# ANEXO A

UNE EN ISO /IEC 27001

| | | |
|---|---|---|
| **A.5 Políticas de seguridad de la información** | | |
| **A.5.1 Directrices de gestión de la seguridad de la información** | | |
| Objetivo: Proporcionar orientación y apoyo a la gestión de la seguridad de la información de acuerdo con los requisitos del negocio, las leyes y normativa pertinentes. | | |
| A.5.1.1 | Políticas para la seguridad de la información | *Control : Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes.* |
| A.5.1.2 | Revisión de las políticas para la seguridad de la información | Control: Las políticas de seguridad de la información deben revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia. |
| **A.6 Organización de la seguridad de la información** | | |
| **A.6.1 Organización interna** | | |
| Objetivo: Establecer un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización. | | |
| A.6.1.1 | Roles y responsabilidades en seguridad de la información | *Control*<br><br>Todas las responsabilidades en seguridad de la información deben ser definidas y asignadas. |
| A.6.1.2 | Segregación de tareas | *Control*<br><br>Las funciones y áreas de responsabilidad deben segregarse para reducir la posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de la organización. |
| A.6.1.3 | Contacto con las autoridades | |
| A.6.1.4 | Contacto con grupos de interés especial | *Control*<br><br>Deben mantenerse los contactos apropiados con grupos de interés especial, u otros foros y asociaciones profesionales especializados en seguridad. |
| A.6.1.5 | Seguridad de la información en la gestión de proyectos | *Control*<br><br>La seguridad de la información debe tratarse dentro de la gestión de proyectos, independientemente de la naturaleza del proyecto. |
| **A.6.2 Los dispositivos móviles y el teletrabajo** | | |
| Objetivo: Garantizar la seguridad en el teletrabajo y en el uso de dispositivos móviles. | | |
| A.6.2.1 | Política de dispositivos móviles | *Control*<br><br>Se debe adoptar una política y unas medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de dispositivos móviles. |
| A.6.2.2 | Teletrabajo | *Control*<br><br>Se debe implementar una política y unas medidas de seguridad adecuadas para proteger la información accedida, tratada o almacenada en emplazamientos de teletrabajo. |
| **A.7 Seguridad relativa a los recursos humanos** | | |
| **A.7.1 Antes del empleo** | | |
| Objetivo: Para asegurarse que los empleados y contratistas entiendan sus responsabilidades y son adecuados para las funciones para las que se consideran. | | |
| A.7.1.1 | Investigación de antecedentes | *Control*<br><br>La comprobación de los antecedentes de todos los candidatos al puesto de trabajo se debe llevar a cabo de acuerdo con las leyes, normativa y códigos éticos que sean de aplicación y debe ser proporcional a las necesidades del negocio, la clasificación de la información a la que se accede y los riesgos percibidos. |
| A.7.1.2 | Términos y condiciones del empleo | *Control*<br><br>Cómo parte de sus obligaciones contractuales, los empleados y contratistas deben establecer los términos y condiciones en su contrato de trabajo en lo que respecta a la seguridad de la información, tanto hacia el empleado como hacia la organización |
| **A.7.2 Durante el empleo** | | |
| Objetivo: Asegurar que los empleados y contratistas conozcan y cumplan con sus responsabilidades en seguridad de la información. | | |
| A.7.2.1 | Responsabilidades de gestión | *Control*<br><br>La dirección debe exigir a los empleados y contratistas, que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos en la organización. |
| A.7.2.2 | Concienciación, educación y capacitación en seguridad de la información | *Control*<br><br>Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo. |

| | | |
|---|---|---|
| **A.5 Políticas de seguridad de la información** | | |
| A.7.2.3 | Proceso disciplinario | *Control*<br><br>Debe existir un proceso disciplinario formal que haya sido comunicado a los empleados, que recoja las acciones a tomar ante aquellos que hayan provocado alguna brecha de seguridad. |
| **A.7.3 Finalización del empleo o cambio en el puesto de trabajo** | | |
| Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o finalización del empleo. | | |
| A.7.3.1 | Responsabilidades ante la finalización o cambio | *Control*<br><br>Las responsabilidades en seguridad de la información y obligaciones que siguen vigentes después del cambio o finalización del empleo se deben definir, comunicar al empleado o contratista y se deben cumplir. |
| **A.8 Gestión de activos** | | |
| **A.8.1 Responsabilidad sobre los activos** | | |
| Objetivo: Identificar los activos de la organización y definir las responsabilidades de protección adecuadas. | | |
| A.8.1.1 | Inventario de activos | *Control*<br><br>La información y otros activos asociados a la información y a los recursos para el tratamiento de la información deben estar claramente identificados y debe elaborarse y mantenerse un inventario. |
| A.8.1.2 | Propiedad de los activos | Control : Todos los activos que figuran en el inventario deben tener un propietario |
| A.8.1.3 | Uso aceptable de los activos | *Control*<br><br>Se deben identificar, documentar e implementar las reglas de uso aceptable de la información y de los activos asociados con los recursos para el tratamiento de la información. |
| A.8.1.4 | Devolución de activos | *Control*<br><br>Todos los empleados y terceras partes deben devolver todos los activos de la organización que estén en su poder al finalizar su empleo, contrato o acuerdo. |
| **A.8.2 Clasificación de la información** | | |
| Objetivo: Asegurar que la información reciba un nivel adecuado de protección de acuerdo con su importancia para la organización | | |
| A.8.2.1 | Clasificación de la información | *Control*<br><br>La información debe ser clasificada en términos de la importancia de su revelación frente a requisitos legales, valor, sensibilidad y criticidad ante revelación o modificación no autorizadas. |
| A.8.2.2 | Etiquetado de la información | *Control*<br><br>Debe desarrollarse e implantarse un conjunto adecuado de procedimientos para etiquetar la información, de acuerdo con el esquema de clasificación adoptado por la organización. |
| A.8.2.3 | Manipulado de la información | *Control*<br><br>Debe desarrollarse e implantarse un conjunto adecuado de procedimientos para la manipulación de la información, de acuerdo con el esquema de clasificación adoptado por la organización. |
| **A.8.3 Manipulación de los soportes** | | |
| Objetivo: Evitar la revelación, modificación, eliminación o destrucción no autorizadas de la información almacenada en soportes. | | |
| A.8.3.1 | Gestión de soportes extraíbles | *Control*<br><br>Se deben implementar procedimientos para la gestión de los soportes extraíbles, de acuerdo con el esquema de clasificación adoptado por la organización. |
| A.8.3.2 | Eliminación de soportes | *Control*<br><br>Los soportes deben eliminarse de forma segura cuando ya no vayan a ser necesarios, mediante procedimientos formales. |
| A.8.3.3 | Soportes físicos en tránsito | *Control*<br><br>Durante el transporte fuera de los límites físicos de la organización, los soportes que contengan información deben estar protegidos contra accesos no autorizados, usos indebidos o deterioro. |
| **A.9 Control de acceso** | | |
| **A.9.1 Requisitos de negocio para el control de acceso** | | |
| Objetivo: Limitar el acceso a los recursos de tratamiento de la información y a la información. | | |
| A.9.1.1 | Política de control de acceso | *Control*<br><br>Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información. |
| A.9.1.2 | Acceso a las redes y a los servicios de red | *Control*<br><br>Únicamente se debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados. |
| **A.9.2 Gestión de acceso de usuario** | | |
| Objetivo: Garantizar el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios | | |
| A.9.2.1 | Registro y baja de usuario | *Control*<br><br>Debe implantarse un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso. |

| | | |
|---|---|---|
| **A.5 Políticas de seguridad de la información** | | |
| A.9.2.2 | Provisión de acceso de usuario | *Control*<br><br>Debe implantarse un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios. |
| A.9.2.3 | Gestión de privilegios de acceso | Control: La asignación y el uso de privilegios de acceso debe estar restringida y control |
| A.9.2.4 | Gestión de la información secreta de autenticación de los usuarios | *Control*<br><br>La asignación de la información secreta de autenticación debe ser controlada a través de un proceso formal de gestión. |
| A.9.2.5 | Revisión de los derechos de acceso de usuario | *Control*<br><br>Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares. |
| A.9.2.6 | Retirada o reasignación de los derechos de acceso | *Control*<br><br>Los derechos de acceso de todos los empleados y terceras partes, a la información y a los recursos de tratamiento de la información deben ser retirados a la finalización del empleo, del contrato o del acuerdo, o ajustados en caso de cambio. |
| **A.9.3 Responsabilidades del usuario** | | |
| Objetivo: Para que los usuarios se hagan responsables de salvaguardar su información de autenticación. | | |
| A.9.3.1 | Uso de la información secreta de autenticación | *Control*<br><br>Se debe requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación. |
| **A.9.4 Control de acceso a sistemas y aplicaciones** | | |
| Objetivo: Prevenir el acceso no autorizado a los sistemas y aplicaciones. | | |
| A.9.4.1 | Restricción del acceso a la información | *Control*<br><br>Se debe restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida. |
| A.9.4.2 | Procedimientos seguros de inicio de sesión | Control Cuando así se requiera en la política de control de acceso, el acceso a los sistemas y a las aplicaciones se debe controlar por medio de un procedimiento seguro de inicio de sesión. |
| A.9.4.3 | Sistema de gestión de contraseñas | *Control*<br><br>Los sistemas para la gestión de contraseñas deben ser interactivos y establecer contraseñas seguras y robustas. |
| A.9.4.4 | Uso de utilidades con privilegios del sistema | *Control*<br><br>Se debe restringir y controlar rigurosamente el uso de utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación. |
| A.9.4.5 | Control de acceso al código fuente de los programas | *Control*<br><br>Se debe restringir el acceso al código fuente de los programas. |
| **A.10 Criptografía** | | |
| **A.10.1 Controles criptográficos** | | |
| Objetivo: Garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información. | | |
| A.10.1.1 | Política de uso de los controles criptográficos | *Control*<br><br>Se debe desarrollar e implementar una política sobre el uso de los controles criptográficos para proteger la información. |
| A.10.1.2 | Gestión de claves | *Control*<br><br>Se debe desarrollar e implementar una política sobre el uso, la protección y la duración de las claves de cifrado a lo largo de todo su ciclo de vida. |
| **A.11 Seguridad física y del entorno** | | |
| **A.11.1 Áreas seguras** | | |
| Objetivo: Prevenir el acceso físico no autorizado, los daños e interferencia a la información de la organización y a los recursos de tratamiento de la información. | | |
| A.11.1.1 | Perímetro de seguridad física | *Control*<br><br>Se deben utilizar perímetros de seguridad para proteger las áreas que contienen información sensible así como los recursos de tratamiento de la información. |
| A.11.1.2 | Controles físicos de entrada | *Control*<br><br>Las áreas seguras deben estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado. |
| A.11.1.3 | Seguridad de oficinas, despachos y recursos | *Control*<br><br>Para las oficinas, despachos y recursos, se debe diseñar y aplicar la seguridad física. |

| | | |
|---|---|---|
| **A.5 Políticas de seguridad de la información** | | |
| A.11.1.4 | Protección contra las amenazas externas y ambientales | *Control*<br><br>Se debe diseñar y aplicar una protección física contra desastres naturales, ataques provocados por el hombre o accidentes. |
| A.11.1.5 | El trabajo en áreas seguras | *Control*<br><br>Se deben diseñar e implementar procedimientos para trabajar en las áreas seguras. |
| A.11.1.6 | Áreas de carga y descarga | *Control*<br><br>Deben controlarse los puntos de acceso tales como las áreas de carga y descarga y otros puntos, donde pueda acceder personal no autorizado a las instalaciones, y si es posible, aislar dichos puntos de los recursos de tratamiento de la información para evitar accesos no autorizados. |
| **A.11.2 Seguridad de los equipos** | | |
| Objetivo: Evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la organización. | | |
| A.11.2.1 | Emplazamiento y protección de equipos | *Control*<br><br>Los equipos deben situarse o protegerse de forma que se reduzcan los riesgos de las amenazas y los riesgos ambientales así como las oportunidades de que se produzcan accesos no autorizados. |
| A.11.2.2 | Instalaciones de suministro | *Control*<br><br>Los equipos deben estar protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro. |
| A.11.2.3 | Seguridad del cableado | *Control*<br><br>El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información debe estar protegido frente a interceptaciones, interferencias o daños. |
| A.11.2.4 | Mantenimiento de los equipos | *Control*<br><br>Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad y su integridad continuas. |
| A.11.2.5 | Retirada de materiales propiedad de la empresa | *Control*<br><br>Sin autorización previa, los equipos, la información o el software no deben sacarse de las instalaciones. |
| A.11.2.6 | Seguridad de los equipos fuera de las instalaciones | *Control*<br><br>Deben aplicarse medidas de seguridad a los equipos situados fuera las instalaciones de la organización, teniendo en cuenta los diferentes riesgos que conlleva trabajar fuera de dichas instalaciones. |
| A.11.2.7 | Reutilización o eliminación segura de equipos | *Control*<br><br>Todos los soportes de almacenamiento deben ser comprobados para confirmar que todo dato sensible y software bajo licencia se ha eliminado de manera segura, antes de deshacerse de ellos. |
| A.11.2.8 | Equipo de usuario desatendido | *Control*<br><br>Los usuarios deben asegurarse que el equipo desatendido tiene la protección adecuada. |
| A.11.2.9 | Política de puesto de trabajo despejado y pantalla limpia | *Control*<br><br>Debe adoptarse una política de puesto de trabajo despejado de papeles y medios de almacenamiento desmontables y una política de pantalla limpia para los recursos de tratamiento de la información. |
| **A.12 Seguridad de las operaciones** | | |
| **A.12.1 Procedimientos y responsabilidades operacionales** | | |
| Objetivo: Asegurar el funcionamiento correcto y seguro de las instalaciones de tratamiento de la información. | | |
| A.12.1.1 | Documentación de procedimientos operacionales | *Control*<br><br>Deben documentarse y mantenerse procedimientos operacionales y ponerse a disposición de todos los usuarios que los necesiten. |
| A.12.1.2 | Gestión de cambios | *Control*<br><br>Los cambios en la organización, los procesos de negocio, instalaciones de tratamiento de la información y los sistemas que afectan a la seguridad de la información deben ser controlados. |
| A.12.1.3 | Gestión de capacidades | *Control*<br><br>Se debe supervisar y ajustar la utilización de los recursos, así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el rendimiento requerido del sistema. |
| A.12.1.4 | Separación de los recursos de desarrollo, prueba y operación | *Control*<br><br>Deben separarse los recursos de desarrollo, pruebas y operación, para reducir los riesgos de acceso no autorizado o los cambios del sistema en producción. |
| **A.12.2 Procedimientos y responsabilidades operacionales** | | |
| Objetivo: Asegurar que los recursos de tratamiento de información y la información están protegidas contra el *malware.* | | |
| A.12.2.1 | Controles contra el código malicioso | *Control*<br><br>Se deben implementar los controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso, así como procedimientos adecuados de concienciación al usuario. |
| **A.12.3 Copias de seguridad** | | |
| Objetivo: Evitar la pérdida de datos | | |
| A.12.3.1 | Copias de seguridad de la información | *Control*<br><br>Se deben realizar copias de seguridad de la información, del software y del sistema y se deben verificar periódicamente de acuerdo a la política de copias de seguridad acordada. |
| **A.12.4 Registro y supervisión.** | | |

| | | |
|---|---|---|
| **A.5 Políticas de seguridad de la información** | | |
| Objetivo: Registrar eventos y generar evidencias. | | |
| A.12.4.1 | Registro de eventos | *Control*<br><br>Se deben registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información. |
| A.12.4.2 | Protección de la información del registro | *Control*<br><br>Los dispositivos de registro y la información del registro deben estar protegidos contra manipulaciones indebidas y accesos no autorizados. |
| A.12.4.3 | Registros de administración y operación | *Control*<br><br>Se deben registrar, proteger y revisar regularmente las actividades del administrador del sistema y del operador del sistema. |
| A.12.4.4 | Sincronización del reloj | *Control*<br><br>Los relojes de todos los sistemas de tratamiento de la información dentro de una organización o de un dominio de seguridad, deben estar sincronizados con una única fuente de tiempo precisa y acordada. |
| **A.12.5 Control de software de explotación.** | | |
| Objetivo: Asegurar la integridad del software en explotación. | | |
| A.12.4.5 | Instalación del software en explotacion | *Control*<br><br>Se deben implementar procedimientos para controlar la instalación del software en explotación. |
| **A.12.6 Gestion de la vulnerabilidad técnica.** | | |
| Objetivo: Reducir los riesgos resultantes de la explotacion de las vulnerabilidades técnicas. | | |
| A.12.6.1 | Gestión de las vulnerabilidades técnicas | *Control*<br><br>Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado. |
| A.12.6.2 | Restricción en la instalación de software | *Control*<br><br>Se deben establecer y aplicar reglas que rijan la instalación de software por parte de los usuarios. |
| **A.12.7 Consideraciones sobre la auditoria de sistemas de información** | | |
| Objetivo: Minimizar el impacto de las actividades de auditoría en los sistemas operativos. | | |
| A.12.7.1 | Controles de auditoría de sistemas de información | *Control*<br><br>Los requisitos y las actividades de auditoría que impliquen comprobaciones en los sistemas operativos deben ser cuidadosamente planificados y acordados para minimizar el riesgo de interrupciones en los procesos de negocio. |
| **A.13 Seguridad de las comunicaciones** | | |
| **A.13.1 Gestión de la seguridad de las redes** | | |
| Objetivo: Asegurar la protección de la información en las redes y los recursos de tratamiento de la información. | | |
| A.13.1.1 | Controles de red | Control<br>Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones. |
| A.13.1.2 | Seguridad de los servicios de red | Control<br>Se deben identificar los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deben incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan. |
| A.13.1.3 | Segregación en redes | Control<br>Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en redes distintas. |
| **A.13.2 Intercambio de información.** | | |
| Objetivo: Mantener la seguridad de la información que se transfiere dentro de una organización y con cualquier entidad externa. | | |
| A.13.2.1 | Políticas y procedimientos de intercambio de información | Control<br>Deben establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación. |
| A.13.2.2 | Acuerdos de intercambio de información | Control<br>Deben establecerse acuerdos para el intercambio seguro de información del negocio y software entre la organización y terceros. |
| A.13.2.3 | Mensajeria electrónica | Control<br>La información que sea objeto de mensajería electrónica debe estar adecuadamente protegida. |
| A.13.2.4 | Acuerdos de confidencialidad o no revelación | Control<br>Deben identificarse, documentarse y revisarse regularmente los requisitos de los acuerdos de confidencialidad o no revelación |
| **A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información** | | |
| **A.14.1 Requisitos de seguridad en los sistemas de información** | | |
| Objetivo: Garantizar 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. | | |
| A.14.1.1 | Análisis de requisitos y especificaciones de seguridad de la información | Control<br>Los requisitos relacionados con la seguridad de la información deben incluirse en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes. |
| A.14.1.2 | Asegurar los servicios de aplicaciones en redes públicas | Control<br>La información involucrada en aplicaciones que pasan a través de redes públicas debe ser protegida de cualquier actividad fraudulenta, disputa de contrato, revelación y modificación no autorizadas. |
| A.14.1.3 | Protección de las transacciones de servicios de aplicaciones | Control<br>La información involucrada en las transacciones de servicios de aplicaciones debe ser protegida para prevenir la transmisión incompleta, errores de enrutamiento, alteración no autorizada del mensaje, revelación, duplicación, o reproducción de mensaje no autorizadas. |
| **A.14.2 Seguridad en el desarrollo y en los procesos de soporte** | | |
| Objetivo: Garantizar la seguridad de la información que se ha diseñado e implementado en el ciclo de vida de desarrollo de los sistemas de información. | | |
| A.14.2.1 | Política de desarrollo seguro | Control<br>Se deben establecer y aplicar reglas dentro de la organización para el desarrollo de aplicaciones y sistemas. |

| A.5 Políticas de seguridad de la información | | |
|---|---|---|
| A.14.2.2 | Procedimiento de control de cambios en sistemas | Control<br>La implantación de cambios a lo largo del ciclo de vida del desarrollo debe controlarse mediante el uso de procedimientos formales de control de cambios. |
| A.14.2.3 | Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo | Control<br>Cuando se modifiquen los sistemas operativos, las aplicaciones de negocio críticas deben ser revisadas y probadas para garantizar que no existen efectos adversos en las operaciones o la seguridad de la organización. |
| A.14.2.4 | Restricciones a los cambios en los paquetes de software | Control<br>Se deben desaconsejar las modificaciones en los paquetes de software, limitándose a los cambios necesarios, y todos los cambios deben ser objeto de un control riguroso. |
| A.14.2.5 | Principios de ingeniería de sistemas seguros | Control<br>Principios de ingeniería de sistemas seguros se deben establecer, documentar, mantener y aplicarse a todos los esfuerzos de implementación de sistemas de información. |
| A.14.2.6 | Entorno de desarrollo seguro | Control<br>Las organizaciones deben establecer y proteger adecuadamente los entornos de desarrollo seguro para el desarrollo del sistema y los esfuerzos de integración que cubren todo el ciclo de vida de desarrollo del sistema. |
| A.14.2.7 | Externalización del desarrollo de software | Control<br>El desarrollo de software externalizado debe ser supervisado y controlado por la organización. |
| A.14.2.8 | Pruebas funcionales de seguridad de sistemas | Control<br>Se deben llevar a cabo pruebas de la seguridad funcional durante el desarrollo. |
| A.14.2.9 | Pruebas de aceptación de sistemas | Control<br>Se deben establecer programas de pruebas de aceptación y criterios relacionados para nuevos sistemas de información, actualizaciones y nuevas versiones. |
| **A.14.3 Datos de prueba** | | |
| Objetivo: Asegurar la protección de los datos de prueba | | |
| A.14.3.1 | Protección de los datos de prueba | Control<br>Los datos de prueba se deben seleccionar con cuidado y deben ser protegidos y controlados. |
| **A.14.5 Relación con proveedores** | | |
| **A.15.1 Seguridad en las relaciones con proveedores** | | |
| Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores. | | |
| A.15.1.1 | Política de seguridad de la información en las relaciones con los proveedores | Control<br>Los requisitos de seguridad de la información para la mitigación de los riesgos asociados con el acceso del proveedor a los activos de la organización deben acordarse con el proveedor y quedar documentados. |
| A.15.1.2 | Requisitos de seguridad en contratos con terceros | Control<br>Todos los requisitos relacionados con la seguridad de la información deben establecerse y acordarse con cada proveedor que puede acceder, tratar, almacenar, comunicar, o proporcionar componentes de la infraestructura de Tecnología de la Información. |
| A.15.1.3 | Cadena de suministro de tecnología de la información y de las comunicaciones | Control<br>Los acuerdos con proveedores deben incluir requisitos para hacer frente a los riesgos de seguridad de la información relacionados con las tecnologías de la información y las comunicaciones y con la cadena de suministro de productos. |
| **A.15.2 Gestión de la provisión de servicios del proveedor** | | |
| Objetivo: Mantener un nivel acordado de seguridad y de provisión de servicios en línea con acuerdos con proveedores | | |
| A.15.2.1 | Control y revisión de la provisión de servicios del proveedor | Control<br>Las organizaciones deben controlar, revisar y auditar regularmente la provisión de servicios del proveedor |
| A.15.2.2 | Gestión de cambios en la provisión del servicio del proveedor | Control<br>Se deben gestionar los cambios en la provisión del servicio, incluyendo el mantenimiento y la mejora de las políticas, los procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos y sistemas de negocio afectados así como la re-apreciación de los riesgos. |
| **A.16 Gestión de incidentes de seguridad de la información** | | |
| **A.16.1 Gestión de incidentes de seguridad de la información y mejoras** | | |
| Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades. | | |
| A.16.1.1 | Responsabilidades y procedimientos | Control<br>Se deben establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información. |
| A.16.1.2 | Notificación de los eventos de seguridad de la información | Control<br>Los eventos de seguridad de la información se deben notificar por los canales de gestión adecuados lo antes posible. |
| A.16.1.3 | Notificación de puntos débiles de la seguridad | Control<br>Todos los empleados, contratistas, terceras partes usuarias de los sistemas y servicios de información deben ser obligados a anotar y notificar cualquier punto débil que observen o que sospechen que exista, en los sistemas o servicios. |
| A.16.1.4 | Evaluación y decisión sobre los eventos de seguridad de información | Control<br>Los eventos de seguridad de la información deben ser evaluados y debe decidirse si se clasifican como incidentes de seguridad de la información. |
| A.16.1.5 | Respuesta a incidentes de seguridad de la información | Control<br>Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados. |
| A.16.1.6 | Aprendizaje de los incidentes de seguridad de la información | Control<br>El conocimiento obtenido a partir del análisis y la resolución de incidentes de seguridad de la información debe utilizarse para reducir la probabilidad o el impacto de los incidentes en el futuro. |
| A.16.1.7 | Recopilación de evidencias | Control<br>La organización debe definir y aplicar procedimientos para la identificación recogida, adquisición y preservación de la información que puede servir de evidencia. |
| **A.17 Aspectos de seguridad de la información para la gestión de la continuidad de negocio** | | |
| **A.17.1 Continuidad de la seguridad de la información** | | |
| Objetivo: La continuidad de la seguridad de la información debe formar parte de los sistemas de gestión de la continuidad de negocio de la organización. | | |
| A.17.1.1 | Planificación de la continuidad de la seguridad de la información | Control<br>La organización debe determinar sus necesidades de seguridad de la información y de continuidad para la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre. |

| | | |
|---|---|---|
| **A.5 Políticas de seguridad de la información** | | |
| A.17.1.2 | Implementar la continuidad de la seguridad de la información. | Control<br>La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de la seguridad de la información durante una situación adversa. |
| A.17.1.3 | Verificación, revisión y evaluación de la continuidad de la seguridad de la información | Control<br>La organización debe comprobar los controles establecidos e implementados a intervalos regulares para asegurar que son válidos y eficaces durante situaciones adversas. |
| **A.17.2 Redundancias.** | | |
| Objetivo: Asegurar la disponibilidad de los recursos de tratamiento de la información. | | |
| A.17.2.1 | Disponibilidad de los recursos de tratamiento de la información | Control<br>Los recursos de tratamiento de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad |
| **A.18 Cumplimiento** | | |
| **A.18.1 Cumplimiento de los requisitos legales y contractuales** | | |
| Objetivo: Evitar incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relativas a la seguridad de la información o de los requisitos de seguridad. | | |
| A.18.1.1 | Identificación de la legislación aplicable y de los requisitos contractuales | Control<br>Todos los requisitos pertinentes, tanto legales como regulatorios, estatutarios o contractuales, y el enfoque de la organización para cumplirlos, deben definirse de forma explícita, documentarse y mantenerse actualizados para cada sistema de información de la organización. |
| A.18.1.2 | Derechos de Propiedad Intelectual (DPI) | Control<br>Deben implementarse procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, regulatorios y contractuales sobre el uso de materiales, con respecto a los cuales puedan existir derechos de propiedad intelectual y sobre el uso de productos de software patentados. |
| A.18.1.3 | Protección de los registros de la organización | Control<br>Los registros deben estar protegidos contra la pérdida, destrucción, falsificación, revelación o acceso no autorizados de acuerdo con los requisitos legales, regulatorios, contractuales y de negocio. |
| A.18.1.4 | Protección y privacidad de la información de carácter personal | Control<br>Debe garantizarse la protección y la privacidad de los datos, según se requiera en la legislación y la reglamentación aplicables. |
| A.18.1.5 | Regulación de los controles criptográficos | Control<br>Los controles criptográficos se deben utilizar de acuerdo con todos los contratos, leyes y regulaciones pertinentes. |
| **A.18.2 Revisiones de la seguridad de la información** | | |
| Objetivo: Garantizar que la seguridad de la información se implementa y opera de acuerdo con las políticas y procedimientos de la organización. | | |
| A.18.2.1 | Revisión independiente de la seguridad de la información | Control<br>El enfoque de la organización para la gestión de la seguridad de la información y su implantación, es decir, objetivos de control, contr oles, políticas, procesos y procedimientos para la seguridad de la información, debe someterse a una revisión independiente a intervalos planificados o siempre que se produzcan cambios significativos en la implantación de la seguridad. |
| A.18.2.2 | Cumplimiento de las políticas y normas de seguridad | Control<br>Los directivos deben asegurarse que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente con el fin de cumplir las políticas y normas de seguridad y cualquier otro requisito de seguridad aplicable |
| A.18.2.3 | Comprobación del cumplimiento técnico | Control<br>Debe comprobarse periódicamente que los sistemas de información cumplen las políticas y normas de seguridad de la información de la organización. |