**Estado y Aplicabilidad de controles de Seguridad de la Información**

| Sección | Controles de Seguridad de la Información | Estado | Recursos | Descripción |
|---|---|---|---|---|
| **A5** | **Políticas de seguridad de la información** | | | |
| **A5.1** | **Directrices de gestión de la seguridad de la información** | | | |
| A5.1.1 | Políticas para la seguridad de la información | Definido | Personal de dirección, plantilla de políticas | Se han establecido políticas de seguridad de la información que abordan el acceso, la clasificación de datos y el uso activos de información. |
| A5.1.2 | Revisión de las políticas para la seguridad de la información | Administrado | Equipo de dirección, responsable de seguridad de la información | Las políticas son revisadas y actualizadas anualmente por el equipo de dirección en colaboración con el responsable de seguridad de la información. |
| **A6** | **Organización de la seguridad de la información** | | | |
| **A6.1** | **Organización interna** | | | |
| A6.1.1 | Roles y responsabilidades en seguridad de la información | Definido | Personal de dirección, responsable de seguridad de la información | Se han asignado roles y responsabilidades específicos para la gestión de la seguridad de la información. |
| A6.1.2 | Segregación de tareas | Repetible | Personal de dirección, equipo de TI | Se han establecido controles para la segregación de tareas entre el equipo de desarrollo, el equipo de operaciones y el equipo de seguridad de la información. |
| A6.1.3 | Contacto con las autoridades | Inicial | Responsable de seguridad de la información | Se están estableciendo procedimientos para el contacto con las autoridades en caso de incidentes de seguridad de la información. |
| A6.1.4 | Contacto con grupos de interés especial | Inicial | Equipo de dirección | Se están identificando y estableciendo relaciones con grupos de interés especial relacionados con la seguridad de la información, como asociaciones industriales y grupos de usuarios. |
| A6.1.5 | Seguridad de la información en la gestión de proyectos | Repetible | Equipo de dirección, equipo de desarrollo | Se han integrado consideraciones de seguridad de la información en la gestión de proyectos, incluida la evaluación de riesgos y la planificación de contingencias. |
| **A6.2** | **Los dispositivos móviles y el teletrabajo** | | | |
| A6.2.1 | Política de dispositivos móviles | Definido | Responsable de seguridad de la información, equipo de TI | Se ha establecido una política de dispositivos móviles que aborda el uso seguro de dispositivos móviles, incluida la autenticación, el cifrado y la gestión remota. |
| A6.2.2 | Teletrabajo | Inicial | Equipo de dirección, equipo de recursos humanos | Se están desarrollando pautas y procedimientos para el trabajo remoto, incluida la seguridad de la conexión remota y la protección de datos confidenciales. |
| **A7** | **Seguridad relativa a los recursos humanos** | | | |
| **A7.1** | **Antes del empleo** | | | |
| A7.1.1 | Investigación de antecedentes | Repetible | Equipo de recursos humanos | Se lleva a cabo una verificación de antecedentes para todos los nuevos empleados antes de su contratación. |
| A7.1.2 | Términos y condiciones del empleo | Definido | Equipo de recursos humanos, departamento legal | Se proporcionan a todos los empleados términos y condiciones de empleo que incluyen disposiciones relacionadas con la seguridad de la información y el cumplimiento de las políticas internas. |
| **A7.2** | **Durante el empleo** | | | |
| A7.2.1 | Responsabilidades de gestión | Definido | Supervisores, equipo de recursos humanos | Los supervisores tienen responsabilidades específicas relacionadas con la seguridad de la información de sus equipos, incluida la supervisión del cumplimiento de las políticas y la gestión de incidentes. |
| A7.2.2 | Concienciación, educación y capacitación en seguridad de la informació | Administrado | Equipo de recursos humanos, responsable de seguridad de la información | Se llevan a cabo programas de concienciación y formación en seguridad de la información para todos los empleados de forma regular. |
| A7.2.3 | Proceso disciplinario | Repetible | Equipo de recursos humanos, supervisores | Se han establecido procedimientos disciplinarios para abordar el incumplimiento de las políticas de seguridad de la información por parte de los empleados. |
| **A7.3** | **Finalización del empleo o cambio en el puesto de trabajo** | | | |
| A7.3.1 | Responsabilidades ante la finalización o cambio | Inicial | Equipo de recursos humanos, equipo de TI | Se están desarrollando procedimientos para la gestión segura de la finalización del empleo o los cambios en los puestos de trabajo, incluida la revocación de acceso y la devolución de activos de información. |
| **A8** | **Gestión de activos** | | | |
| **A8.1** | **Responsabilidad sobre los activos** | | | |
| A8.1.1 | Inventario de activos | Definido | Equipo de TI | Se mantiene un inventario actualizado de todos los activos de información, incluidos hardware, software y datos. |

| | | | | |
|---|---|---|---|---|
| A8.1.2 | Propiedad de los activos | Definido | Equipo de dirección, equipo de TI | Se ha asignado la propiedad de los activos de información a personas o departamentos específicos, y se han establecido procedimientos para su custodia y uso adecuado. |
| A8.1.3 | Uso aceptable de los activos | Administrado | Todos los empleados | Se han establecido políticas y procedimientos para el uso adecuado y seguro de los activos de información, incluidos los dispositivos móviles y los recursos en la nube. |
| A8.1.4 | Devolución de activos | Inicial | Equipo de recursos humanos, equipo de TI | Se están desarrollando procedimientos para la devolución segura de activos de información al finalizar el empleo o al cambiar de puesto de trabajo. |
| **A8.2** | **Clasificación de la información** | | | |
| A8.2.1 | Clasificación de la información | Definido | Equipo de seguridad de la información | Se ha establecido un sistema de clasificación de la información para identificar y proteger datos sensibles y críticos. |
| A8.2.2 | Etiquetado de la información | Definido | Equipo de seguridad de la información | Se aplican etiquetas de clasificación a todos los documentos y datos según el sistema de clasificación establecido. |
| A8.2.3 | Manipulado de la información | Repetible | Todos los empleados | Se han establecido controles para garantizar que la información se maneje de manera segura y conforme a las políticas de seguridad de la información. |
| **A8.3** | **Manipulación de los soportes** | | | |
| A8.3.1 | Gestión de soportes extraíbles | Inicial | Equipo de TI | Se están desarrollando políticas y procedimientos para la gestión segura de soportes extraíbles, como USB y discos duros externos. |
| A8.3.2 | Eliminación de soportes | Repetible | Equipo de TI | Se han establecido procedimientos para la eliminación segura de soportes de almacenamiento al finalizar su vida útil o al desecharlos. |
| A8.3.3 | Soportes físicos en tránsito | Repetible | Personal de entrega, equipo de TI | Se han establecido controles para proteger los soportes físicos de información durante el transporte, incluidas las medidas de seguridad física y el cifrado de datos. |
| **A9** | **Control de acceso** | | | |
| **A9.1** | **Requisitos de negocio para el control de acceso** | | | |
| A9.1.1 | Política de control de acceso | Definido | Equipo de seguridad de la información | Se ha establecido una política de control de acceso que define los requisitos y procedimientos para la gestión de acceso a sistemas y datos. |
| A9.1.2 | Acceso a las redes y a los servicios de red | Definido | Equipo de seguridad de la información | Se han implementado controles para gestionar y supervisar el acceso a las redes y servicios de red, incluido el uso de firewalls y sistemas de detección de intrusiones. |
| **A9.2** | **Gestión de acceso de usuario** | | | |
| A9.2.1 | Registro y baja de usuario | Definido | Equipo de TI, equipo de recursos humanos | Se han establecido procedimientos para la creación y eliminación segura de cuentas de usuario, incluida la revisión y aprobación por parte de la gestión. |
| A9.2.2 | Provisión de acceso de usuario | Repetible | Equipo de TI | Se han establecido controles para proporcionar acceso de usuario de acuerdo con los roles y responsabilidades definidos, incluida la autenticación de dos factores cuando sea posible. |
| A9.2.3 | Gestión de privilegios de acceso | Repetible | Equipo de TI | Se han establecido controles para gestionar y supervisar los privilegios de acceso, incluida la revisión regular de los privilegios asignados. |
| A9.2.4 | Gestión de la información secreta de autenticación de los usuarios | Definido | Equipo de TI | Se han implementado controles para proteger la información secreta de autenticación de los usuarios, incluidas las contraseñas y las claves de acceso. |
| A9.2.5 | Revisión de los derechos de acceso de usuario | Administrado | Equipo de TI, supervisores | Se realizan revisiones regulares de los derechos de acceso de usuario para garantizar que estén alineados con las necesidades del negocio y los principios de seguridad de la información. |
| A9.2.6 | Retirada o reasignación de los derechos de acceso | Repetible | Equipo de TI, supervisores | Se han establecido procedimientos para retirar o reasignar los derechos de acceso de usuario cuando ya no son necesarios o apropiados. |
| **A9.3** | **Responsabilidades del usuario** | | | |
| A9.3.1 | Uso de la información secreta de autenticación | Administrado | Todos los empleados | Se han establecido directrices para el uso seguro de la información secreta de autenticación, incluidas las contraseñas y las claves de acceso. |
| **A9.4** | **Control de acceso a sistemas y aplicaciones** | | | |

| | | | | |
|---|---|---|---|---|
| A9.4.1 | Restricción del acceso a la información | Definido | Equipo de TI | Se han establecido controles para restringir el acceso a la información confidencial y crítica según los principios de necesidad y menor privilegio. |
| A9.4.2 | Procedimientos seguros de inicio de sesión | Definido | Equipo de TI | Se han establecido procedimientos para el inicio de sesión seguro en sistemas y aplicaciones, incluida la autenticación multifactor cuando sea posible. |
| A9.4.3 | Sistema de gestión de contraseñas | Definido | Equipo de TI | Se ha implementado un sistema de gestión de contraseñas para garantizar la seguridad y el cumplimiento de las políticas de contraseña. |
| A9.4.4 | Uso de utilidades con privilegios del sistema | Repetible | Equipo de TI | Se controla y supervisa el uso de utilidades con privilegios del sistema para evitar el abuso y la explotación de vulnerabilidades. |
| A9.4.5 | Control de acceso al código fuente de los programas | Inicial | Equipo de desarrollo | Se están desarrollando controles para proteger el acceso al código fuente de los programas, incluida la autenticación y el control de versiones. |
| **A10** | **Criptografía** | | | |
| **A10.1** | **Controles criptográficos** | | | |
| A10.1.1 | Política de uso de los controles criptográficos | Definido | Equipo de seguridad de la información | Se ha establecido una política que define el uso adecuado de los controles criptográficos, incluida la gestión de claves y el cifrado de datos. |
| A10.1.2 | Gestión de claves | Repetible | Equipo de seguridad de la información | Se han implementado controles para la gestión de claves criptográficas, incluida la generación segura, el almacenamiento y el intercambio de claves. |
| **A11** | **Seguridad física y del entorno** | | | |
| **A11.1** | **Áreas seguras** | | | |
| A11.1.1 | Perímetro de seguridad física | Definido | Equipo de seguridad de la información, equipo de instalaciones | Se ha establecido un perímetro de seguridad física para proteger las instalaciones y los activos de la empresa contra amenazas externas. |
| A11.1.2 | Controles físicos de entrada | Definido | Personal de seguridad, equipo de instalaciones | Se han implementado controles físicos de entrada, como cerraduras electrónicas y sistemas de acceso con tarjeta, para regular el acceso a las instalaciones. |
| A11.1.3 | Seguridad de oficinas, despachos y recursos | Definido | Personal de seguridad, equipo de instalaciones | Se han implementado medidas de seguridad física en oficinas, despachos y áreas de recursos, incluido el control de acceso y la protección contra intrusos. |
| A11.1.4 | Protección contra las amenazas externas y ambientales | Definido | Equipo de seguridad de la información, equipo de instalaciones | Se han implementado controles para proteger las instalaciones y los activos contra amenazas externas y ambientales, como incendios, inundaciones y ataques físicos. |
| A11.1.5 | El trabajo en áreas seguras | Inicial | Personal autorizado, equipo de seguridad de la información | Se están desarrollando pautas y procedimientos para el trabajo seguro en áreas seguras, incluido el control de acceso y la protección de datos sensibles. |
| A11.1.6 | Áreas de carga y descarga | Inicial | Personal de logística, equipo de seguridad de la información | Se están estableciendo controles para garantizar la seguridad durante las operaciones de carga y descarga, incluida la supervisión y la protección de la información durante el transporte. |
| **A11.2** | **Seguridad de los equipos** | | | |
| A11.2.1 | Emplazamiento y protección de equipos | Definido | Equipo de TI, equipo de instalaciones | Se han implementado medidas de seguridad para proteger el emplazamiento y los equipos de tecnología de la información contra amenazas físicas y ambientales. |
| A11.2.2 | Instalaciones de suministro | Definido | Equipo de instalaciones | Se han implementado medidas de seguridad para proteger las instalaciones de suministro de energía y datos contra interrupciones y daños. |
| A11.2.3 | Seguridad del cableado | Definido | Equipo de instalaciones, equipo de TI | Se han implementado controles para garantizar la seguridad del cableado de red y la protección contra interferencias y accesos no autorizados. |
| A11.2.4 | Mantenimiento de los equipos | Repetible | Equipo de TI | Se han establecido procedimientos para el mantenimiento preventivo y correctivo de los equipos de tecnología de la información, incluida la aplicación oportuna de parches de seguridad. |
| A11.2.5 | Retirada de materiales propiedad de la empresa | Inicial | Equipo de TI, equipo de recursos humanos | Se están desarrollando procedimientos para la retirada segura de materiales propiedad de la empresa al finalizar su vida útil o al ser reemplazados. |
| A11.2.6 | Seguridad de los equipos fuera de las instalaciones | Inicial | Personal autorizado, equipo de TI | Se están estableciendo controles para proteger los equipos de tecnología de la información cuando se utilizan fuera de las instalaciones, incluidas las medidas de autenticación y el cifrado de datos. |

| | | | | |
|---|---|---|---|---|
| A11.2.7 | Reutilización o eliminación segura de equipos | Inicial | Equipo de TI, equipo de instalaciones | Se están desarrollando procedimientos para la reutilización o eliminación segura de equipos al finalizar su vida útil, incluida la destrucción segura de datos almacenados. |
| A11.2.8 | Equipo de usuario desatendido | Inicial | Equipo de TI, personal de seguridad | Se están estableciendo controles para proteger el equipo de usuario desatendido contra el acceso no autorizado y el robo de datos. |
| A11.2.9 | Política de puesto de trabajo despejado y pantalla limpia | Inicial | Equipo de TI, personal de seguridad | Se están desarrollando políticas para garantizar que los puestos de trabajo estén despejados y las pantallas estén bloqueadas cuando no estén en uso para proteger la información confidencial. |
| **A12** | **Seguridad de las operaciones** | | | |
| **A12.1** | **Procedimientos y responsabilidades operacionales** | | | |
| A12.1.1 | Documentación de procedimientos operacionales | Definido | Equipo de operaciones, equipo de seguridad de la información | Se han documentado y comunicado los procedimientos operacionales para garantizar la coherencia y la eficiencia en las operaciones de seguridad. |
| A12.1.2 | Gestión de cambios | Definido | Equipo de operaciones, equipo de seguridad de la información | Se ha establecido un proceso formal para la gestión de cambios, que incluye la evaluación de riesgos, la autorización y la documentación de los cambios realizados. |
| A12.1.3 | Gestión de capacidades | Definido | Equipo de operaciones, equipo de seguridad de la información | Se han implementado controles para gestionar la capacidad de los sistemas y aplicaciones, incluida la monitorización del rendimiento y la planificación de la capacidad futura. |
| A12.1.4 | Separación de los recursos de desarrollo, prueba y operación | Definido | Equipo de operaciones, equipo de desarrollo | Se han implementado controles para separar los entornos de desarrollo, prueba y operación para evitar interferencias y riesgos de seguridad. |
| **A12.2** | **Protección contra el software malicioso (malware)** | | | |
| A12.2.1 | Controles contra el código malicioso | Definido | Equipo de seguridad de la información, equipo de TI | Se han implementado controles para proteger los sistemas y aplicaciones contra el código malicioso, incluidos antivirus, firewalls y filtrado de contenido. |
| **A12.3** | **Copias de seguridad** | | | |
| A12.3.1 | Copias de seguridad de la información | Definido | Equipo de TI | Se han establecido procedimientos para realizar copias de seguridad de la información de forma regular y segura, incluida la rotación de medios y la comprobación de integridad. |
| **A12.4** | **Registros y supervisión** | | | |
| A12.4.1 | Registro de eventos | Definido | Equipo de seguridad de la información | Se han implementado sistemas de registro de eventos para capturar y almacenar registros de actividad que puedan ser relevantes para la seguridad de la información. |
| A12.4.2 | Protección de la información del registro | Definido | Equipo de seguridad de la información | Se han implementado controles para proteger la integridad y la confidencialidad de la información de registro, incluida la asignación de permisos de acceso y el cifrado de datos. |
| A12.4.3 | Registros de administración y operación | Definido | Equipo de seguridad de la información | Se mantienen registros de las actividades administrativas y operativas relacionadas con los sistemas y aplicaciones para fines de auditoría y cumplimiento. |
| A12.4.4 | Sincronización del reloj | Definido | Equipo de TI | Se han implementado controles para garantizar la sincronización precisa de los relojes de los sistemas y dispositivos para facilitar la correlación de eventos de registro. |
| **A12.5** | **Control del software en explotación** | | | |
| A12.5.1 | Instalación del software en explotación | Definido | Equipo de TI | Se han establecido procedimientos para la instalación segura de software en los entornos de producción, incluida la verificación de la fuente y la integridad del software. |
| **A12.6** | **Gestión de la vulnerabilidad técnica** | | | |
| A12.6.1 | Gestión de las vulnerabilidades técnicas | Definido | Equipo de seguridad de la información, equipo de TI | Se ha implementado un proceso para identificar, evaluar y mitigar las vulnerabilidades técnicas en los sistemas y aplicaciones, incluida la aplicación de parches de seguridad. |
| A12.6.2 | Restricción en la instalación de software | Definido | Equipo de TI | Se han establecido controles para restringir la instalación de software no autorizado en los sistemas y dispositivos para reducir el riesgo de vulnerabilidades y malware. |
| **A12.7** | **Consideraciones sobre la auditoria de sistemas de información** | | | |
| A12.7.1 | Controles de auditoría de sistemas de información | Definido | Equipo de seguridad de la información | Se han implementado controles para garantizar la integridad, confidencialidad y disponibilidad de los registros de auditoría de sistemas, incluida la protección contra modificaciones no autorizadas. |
| **A13** | **Seguridad de las comunicaciones** | | | |

| | | | | |
|---|---|---|---|---|
| **A13.1** | **Gestión de la seguridad de las redes** | | | |
| A13.1.1 | Controles de red | Definido | Equipo de seguridad de la información, equipo de TI | Se han implementado controles para proteger la infraestructura de red contra amenazas, incluido el filtrado de paquetes, la detección de intrusiones y la segmentación de red. |
| A13.1.2 | Seguridad de los servicios de red | Definido | Equipo de seguridad de la información, equipo de TI | Se han implementado controles para proteger los servicios de red contra amenazas, incluida la autenticación, la autorización y el cifrado de datos. |
| A13.1.3 | Segregación en redes | Definido | Equipo de seguridad de la información, equipo de TI | Se han establecido segmentos de red separados para aislar y proteger sistemas y datos sensibles de otros recursos no confiables. |
| **A13.2** | **Intercambio de información** | | | |
| A13.2.1 | Políticas y procedimientos de intercambio de información | Definido | Equipo de seguridad de la información | Se han establecido políticas y procedimientos para regular el intercambio seguro y eficiente de información entre partes internas y externas. |
| A13.2.2 | Acuerdos de intercambio de información | Definido | Equipo de seguridad de la información, equipo legal | Se han establecido acuerdos formales para regular el intercambio de información con partes externas, incluidos los requisitos de seguridad y privacidad. |
| A13.2.3 | Mensajería electrónica | Definido | Equipo de seguridad de la información | Se han implementado controles para proteger la mensajería electrónica contra amenazas, incluido el cifrado de correo electrónico y la detección de phishing. |
| A13.2.4 | Acuerdos de confidencialidad o no revelación | Definido | Equipo de seguridad de la información, equipo legal | Se han establecido acuerdos formales de confidencialidad o no revelación para proteger la información sensible compartida con partes externas. |
| **A14** | **Adquisición, desarrollo y mantenimiento de los sistemas de inform** | | | |
| **A14.1** | **Requisitos de seguridad en los sistemas de información** | | | |
| A14.1.1 | Análisis de requisitos y especificaciones de seguridad de la información | Definido | Equipo de seguridad de la información, equipo de desarrollo | Se han establecido procesos para analizar y especificar requisitos de seguridad de la información durante el ciclo de vida del desarrollo de sistemas. |
| A14.1.2 | Asegurar los servicios de aplicaciones en redes públicas | Definido | Equipo de seguridad de la información, equipo de desarrollo | Se han implementado controles para garantizar la seguridad de los servicios de aplicaciones que operan en redes públicas, incluido el cifrado de datos y la autenticación robusta. |
| A14.1.3 | Protección de las transacciones de servicios de aplicaciones | Definido | Equipo de seguridad de la información, equipo de desarrollo | Se han implementado controles para proteger las transacciones de servicios de aplicaciones contra amenazas, incluidas las técnicas de cifrado y la gestión de sesiones. |
| **A14.2** | **Seguridad en el desarrollo y en los procesos de soporte** | | | |
| A14.2.1 | Política de desarrollo seguro | Definido | Equipo de seguridad de la información, equipo de desarrollo | Se ha establecido una política para el desarrollo seguro de aplicaciones, que incluye la identificación y mitigación proactiva de vulnerabilidades. |
| A14.2.2 | Procedimiento de control de cambios en sistemas | Definido | Equipo de seguridad de la información, equipo de desarrollo | Se ha establecido un procedimiento para gestionar y documentar los cambios realizados en los sistemas y aplicaciones, incluidas las pruebas de seguridad y la aprobación de la gestión. |
| A14.2.3 | Revisión técnica de las aplicaciones tras efectuar cambios en el sistema | Definido | Equipo de seguridad de la información, equipo de desarrollo | Se han establecido controles para realizar revisiones técnicas de las aplicaciones después de realizar cambios en el sistema operativo subyacente, para garantizar la integridad y la compatibilidad. |
| A14.2.4 | Restricciones a los cambios en los paquetes de software | Definido | Equipo de seguridad de la información, equipo de desarrollo | Se han implementado controles para restringir y gestionar los cambios en los paquetes de software utilizados en los sistemas y aplicaciones, incluida la evaluación de riesgos y la aprobación de la gestión. |
| A14.2.5 | Principios de ingeniería de sistemas seguros | Definido | Equipo de seguridad de la información, equipo de desarrollo | Se han establecido principios de ingeniería de sistemas seguros para guiar el diseño, desarrollo e implementación de sistemas y aplicaciones seguros. |
| A14.2.6 | Entorno de desarrollo seguro | Definido | Equipo de seguridad de la información, equipo de desarrollo | Se ha implementado un entorno de desarrollo seguro que incluye controles de acceso, monitorización de actividad y restricciones de red para proteger los sistemas y datos sensibles. |
| A14.2.7 | Externalización del desarrollo de software | Definido | Equipo de seguridad de la información, equipo de desarrollo | Se han establecido controles para gestionar los riesgos asociados con la externalización del desarrollo de software, incluida la evaluación de proveedores y la protección de la propiedad intelectual. |
| A14.2.8 | Pruebas funcionales de seguridad de sistemas | Definido | Equipo de seguridad de la información, equipo de desarrollo | Se han implementado pruebas funcionales de seguridad de sistemas para evaluar la resistencia de los sistemas y aplicaciones a ataques y vulnerabilidades conocidos. |

| | | | | |
|---|---|---|---|---|
| A14.2.9 | Pruebas de aceptación de sistemas | Definido | Equipo de seguridad de la información, equipo de desarrollo | Se han establecido criterios y procedimientos para realizar pruebas de aceptación de sistemas que incluyan requisitos de seguridad y funcionales. |
| **A14.3** | **Datos de prueba** | | | |
| A14.3.1 | Protección de los datos de prueba | Definido | Equipo de seguridad de la información, equipo de desarrollo | Se han implementado controles para proteger los datos de prueba contra accesos no autorizados y su uso indebido, incluida la anonimización y cifrado de datos sensibles. |
| **A15** | **Relación con proveedores** | | | |
| **A15.1** | **Seguridad en las relaciones con proveedores** | | | |
| A15.1.1 | Política de seguridad de la información en las relaciones con los provee | Definido | Equipo de seguridad de la información, equipo legal | Se ha establecido una política de seguridad de la información para regular las relaciones con los proveedores, incluida la evaluación de riesgos y la protección de datos. |
| A15.1.2 | Requisitos de seguridad en contratos con terceros | Definido | Equipo de seguridad de la información, equipo legal | Se han establecido requisitos de seguridad en los contratos con terceros para garantizar el cumplimiento de las políticas y normativas de seguridad de la información de la organización. |
| A15.1.3 | Cadena de suministro de tecnología de la información y de las comunic | Definido | Equipo de seguridad de la información, equipo de compras | Se han implementado controles para gestionar los riesgos asociados con la cadena de suministro de tecnología de la información y de las comunicaciones, incluida la evaluación de proveedores y la gestión de cambios. |
| **A15.2** | **Gestión de la provisión de servicios del proveedor** | | | |
| A15.2.1 | Control y revisión de la provisión de servicios del proveedor | Definido | Equipo de seguridad de la información, equipo de TI | Se han establecido controles para supervisar y revisar la provisión de servicios del proveedor para garantizar el cumplimiento de los acuerdos y los requisitos de seguridad. |
| A15.2.2 | Gestión de cambios en la provisión del servicio del proveedor | Definido | Equipo de seguridad de la información, equipo de TI | Se ha establecido un proceso para gestionar y documentar los cambios realizados por los proveedores de servicios, incluida la evaluación de riesgos y la aprobación de la gestión. |
| **A16** | **Gestión de incidentes de seguridad de la información** | | | |
| **A16.1** | **Gestión de incidentes de seguridad de la información y mejoras** | | | |
| A16.1.1 | Responsabilidades y procedimientos | Definido | Equipo de seguridad de la información | Se han establecido roles y responsabilidades claros para la gestión de incidentes de seguridad de la información, incluida la notificación y respuesta a incidentes. |
| A16.1.2 | Notificación de los eventos de seguridad de la información | Definido | Equipo de seguridad de la información | Se han establecido procedimientos para notificar y registrar los eventos de seguridad de la información, incluida la comunicación con partes internas y externas según sea necesario. |
| A16.1.3 | Notificación de puntos débiles de la seguridad | Definido | Equipo de seguridad de la información | Se han establecido canales de comunicación para notificar y abordar los puntos débiles identificados en la seguridad de la información, incluidas las vulnerabilidades y deficiencias en los controles. |
| A16.1.4 | Evaluación y decisión sobre los eventos de seguridad de información | Definido | Equipo de seguridad de la información | Se ha establecido un proceso para evaluar y tomar decisiones sobre los eventos de seguridad de la información, incluida la asignación de prioridades y la asignación de recursos. |
| A16.1.5 | Respuesta a incidentes de seguridad de la información | Definido | Equipo de seguridad de la información | Se han establecido procedimientos para responder de manera rápida y efectiva a los incidentes de seguridad de la información, incluida la contención, erradicación y recuperación. |
| A16.1.6 | Aprendizaje de los incidentes de seguridad de la información | Definido | Equipo de seguridad de la información | Se ha establecido un proceso para aprender de los incidentes de seguridad de la información y mejorar continuamente la postura de seguridad de la organización. |
| A16.1.7 | Recopilación de evidencias | Definido | Equipo de seguridad de la información | Se ha establecido un proceso para recopilar y preservar evidencia digital en caso de incidentes de seguridad de la información, cumpliendo con los requisitos legales y regulatorios. |
| **A17** | **Aspectos de seguridad de la información para la gestión de la cont** | | | |
| **A17.1** | **Continuidad de la seguridad de la información** | | | |
| A17.1.1 | Planificación de la continuidad de la seguridad de la información | Definido | Equipo de seguridad de la información, equipo de continuidad del negocio | Se han identificado los requisitos de continuidad de la seguridad de la información y se ha desarrollado un plan integral para garantizar la disponibilidad y la integridad de los datos críticos. |

| | | | | |
|---|---|---|---|---|
| A17.1.2 | Implementar la continuidad de la seguridad de la información | Definido | Equipo de seguridad de la información, equipo de continuidad del negocio | Se han implementado medidas y controles para asegurar la continuidad de la seguridad de la información en situaciones de emergencia o interrupción del negocio, incluida la copia de seguridad y la recuperación de datos. |
| A17.1.3 | Verificación, revisión y evaluación de la continuidad de la seguridad de l | Definido | Equipo de seguridad de la información, equipo de continuidad del negocio | Se realizan revisiones periódicas y evaluaciones de la continuidad de la seguridad de la información para identificar áreas de mejora y garantizar la alineación con los objetivos del negocio. |
| **A17.2** | **Redundancias** | | | |
| A17.2.1 | Disponibilidad de los recursos de tratamiento de la información | Definido | Equipo de TI, equipo de continuidad del negocio | Se han implementado redundancias y failovers para garantizar la disponibilidad continua de los recursos de tratamiento de la información en caso de interrupción o falla del sistema. |
| **A18** | **Cumplimiento** | | | |
| **A18.1** | **Cumplimiento de los requisitos legales y contractuales** | | | |
| A18.1.1 | Identificación de la legislación aplicable y de los requisitos contractuales | Definido | Equipo de cumplimiento, equipo legal | Se han identificado y documentado los requisitos legales y contractuales aplicables a la seguridad de la información, incluidos los estándares de la industria y las regulaciones gubernamentales. |
| A18.1.2 | Derechos de Propiedad Intelectual (DPI) | Definido | Equipo de cumplimiento, equipo legal | Se han establecido controles para proteger los derechos de propiedad intelectual relacionados con la seguridad de la información, incluidos los derechos de autor y las patentes. |
| A18.1.3 | Protección de los registros de la organización | Definido | Equipo de cumplimiento, equipo de seguridad de la información | Se han implementado controles para proteger la confidencialidad, integridad y disponibilidad de los registros de la organización, incluidos los registros de seguridad de la información. |
| A18.1.4 | Protección y privacidad de la información de carácter personal | Definido | Equipo de cumplimiento, equipo de seguridad de la información | Se han establecido medidas para proteger la privacidad y confidencialidad de la información de carácter personal, incluido el cumplimiento de leyes y regulaciones de privacidad de datos. |
| A18.1.5 | Regulación de los controles criptográficos | Definido | Equipo de cumplimiento, equipo de seguridad de la información | Se han implementado controles criptográficos para proteger la confidencialidad e integridad de la información según lo exijan las leyes y regulaciones aplicables. |
| **A18.2** | **Revisiones de la seguridad de la información** | | | |
| A18.2.1 | Revisión independiente de la seguridad de la información | Definido | Equipo de auditoría interna, equipo de seguridad de la información | Se han establecido procesos para realizar revisiones independientes de la seguridad de la información, incluida la evaluación de controles y prácticas de seguridad. |
| A18.2.2 | Cumplimiento de las políticas y normas de seguridad | Definido | Equipo de cumplimiento, equipo de seguridad de la información | Se han establecido procedimientos para verificar el cumplimiento de las políticas y normas de seguridad de la información, incluidas las revisiones periódicas y las pruebas de conformidad. |
| A18.2.3 | Comprobación del cumplimiento técnico | Definido | Equipo de cumplimiento, equipo de seguridad de la información | Se han implementado controles y procesos para verificar el cumplimiento técnico con los estándares y las regulaciones de seguridad de la información, incluidas las evaluaciones de vulnerabilidades y las pruebas de seguridad. |



Número de Controles