CONTROLES ISO 27001:2013 A IMPLEMENTAR

Dominio	Objetivo de Control	Numeral Control	Control
A.5 POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN	A.5.1 Orientación de la dirección para la gestión de la seguridad de la información	A.5.1.1 Políticas para la seguridad de la información	Se debe definir un conjunto de políticas para la seguridad de la información, aprobadas por la dirección, publicadas y comunicadas a los empleados y partes externas pertinentes.
		A.5.1.2 Revisión de las políticas para seguridad de la información	Las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su idoneidad, adecuación y eficacia continuas.
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	A.6.1 Organización interna	A.6.1.1 Roles y responsabilidades para la Seguridad de la información	Se deben definir y asignar todas las responsabilidades para la seguridad de la información.
		A.6.1.2 Separación de deberes	Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir la posibilidad 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	Se deben mantener contactos apropiados con las autoridades pertinentes.
		A.6.1.4 Contacto con grupos de interés especial	Se deben mantener controles apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.

		A.6.1.5 Seguridad de la información en gestión de proyectos	La seguridad de la información debe ser considerada en la gestión de proyectos, independientemente del tipo de proyecto.
	A.6.2 Dispositivos móviles y teletrabajo	A.6.2.1 Política para dispositivos móviles	Se debe adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos generados por el uso de dispositivos móviles.
		A.6.2.2 Teletrabajo	Se debe 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	A.7.1.1 Selección	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deben 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	Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a seguridad de la información.

	A.7.2 Durante la ejecución del empleo	A.7.2.1 Responsabilidades de la dirección	La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos de la organización.
		A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben 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	Se debe contar con un proceso formal y comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.

	A.7.3 Terminación y cambio de empleo	A.7.3.1 Terminación o cambio de responsabilidades de empleo	Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.
A.8 GESTIÓN DE ACTIVOS	A.8.1 Responsabilidad por los activos	A.8.1.1 Inventario de activos	Se deben identificar los activos asociados con información e instalaciones de procesamiento de información y se debe elaborar y mantener un inventario de estos activos.
		A.8.1.2 Propiedad de los activos	Los activos mantenidos en el inventario deben ser propios.
		A.8.1.3 Uso aceptable de los activos	Se deben 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	Todos los empleados y usuarios de partes externas deben 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	A.8.2.1 Clasificación de la información	La información se debe 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	Se debe desarrollar e implementar un conjunto apropiado 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	Se deben 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 Manejo de medios de soporte	A.8.3.1 Gestión de medios removibles	Se deben implementar procedimientos para la gestión de medios de soporte removibles, de acuerdo con el esquema de clasificación adoptado por la organización.
		A.8.3.2 Disposición de los medios	Se debe disponer en forma segura de los medios de soporte cuando ya no se requieran, utilizando procedimientos formales.
		A.8.3.3 Transferencia de medios de físicos	Los medios que contienen información se deben 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	A.9.1.1 Política de control de acceso	Se debe 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 Acceso a redes y a servicios en red	Solo se debe 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	A.9.2.1 Registro y cancelación del registro de usuarios	Se debe implementar un proceso formal de registro y de cancelación del registro, para posibilitar la asignación de los derechos de acceso.

		A.9.2.2 Suministro de acceso de usuarios	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o cancelar los derechos de acceso a todo tipo de usuarios a todos los sistemas y servicios.
		A.9.2.3 Gestión de derechos de acceso privilegiado	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.
		A.9.2.4 Gestión de información de autenticación secreta de usuarios	La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.
		A.9.2.5 Revisión de los derechos de acceso de usuarios	Los dueños de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.
		A.9.2.6 Retiro o ajuste de los derechos de acceso	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben cancelar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.
	A.9.3 Responsabilidades de los usuarios	A.9.3.1 Uso de información de autenticación secreta	Se debe 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	A.9.4.1 Restricción de acceso a información	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.
		A.9.4.2 Procedimiento de ingreso seguro	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.
		A.9.4.3 Sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.
		A.9.4.4 Uso de programas utilitarios privilegiados	Se debe restringir y controlar estrechamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.

		A.9.4.5 Control de acceso a códigos fuente de programas	Se debe restringir el acceso a códigos fuente de programas.
A.10 CRIPTOGRAFÍA	A.10.1 Controles criptográficos	A.10.1.1 Política sobre el uso de controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de Controles criptográficos para protección de información.
		A.10.1.2 Gestión de llaves	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de llaves criptográficas, durante todo su ciclo de vida.
A.11 SEGURIDAD FÍSICA Y AMBIENTAL	A.11.1 Áreas seguras	A.11.1.1 Perímetro de seguridad física	Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.

		A.11.1.2 Controles de acceso físicos	Las áreas seguras se deben proteger mediante controles de accesos apropiados para asegurar que solamente se permite el acceso a personal autorizado.
		A.11.1.3 Seguridad de oficinas, recintos e instalaciones	Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.
		A.11.1.4 Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
		A.11.1.5 Trabajo en áreas seguras	Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.
		A.11.1.6 Áreas de despacho y carga	Se deben 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	A.11.2.1 Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, y las posibilidades de acceso no autorizado.
		A.11.2.2 Servicios de suministro	Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
		A.11.2.3 Seguridad del cableado	El cableado de potencia y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño
		A.11.2.4 Mantenimiento de equipos	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
		A.11.2.5 Retiro de activos	Los equipos, información o software no se deben retirar de su sitio sin autorización previa.
		A.11.2.6 Seguridad de equipos y activos fuera de las instalaciones	Se deben 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	Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reúso.
		A.11.2.8 Equipos de usuario desatendido	Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.
		A.11.2.9 Política de escritorio limpio y pantalla limpia	Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia para las instalaciones de procesamiento de información.
A.12 SEGURIDAD DE LAS OPERACIONES	A.12.1 Procedimientos operacionales y responsabilidades	A.12.1.1 Procedimientos de operación documentados	Los procedimientos operativos se deben documentar y poner a disposición de todos los usuarios que los necesitan.
		A.12.1.2 Gestión de cambios	Se deben 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	Se debe hacer seguimiento al uso de recursos, hacer los ajustes y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.
		A.12.1.4 Separación de los ambientes de desarrollo, pruebas, y operacionales	Se deben separar los ambientes de desarrollo, prueba y operativos, para reducir los riesgos de acceso o cambios no autorizados al ambiente operacional.
	A.12.2 Protección contra códigos maliciosos	A.12.2.1 Controles contra códigos maliciosos	Se deben 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	A.12.3.1 Copias de respaldo de la información	Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.
	A.12.4 Registro y seguimiento	A.12.4.1 Registro de eventos	Se deben elaborar, conservar y revisar regularmente los registros de eventos acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
		A.12.4.2 Protección de la información de registro	Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.

		A.12.4.3 Registros del administrador y del operador	Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.
		A.12.4.4 Sincronización de relojes	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.
	A.12.5 Control de software operacional	A.12.5.1 Instalación de software en sistemas operativos	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.
	A.12.6 Gestión de la vulnerabilidad técnica	A.12.6.1 Gestión de las vulnerabilidades técnicas	Se debe 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	Se debe establecer e implementar el reglamento de instalación de software por parte de los usuarios.

	A.12.7 Consideraciones sobre auditorías de sistemas de información	A.12.7.1 Controles de auditorías de sistemas de información	Se deben planificar y acordar cuidadosamente los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos para minimizar las interrupciones en los procesos del negocio.
A.13 SEGURIDAD DE LAS COMUNICACIONES	A.13.1 Gestión de la seguridad de redes	A.13.1.1 Controles de redes	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.
		A.13.1.2 Seguridad de los servicios de red	Se deben 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 servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.
		A.13.1.3 Separación en las redes	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.
	A.13.2 Transferencia de información	A.13.2.1 Políticas y procedimientos de transferencia de información	Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.
		A.13.2.2 Acuerdos sobre transferencia de información	Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.

		A.13.2.3 Mensajes electrónicos	Se debe proteger apropiadamente la información incluida en los mensajes electrónicos.
		A.13.2.4 Acuerdos de confidencialidad o de no divulgación	Se deben 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 MANTENIMIENTO DE SISTEMAS	A.14.1 Requisitos de seguridad de los sistemas de información	A.14.1.1 Análisis y especificación de requisitos de seguridad de la información	Los requisitos relacionados con seguridad de la información se deben 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 públicas	La información involucrada en servicios de aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.
		A.14.1.3 Protección de transacciones de servicios de aplicaciones	La información involucrada en las transacciones de servicios de aplicaciones se debe proteger para prevenir 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 de soporte	A.14.2.1 Política de desarrollo seguro	Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas dentro de la organización.
		A.14.2.2 Procedimientos de control de cambios en sistemas	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.
		A.14.2.3 Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones	Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y poner a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad organizacionales.
		A.14.2.4 Restricciones sobre cambios en los paquetes de software	Se deben desalentar las modificaciones a los paquetes de software, las cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.
		A.14.2.5 Principios de organización de sistemas seguros	Se deben establecer, documentar y mantener principios para la organización de sistemas seguros, y aplicarlos a cualquier trabajo de implementación de sistemas de información.

		A.14.2.6 Ambiente de desarrollo seguro	Las organizaciones deben 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	La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas subcontratados.
		A.14.2.8 Pruebas de seguridad de sistemas	Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.
		A.14.2.9 Prueba de aceptación de sistemas	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba y criterios relacionados.
	A.14.3 Datos de prueba	A.14.3.1 Protección de datos de prueba	Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.

A.15 RELACIONES CON LOS PROVEEDORES	A.15.1 Seguridad de la información en las relaciones con los proveedores	A.15.1.1 Política de seguridad de la información para las relaciones con proveedores	Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con éstos y se deben documentar.
		A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores	Se deben 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	Los acuerdos con proveedores deben 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 de proveedores	A.15.2.1 Seguimiento y revisión de los servicios de los proveedores	La organización debe hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.
		A.15.2.2 Gestión de cambios a los servicios de los proveedores	Se deben gestionar los cambios en el suministro de servicios 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 reevaluación 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	A.16.1.1 Responsabilidades y procedimientos	Se deben 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 Reportes de eventos de seguridad de la información	Los eventos de seguridad de la información se deben 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	Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten 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.	Los eventos de seguridad de la información se deben evaluar y se debe 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	Se debe 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	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.
		A.16.1.7 Recolección de evidencia	La organización debe 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	A.17.1.1 Planificación de la continuidad de la seguridad de la información	La organización debe 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	La organización debe 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	La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.
	A.17.2 Redundancias	A.17.2.1 Disponibilidad de instalaciones de procesamiento de información.	Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.

A.18 CUMPLIMIENTO	A.18.1 Cumplimiento de requisitos legales y contractuales	A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales	Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para la organización
		A.18.1.2 Derechos de propiedad intelectual	Se deben 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	Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legales de reglamentación, contractuales y de negocio.
		A.18.1.4 Privacidad y protección de información de datos personales	Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.

		A.18.1.5 Reglamentación de controles criptográficos	Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.
	A.18.2 Revisiones de seguridad de la información	A.18.2.1 Revisión independiente de la seguridad de la información	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 deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.
		A.18.2.2 Cumplimiento con las políticas y normas de seguridad	Los directores deben 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	Los sistemas de información se deben revisar con periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.