# Controles de Seguridad y Privacidad de la Información

SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

**Guía No. 8**

MINTIC vive digital Colombia TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN

## HISTORIA

| VERSIÓN | FECHA | CAMBIOS INTRODUCIDOS |
|---|---|---|
| 1.0.0 | 15/12/2010 | Versión inicial del documento |
| 2.0.0 | 30/09/2011 | Restructuración de forma |
| 2.0.1 | 30/11/2011 | Actualización del documento |
| 3.0.0 | 08/01/2015 | Actualización según restructuración del modelo |
| 3.0.1 | 14/03/2016 | Revisión y actualización |

## TABLA DE CONTENIDO

**PÁG.**

## 1. DERECHOS DE AUTOR

## 2. AUDIENCIA

Entidades públicas de orden nacional y entidades públicas del orden territorial, así como proveedores de servicios de Gobierno en Línea, y terceros que deseen adoptar el Modelo de Seguridad y Privacidad de TI en el marco de la Estrategia de Gobierno en Línea.

## 3. INTRODUCCIÓN

El Modelo de Seguridad y Privacidad de la Información en la fase de Planificación se realiza la selección de controles, y durante la fase Implementación se ejecuta la implementación de controles de seguridad de la información, por lo cual se cuenta con el anexo de controles del estándar ISO 27002.

El documento presenta los objetivos de control del estándar ISO 27002.

La información es un recurso que, como el resto de los activos, tiene valor para el organismo y por consiguiente debe ser debidamente protegida. Las políticas de seguridad y privacidad de la información protegen a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos de las entidades del Estado.

Es importante que los principios de la política de seguridad y privacidad descritos en el presente documento se entiendan y se asimilen al interior de las entidades como una directriz de Gobierno que será exitosa en la medida que se cuente con un compromiso manifiesto de la máxima autoridad en cada entidad.

## 4. OBJETIVO

Proteger la información de las entidades del Estado, los mecanismos utilizados para el procesamiento de la información, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad y confiabilidad de la información.

### OBJETIVO DE LAS ENTIDADES:

Establecer, implementar, operar, monitorear, revisar, mantener y mejorar un sistema de gestión de seguridad de la información dentro de las entidades del Estado, que reporte a nivel central su estado de avance.

Fomentar la consulta y cooperación con organismos especializados para la obtención de asesoría en materia de seguridad de la información.

Garantizar la aplicación de medidas de seguridad adecuadas en los accesos a la información propiedad de las entidades del Estado.

## 5. ALCANCE

Este documento de políticas aplica a todas las entidades del Estado que estén vinculadas de alguna manera, como usuarios o prestadores de servicios de la estrategia de Gobierno en línea, a sus recursos, a sus procesos y al personal interno o externo vinculado a la entidad a través de contratos o acuerdos.

### TERCEROS:

Las entidades pueden requerir que terceros accedan a información interna, la copien, la modifiquen, o bien puede ser necesaria la tercerización de ciertas funciones relacionadas con el procesamiento de la información. En estos casos, los terceros deben tener y las entidades les deben exigir, que se establezcan las medidas adecuadas para la protección de la información de acuerdo a su clasificación y análisis de riesgo.

## 6. TABLA DE CONTROLES

La siguiente tabla, muestra la organización de los controles detallando los dominios definidos en el componente de Planificación. SIEMPRE se deben mencionar los controles correspondientes al Anexo A de la norma NTC: ISO/IEC 27001, cual trata de los objetivos de control, y se estructurarán tal como lo muestra la Tabla 1:

*Tabla 1. Estructura de controles*

| **Política general** | | | |
|---|---|---|---|
| Núm. | Nombre | Seleccionado / Excepción | Descripción / Justificación |
| | Nombre | Control | |
| | … | | |

Cada campo se define así:

- Núm.: Este campo identifica cada uno de los controles correspondientes al Anexo A de la norma NTC: ISO/IEC 27001.
- Nombre: Este campo hace referencia al nombre del control que se debe aplicar para dar cumplimiento a la política definida.
- Control: Este campo describe el control que se debe implementar con el fin de dar cumplimiento a la política definida.
- Dominio: Este campo describe si el control aplica para uno o múltiples dominios.
- Seleccionado / Excepción: El listado de controles además debe ser utilizado para la generación de la declaración de aplicabilidad, donde cada uno de los controles es justificado tanto si se implementa como si se excluye de ser implementado, lo cual ayuda a que la entidad tenga documentado y de fácil acceso el inventario de controles.
- Descripción / Justificación: El listado de controles cuenta con la descripción de cada control en la tabla. Adicionalmente, es posible utilizarlo para la generación de la declaración de aplicabilidad, donde cada uno de los controles es justificado tanto si se implementa como si se excluye de ser implementado.

*Tabla 2 – Controles del Anexo A del estándar ISO/IEC 27001:2013 y dominios a los que pertenece*

| Núm. | Nombre | Selección / Excención | Descripción / Justificación |
|---|---|---|---|
| 1 | Objeto y campo de aplicación | | Seleccionar los controles dentro del proceso de implementación del Sistema de Gestión de Seguridad de la Información - SGSI |
| 2 | Referencias normativas | | La ISO/IEC 27000, es referenciada parcial o totalmente en el documento y es indispensable para su aplicación. |
| 3 | Términos y definiciones | | Para los propósitos de este documento se aplican los términos y definiciones presentados en la norma ISO/IEC 27000. |
| 4 | Estructura de la norma | | La norma ISO/IEC 27000, contiene 14 numérales de control de seguridad de la información que en su conjunto contienen más de 35 categorías de seguridad principales y 114 controles. |
| A.5 | Políticas de seguridad de la información | | |
| A.5.1 | Directrices establecidas por la dirección para la seguridad de la información | | Objetivo: Brindar orientación y apoyo por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes. |
| A.5.1.1 | Políticas para la seguridad de la información | | Control: Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes. |
| A.5.1.2 | Revisión de las políticas para seguridad de la información | | Control: Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas. |
| A.6 | Organización de la seguridad de la información | | |
| A.6.1 | Organización interna | | Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización. |
| A.6.1.1 | Roles y responsabilidades para la seguridad de información | | Control: Se deberían definir y asignar todas las responsabilidades de la seguridad de la información. |
| A.6.1.2 | Separación de deberes | | Control: Los deberes y áreas de responsabilidad en conflicto se deberían separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización. |
| A.6.1.3 | Contacto con las autoridades | | Control: Se deberían mantener los contactos apropiados con las autoridades pertinentes. |
| A.6.1.4 | Contacto con grupos de interés especial | | Control: Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad. |
| A.6.1.5 | Seguridad de la información en la gestión de proyectos | | Control: La seguridad de la información se debería tratar en la gestión de proyectos, independientemente del tipo de proyecto. |
| A.6.2 | Dispositivos móviles y teletrabajo | | Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles. |
| A.6.2.1 | Política para dispositivos móviles | | Control: Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles. |
| A.6.2.2 | Teletrabajo | | Control: Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo. |
| A.7 | Seguridad de los recursos humanos | | |
| A.7.1 | Antes de asumir el empleo | | Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran. |

| | | | |
|---|---|---|---|
| A.7.1.1 | Selección | | Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos. |
| A.7.1.2 | Términos y condiciones del empleo | | Control: Los acuerdos contractuales con empleados y contratistas, deberían establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información. |
| A.7.2 | Durante la ejecución del empleo | | Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan. |
| A.7.2.1 | Responsabilidades de la dirección | | Control: La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización. |
| A.7.2.2 | Toma de conciencia, educación y formación en la seguridad de la información | | Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo. |
| A.7.2.3 | Proceso disciplinario | | Control: Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información. |
| A.7.3 | Terminación o cambio de empleo | | Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación del contrato. |
| A.7.3.1 | Terminación o cambio de responsabilidades de empleo | | Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir. |
| A.8 | Gestión de activos | | |
| A.8.1 | Responsabilidad por los activos | | Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas. |
| A.8.1.1 | Inventario de activos | | Control: Se deberían identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos. |
| A.8.1.2 | Propiedad de los activos | | Control: Los activos mantenidos en el inventario deberían tener un propietario. |
| A.8.1.3 | Uso aceptable de los activos | | Control: Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información. |
| A.8.1.4 | Devolución de activos | | Control: Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo. |
| A.8.2 | Clasificación de la información | | Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización. |
| A.8.2.1 | Clasificación de la información | | Control: La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada. |
| A.8.2.2 | Etiquetado de la información | | Control: Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización. |
| A.8.2.3 | Manejo de activos | | Control: Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización. |
| A.8.3.1 | Gestión de medios removibles | | Control: Se deberían implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización. |
| A.8.3.2 | Disposición de los medios | | Control: Se debería disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales. |
| A.8.3.3 | Transferencia de medios físicos | | Control: Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte. |

| | | | |
|---|---|---|---|
| A.9 | Control de acceso | | |
| A.9.1 | Requisitos del negocio para control de acceso | | Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información. |
| A.9.1.1 | Política de control de acceso | | Control: Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información. |
| A.9.1.2 | Política sobre el uso de los servicios de red | | Control: Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente. |
| A.9.2 | Gestión de acceso de usuarios | | Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios. |
| A.9.2.1 | Registro y cancelación del registro de usuarios | | Control: Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso. |
| A.9.2.2 | Suministro de acceso de usuarios | | Control: Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios. |
| A.9.2.3 | Gestión de derechos de acceso privilegiado | | Control: Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado. |
| A.9.2.4 | Gestión de información de autenticación secreta de usuarios | | Control: La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal. |
| A.9.2.5 | Revisión de los derechos de acceso de usuarios | | Control: Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares. |
| A.9.2.6 | Retiro o ajuste de los derechos de acceso | | Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios. |
| A.9.3 | Responsabilidades de los usuarios | | Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación. |
| A.9.3.1 | Uso de la información de autenticación secreta | | Control: Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta. |
| A.9.4 | Control de acceso a sistemas y aplicaciones | | Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones. |
| A.9.4.1 | Restricción de acceso Información | | Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso. |
| A.9.4.2 | Procedimiento de ingreso seguro | | Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro. |
| A.9.4.3 | Sistema de gestión de contraseñas | | Control: Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas. |
| A.9.4.4 | Uso de programas utilitarios privilegiados | | Control: Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones. |
| A.9.4.5 | Control de acceso a códigos fuente de programas | | Control: Se debería restringir el acceso a los códigos fuente de los programas. |
| A.10 | Criptografía | | |
| A.10.1 | Controles criptográficos | | Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información. |
| A.10.1.1 | Política sobre el uso de controles criptográficos | | Control: Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información. |
| A.10.1.2 | Gestión de llaves | | Control: Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida. |
| A.11 | Seguridad física y del entorno | | |

| | | | |
|---|---|---|---|
| A.11.1 | Áreas seguras | | Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización. |
| A.11.1.1 | Perímetro de seguridad física | | Control: Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información. |
| A.11.1.2 | Controles físicos de entrada | | Control: Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado. |
| A.11.1.3 | Seguridad de oficinas, recintos e instalaciones | | Control: Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones. |
| A.11.1.4 | Protección contra amenazas externas y ambientales | | Control: Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes. |
| A.11.1.5 | Trabajo en áreas seguras | | Control: Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras. |
| A.11.1.6 | Áreas de despacho y carga | | Control: Se deberían controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado. |
| A.11.2 | Equipos | | Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización. |
| A.11.2.1 | Ubicación y protección de los equipos | | Control: Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado. |
| A.11.2.2 | Servicios de suministro | | Control: Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro. |
| A.11.2.3 | Seguridad del cableado | | Control: El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño. |
| A.11.2.4 | Mantenimiento de equipos | | Control: Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas. |
| A.11.2.5 | Retiro de activos | | Control: Los equipos, información o software no se deberían retirar de su sitio sin autorización previa. |
| A.11.2.6 | Seguridad de equipos y activos fuera de las instalaciones | | Control: Se deberían aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones. |
| A.11.2.7 | Disposición segura o reutilización de equipos | | Control: Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización. |
| A.11.2.8 | Equipos de usuario desatendidos | | Control: Los usuarios deberían asegurarse de que a los equipos desatendidos se les dé protección apropiada. |
| A.11.2.9 | Política de escritorio limpio y pantalla limpia | | Control: Se debería adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información. |
| A.12 | Seguridad de las operaciones | | |
| A.12.1 | Procedimientos operacionales y responsabilidades | | Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información. |
| A.12.1.1 | Procedimientos de operación documentados | | Control: Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten. |
| A.12.1.2 | Gestión de cambios | | Control: Se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información. |
| A.12.1.3 | Gestión de capacidad | | Control: Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura. |
| A.12.1.4 | Separación de los ambientes de desarrollo, pruebas y operación | | Control: Se deberían separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación. |

| | | | |
|---|---|---|---|
| A.12.2 | Protección contra códigos maliciosos | | Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos. |
| A.12.2.1 | Controles contra códigos maliciosos | | Control: Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos. |
| A.12.3 | Copias de respaldo | | Objetivo: Proteger contra la perdida de datos. |
| A.12.3.1 | Respaldo de información | | Control: Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada. |
| A.12.4 | Registro y seguimiento | | Objetivo: Registrar eventos y generar evidencia. |
| A.12.4.1 | Registro de eventos | | Control: Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información. |
| A.12.4.2 | Protección de la información de registro | | Control: Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado. |
| A.12.4.3 | Registros del administrador y del operador | | Control: Las actividades del administrador y del operador del sistema se deberían registrar, y los registros se deberían proteger y revisar con regularidad. |
| A.12.4.4 | sincronización de relojes | | Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo. |
| A.12.5 | Control de software operacional | | Objetivo: Asegurar la integridad de los sistemas operacionales. |
| A.12.5.1 | Instalación de software en sistemas operativos | | Control: Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos. |
| A.12.6 | Gestión de la vulnerabilidad técnica | | Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas. |
| A.12.6.1 | Gestión de las vulnerabilidades técnicas | | Control: Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado. |
| A.12.6.2 | Restricciones sobre la instalación de software | | Control: Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios. |
| A.12.7 | Consideraciones sobre auditorias de sistemas de información | | Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales. |
| A.12.7.1 | Información controles de auditoría de sistemas | | Control: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del 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 sus instalaciones de procesamiento de información de soporte. |
| A.13.1.1 | Controles de redes | | Control: Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones. |
| A.13.1.2 | Seguridad de los servicios de red | | Control: Se deberían identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente. |
| A.13.1.3 | Separación en las redes | | Control: Los grupos de servicios de información, usuarios y sistemas de información se deberían separar en las redes. |
| A.13.2 | Transferencia de información | | Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa. |
| A.13.2.1 | Políticas y procedimientos de transferencia de información | | Control: Se debería contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación. |

| | | | |
|---|---|---|---|
| A.13.2.2 | Acuerdos sobre transferencia de información | | Control: Los acuerdos deberían tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas. |
| A.13.2.3 | Mensajería electrónica | | Control: Se debería proteger adecuadamente la información incluida en la mensajería electrónica. |
| A.13.2.4 | Acuerdos de confidencialidad o de no divulgación | | Control: Se deberían identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información. |
| A.14 | Adquisición, desarrollo y mantenimientos de sistemas | | |
| A.14.1.1 | Requisitos de seguridad de los sistemas de información | | Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas. |
| A.14.1.1 | Análisis y especificación de requisitos de seguridad de la información | | Control: Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes. |
| A.14.1.2 | Seguridad de servicios de las aplicaciones en redes publicas | | Control: La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas. |
| A.14.1.3 | Protección de transacciones de los servicios de las aplicaciones | | Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debería proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada. |
| A.14.2 | Seguridad en los procesos de desarrollo y soporte | | Objetivo: Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información. |
| A.14.2.1 | Política de desarrollo seguro | | Control: Se deberían establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización. |
| A.14.2.2 | Procedimientos de control de cambios en sistemas | | Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deberían controlar mediante el uso de procedimientos formales de control de cambios. |
| A.14.2.3 | Revisión técnica de las aplicaciones después de cambios en la plataforma de operación | | Control: Cuando se cambian las plataformas de operación, se deberían revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización. |
| A.14.2.4 | Restricciones en los cambios a los paquetes de software | | Control: Se deberían desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deberían controlar estrictamente. |
| A.14.2.5 | Principios de construcción de sistemas seguros | | Control: Se deberían establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información. |
| A.14.2.6 | Ambiente de desarrollo seguro | | Control: Las organizaciones deberían establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas. |
| A.14.2.7 | Desarrollo contratado externamente | | Control: La organización debería supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente. |
| A.14.2.8 | Pruebas de seguridad de sistemas | | Control: Durante el desarrollo se deberían llevar a cabo pruebas de funcionalidad de la seguridad. |
| A.14.2.9 | Prueba de aceptación de sistemas | | Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados. |
| A.14.3 | Datos de prueba | | Objetivo: Asegurar la protección de los datos usados para pruebas. |
| A.14.3.1 | Protección de datos de prueba | | Control: Los datos de ensayo se deberían seleccionar, proteger y controlar cuidadosamente. |

| | | | |
|---|---|---|---|
| A.15 | Relación con los proveedores | | |
| A.15.1 | Seguridad de la información en las relaciones con los 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 para las relaciones con proveedores | | Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deberían acordar con estos y se deberían documentar. |
| A.15.1.2 | Tratamiento de la seguridad dentro de los acuerdos con proveedores | | Control: Se deberían establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización. |
| A.15.1.3 | Cadena de suministro de tecnología de información y comunicación | | Control: Los acuerdos con proveedores deberían incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación. |
| A.15.2 | Gestión de la prestación de servicios con los proveedores | | Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores. |
| A.15.2.1 | Seguimiento y revisión de los servicios de los proveedores | | Las organizaciones deberían hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores. |
| A.15.2.2 | Gestión de cambios en los servicios de proveedores | | Control: Se deberían gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes , teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos. |
| A.16 | Gestión de incidentes de seguridad de la información | | |
| A.16.1 | Gestión de incidentes y mejoras en la seguridad de la información | | Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades. |
| A.16.1.1 | Responsabilidad y procedimientos | | Control: Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información. |
| A.16.1.2 | Reporte de eventos de seguridad de la información | | Control: Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible. |
| A.16.1.3 | Reporte de debilidades de seguridad de la información | | Control: Se debería exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios. |
| A.16.1.4 | Evaluación de eventos de seguridad de la información y decisiones sobre ellos | | Control: Los eventos de seguridad de la información se deberían evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información. |
| A.16.1.5 | Respuesta a incidentes de seguridad de la información | | Control: Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados. |
| A.16.1.6 | Aprendizaje obtenido de los incidentes de seguridad de la información | | Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros. |
| A.16.1.7 | Recolección de evidencia | | Control: La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia. |
| A.17 | Aspectos de seguridad de la información de la gestión de continuidad de negocio | | |
| A.17.1 | Continuidad de seguridad de la información | | Objetivo: La continuidad de seguridad de la información se debería incluir en 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: La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre. |
| A.17.1.2 | Implementación de la continuidad de la seguridad de la información | | Control: La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para 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: La organización debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son validos y eficaces durante situaciones adversas. |
| A.17.2 | Redundancias | | Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información. |
| A.17.2.1 | Disponibilidad de instalaciones de procesamiento de información. | | Control: Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad. |
| A.18 | Cumplimiento | | |
| A.18.1 | Cumplimiento de requisitos legales y contractuales | | Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad. |
| A.18.1.1 | Identificación de la legislación aplicable y de los requisitos contractuales | | Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deberían identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización. |
| A.18.1.2 | Derechos de propiedad intelectual | | Control: Se deberían implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados. |
| A.18.1.3 | Protección de registros | | Control: Los registros se deberían proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio. |
| A.18.1.4 | Privacidad y protección de datos personales | | Control: Cuando sea aplicable, se deberían asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes. |
| A.18.1.5 | Reglamentación de controles criptográficos | | Control: Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes. |
| A.18.2 | Revisiones de seguridad de la información | | Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales. |
| A.18.2.1 | Revisión independiente de la seguridad de la información | | Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deberían revisar independientemente a intervalos planificados o cuando ocurran cambios significativos. |
| A.18.2.2 | Cumplimiento con las políticas y normas de seguridad | | Control: Los directores deberían revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad. |
| A.18.2.3 | Revisión del cumplimiento técnico | | Control: Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información. |

## 7. DECLARACIÓN DE APLICABILIDAD

La Declaración de Aplicabilidad, por sus siglas en ingles *Statement of Applicability (SoA)*, es un elemento fundamental para la implementación del Modelo de Seguridad y Privacidad de la Información.

- La declaración de aplicabilidad se debe realizar luego del tratamiento de riesgos, y a su vez es la actividad posterior a la evaluación de riesgos.
- La declaración de aplicabilidad debe indicar si los objetivos de control y los controles se encuentran implementados y en operación, los que se hayan descartado, de igual manera se debe justificar por qué algunas medidas han sido excluidas (las innecesarias y la razón del por qué no son requerías por la Entidad).

Dentro de las actividades a seguir, después de la selección de los controles de seguridad, se procede a crear el plan de tratamiento de riesgos, esto con la finalidad de definir las actividades necesarias para la aplicación de los controles de seguridad.

A continuación se presenta un ejemplo de formato de Declaración de aplicabilidad:

| | | Objetivo de control o control seleccionado Si/No | Razón de la Selección | Objetivo de control o control Implementado Si/No | Justificación de exclusión | Referencia | Aprobado por la alta dirección Firma director de la entidad |
|---|---|---|---|---|---|---|---|
| Dominio | A.5 Políticas de seguridad de la información | | | | | | |
| Objetivo de control | A. 5.1 Directrices establecidas por la dirección para la seguridad de la información | | | | | | |
| Control | A. 5.1.1 Políticas para la seguridad de la información | | | | | | |
| Control | A. 5.1.2 Revisión de las políticas para seguridad de la información | | | | | | |

*Tabla 3. Formato Ejemplo Declaración de Aplicabilidad.*