evento relevante deberían ser generados, guardados, protegidos y analizados
Principios	Para registrar eventos, generar pruebas, garantizar la integridad de la información de registro, prevenir contra el acceso no autorizado,

A8.15	Inicio de sesión
	identificar eventos de seguridad de la información que puedan conducir a un incidente de seguridad de la información y apoyar las investigaciones. Se deben registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información. Los dispositivos de registro y la información del registro deben estar protegidos contra manipulaciones indebidas y accesos no autorizados Se deben registrar, proteger y revisar regularmente las actividades del administrador del sistema y del operador del sistema. Los sistemas deberían ser monitoreados y los eventos de la seguridad de información registrados. El registro de los operadores y el registro de fallos deberían ser usados para garantizar la identificación de los problemas del sistema de información. La organización debería cumplir con todos los requerimientos legales aplicables para el monitoreo y el registro de actividades. El monitoreo del sistema debería ser utilizado para verificar la efectividad de los controles adoptados y para verificar la conformidad del modelo de política de acceso.
Información	El viejo axioma del aseguramiento de la calidad "no puedes controlar lo que no puedes medir o monitorizar" es también válido para la seguridad de la información. La necesidad de implantar procesos de supervisión es más evidente ahora que la medición de la eficacia de los controles se ha convertido en un requisito específico. Analice la criticidad e importancia de los datos que va a monitorizar y cómo esto afecta a los objetivos globales de negocio de la organización en relación a la seguridad de la información. Los incidentes de seguridad de la información presuntos y reales deben ser identificados (por ejemplo, infección de malware o sondeo de cortafuegos) y ser objeto de una investigación posterior

A8.15	Inicio de sesión
	(por ejemplo, como parte de un proceso de gestión de incidentes de seguridad de la información, véase 5.25). Puede ser necesario archivar algunos registros de auditoría debido a los requisitos de retención de datos o a los requisitos de recopilación y conservación de pruebas (véase 5.28). Cuando la organización necesite enviar registros del sistema o de la aplicación a un proveedor para ayudar a depurar o solucionar errores, los registros deben ser desidentificados cuando sea posible utilizando técnicas de enmascaramiento de datos (véase 8.11) para información como nombres de usuario, direcciones de protocolo de Internet (IP), nombres de host o nombre de la organización, antes de enviarlos al proveedor. Los registros de eventos pueden contener datos sensibles e información personal identificable. Deben tomarse las medidas adecuadas de protección de la privacidad (véase 5.34). En los entornos de nube, las responsabilidades de gestión de registros pueden ser compartidas entre el cliente del servicio de nube y el proveedor de servicios de nube. Las responsabilidades varían en función del tipo de servicio en la nube que se utilice. En la norma ISO/IEC 27017 se pueden encontrar más orientaciones.
Medición	Porcentaje de sistemas cuyos logs de seguridad: (a) están adecuadamente configurados, (b) son transferidos con seguridad a un sistema de gestión centralizada de logs y (c) son monitorizados/revisados/evaluados regularmente. Tendencia en el número de entradas en los logs de seguridad que (a) han sido registradas, (b) han sido analizadas y (c) han conducido a actividades de seguimiento.

A8.17	Sincronización de los relojes
Objetivo	Los relojes de los sistemas de procesamiento de información utilizados por la organización deberían estar sincronizados con las fuentes de tiempo aprobadas.
Principios	Permitir la correlación y el análisis de eventos relacionados con la seguridad y otros datos registrados, y apoyar las investigaciones sobre incidentes de seguridad de la información. Es necesario revisar periódicamente las actividades de los usuarios incluyendo administradores y operadores de los sistemas y que todos los relojes de los sistemas estén debidamente sincronizados para contar con evidencias y registros precisos en tiempo.
Información	El viejo axioma del aseguramiento de la calidad "no puedes controlar lo que no puedes medir o monitorizar" es también válido para la seguridad de la información. Los requisitos externos e internos para la representación del tiempo, la sincronización fiable y la precisión deben documentarse y aplicarse. Dichos requisitos pueden provenir de necesidades legales, estatutarias, reglamentarias, contractuales, normativas y de control interno. Debe definirse y considerarse una hora de referencia estándar para su uso dentro de la organización para todos los sistemas, incluidos los sistemas de gestión de edificios, los sistemas de entrada y salida y otros que puedan utilizarse para ayudar en las investigaciones. Como reloj de referencia para los sistemas de registro debe utilizarse un reloj vinculado a una emisión horaria por radio de un reloj atómico nacional o un sistema de posicionamiento global (GPS); una fuente de fecha y hora coherente y de confianza que garantice la exactitud de las marcas horarias. Deben utilizarse protocolos como el protocolo de tiempo de red (NTP) o el protocolo de tiempo de precisión (PTP) para mantener todos los sistemas en red sincronizados con un reloj de referencia.

A8.17	Sincronización de los relojes
	La organización puede utilizar dos fuentes de tiempo externas al mismo tiempo para mejorar la fiabilidad de los relojes externos y gestionar adecuadamente cualquier variación. El ajuste correcto de los relojes de los ordenadores es importante para garantizar la exactitud de los registros de eventos, que pueden ser necesarios para las investigaciones o como prueba en casos legales y disciplinarios. Los registros de auditoría inexactos pueden obstaculizar dichas investigaciones y dañar la credibilidad de dichas pruebas.
Medición	Porcentaje de sistemas cuyos logs de seguridad: (a) están adecuadamente configurados, (b) son transferidos con seguridad a un sistema de gestión centralizada de logs y (c) son monitorizados/revisados/evaluados regularmente. Tendencia en el número de entradas en los logs de seguridad que (a) han sido registradas, (b) han sido analizadas y (c) han conducido a actividades de seguimiento.

A8.19	Instalación de software en los sistemas operativos
Objetivo	Deberían ser implementados procedimientos y medidas para gestionar de forma segura la instalación de software en los sistemas operativos.
Principios	Garantizar la integridad de los sistemas operativos y evitar la explotación de las vulnerabilidades técnicas. La organización debería aplicar procedimientos para controlar la instalación de software en los sistemas operativos.
Información	Para gestionar de forma segura los cambios y la instalación de software en los sistemas operativos, deben tenerse en cuenta las siguientes directrices

A8.19	Instalación de software en los sistemas operativos
	a) realizar las actualizaciones del software operativo únicamente por parte de administradores capacitados previa autorización de la dirección (véase 8.5); b) garantizar que sólo se instala en los sistemas operativos código ejecutable aprobado y no código de desarrollo o compiladores c) instalar y actualizar el software sólo después de haber realizado pruebas exhaustivas y satisfactorias (véanse los apartados 8.29 y 8.31) d) actualizar todas las bibliotecas de fuentes de programas correspondientes e) utilizar un sistema de control de la configuración para mantener el control de todo el software operativo, así como de la documentación del sistema f) definir una estrategia de reversión antes de aplicar los cambios g) mantener un registro de auditoría de todas las actualizaciones del software operativo h) archivar las versiones antiguas de los programas informáticos, junto con toda la información y los parámetros necesarios, los procedimientos, los detalles de configuración y los programas informáticos de apoyo, como medida de contingencia, y durante todo el tiempo que el programa informático deba leer o procesar los datos archivados. La organización debe definir y aplicar normas estrictas sobre los tipos de software que los usuarios pueden instalar. El principio de mínimo privilegio debe aplicarse a la instalación de software en los sistemas operativos. La organización debe identificar qué tipos de instalaciones de software están permitidas (por ejemplo, actualizaciones y parches de seguridad para el software existente) y qué tipos de instalaciones están prohibidas (por ejemplo, software que es sólo para uso personal y software

A8.19	Instalación de software en los sistemas operativos
	cuyo origen es desconocido o sospechoso y por ello se considera potencialmente malicioso.). Estos privilegios deben concederse en función de las funciones de los usuarios afectados.
Medición	Coste del tiempo de inactividad debido al incumplimiento de los acuerdos de nivel de servicio. Evaluación del rendimiento de proveedores incluyendo la calidad de servicio, entrega, coste, etc. Porcentaje de cambios de riesgo bajo, medio, alto y de emergencia. Número y tendencia de cambios revertidos y rechazados frente a cambios exitosos. Porcentaje de sistemas (a) que deberían cumplir con estándares de seguridad básica o similar y (b) cuya conformidad con dichos estándares ha sido comprobada mediante benchmarking o pruebas.

A8.8	Gestión de vulnerabilidades técnicas
Objetivo	Se deberían obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se deberían evaluar la exposición de la organización a tales vulnerabilidades y se deberían tomar las medidas apropiadas.
Principios	Para evitar la explotación de las vulnerabilidades técnicas. Se debe obtener información acerca de las vulnerabilidades técnicas de los sistemas de información que se utilizan. Se debe medir la exposición de la organización a tales vulnerabilidades y aplicar las medidas adecuadas para hacer frente al riesgo asociado. Es importante establecer las normas que rigen la instalación de software por los usuarios.

A8.8	Gestión de vulnerabilidades técnicas
	Se deberían realizar revisiones regulares de la seguridad de los sistemas de información. Las revisiones se deberían realizar según las políticas de seguridad apropiadas y las plataformas técnicas y sistemas de información deberían ser auditados para el cumplimiento de los estándares adecuados de implantación de la seguridad y controles de seguridad documentados.
Información	Adopte procesos estructurados de planificación de capacidad TI, desarrollo seguro, pruebas de seguridad, etc., usando estándares aceptados como ISO 20000 (ITIL) donde sea posible. Defina e imponga estándares de seguridad básica (mínimos aceptables) para todas las plataformas de sistemas operativos, usando las recomendaciones de seguridad de CIS, NIST, NSA y fabricantes de sistemas operativos y, por supuesto, sus propias políticas de seguridad de la información. La organización debe contar con un inventario preciso de activos (véanse los puntos 5.9 a 5.14) como requisito previo para una gestión eficaz de la vulnerabilidad técnica; el inventario debe incluir el proveedor de software, el nombre del software, los números de versión, el estado actual de despliegue (por ejemplo, qué software está instalado en qué sistemas) y la(s) persona(s) dentro de la organización responsable(s) del software. Alinee los procesos de autoevaluación de controles de seguridad con las autoevaluaciones de gobierno corporativo, cumplimiento legal y regulador, etc., complementados por revisiones de la dirección y verificaciones externas de buen funcionamiento. Para más información relacionada con la gestión de las vulnerabilidades técnicas cuando se utiliza la computación en nube, véase la serie ISO/IEC 19086 y la ISO/IEC 27017. La norma ISO/IEC 29147 proporciona información detallada sobre la recepción de informes de vulnerabilidad y la publicación de avisos de vulnerabilidad. La norma ISO/IEC 30111 proporciona información

A8.8	Gestión de vulnerabilidades técnicas
	detallada sobre la gestión y resolución de las vulnerabilidades notificadas.
Medición	Porcentaje de cambios de riesgo bajo, medio, alto y de emergencia. Número y tendencia de cambios revertidos y rechazados frente a cambios exitosos. Porcentaje de sistemas (a) que deberían cumplir con estándares de seguridad básica o similar y (b) cuya conformidad con dichos estándares ha sido comprobada mediante benchmarking o pruebas. Número de cuestiones o recomendaciones de política interna y otros aspectos de cumplimiento, agrupadas y analizadas por su estado (cerradas, abiertas, nuevas, retrasadas) e importancia o nivel de riesgo (alto, medio o bajo). Porcentaje de revisiones de cumplimiento de seguridad de la información sin incumplimientos sustanciales.

A.8.34	Protección de los sistemas de información durante las pruebas de auditoría
Objetivo	Las pruebas de auditoría y otras actividades de garantía que impliquen la evaluación de los sistemas operativos deberían estar planificadas y acordadas entre el encargado de realizar las pruebas y la dirección correspondiente
Principios	Reducir al mínimo el impacto de las auditorías y otras actividades de garantía en los sistemas operativos y los procesos empresariales. Los Requisitos y actividades que implican la auditoria de los sistemas operativos deben ser cuidadosamente planificados y acordadas para reducir al mínimo las interrupciones en los procesos de negocio.

A.8.34	Protección de los sistemas de información durante las pruebas de auditoría
Información	Las siguientes pautas deben ser observadas: a) los requisitos de auditoría de acceso a los sistemas y datos deben prepararse con una gestión adecuada. b) el alcance de las pruebas técnicas de auditoría debería ser acordado y controlado. c) las pruebas de auditoría que requieran comprobaciones en los sistemas operativos deben ser planificadas con el fin de minimizar el riesgo en la operación de los procesos de negocio. d) el acceso debe ser monitoreado y registrado para producir una evidencia de auditoría. Las pruebas de auditoría y otras actividades de aseguramiento también pueden tener lugar en los sistemas de desarrollo y de prueba, donde dichas pruebas pueden afectar, por ejemplo, a la integridad del código o llevar a la divulgación de cualquier información sensible que se encuentre en dichos entornos.
Medición	Número de auditorías de sistemas y de aplicaciones por año. Comparativa con otros años.