Documento: Declaración de Aplicabilidad - NTC-ISO IEC 27001:2013

Proceso: Seguridad de la Información

Fecha: 30 de noviembre 2021

DIAN
POR UNA COLOMBIA MÁS HONESTA

RL: Requerimientos Legales, OC: Obligaciones Contractuales, RN/MP: Requerimientos del Negocio/Mejores Prácticas adoptadas, RVR: Resultado de la Valoración de Riesgos

ISO 27001:2013 Controles de Seguridad	Núm.	Descripción	Exclusión (Sí / No)	Justificación de exclusión	Controles seleccionados y razones de selección (justificación inclusión)			
					RL	OC	RN/MP	RVR
5 Políticas de Seguridad	5,1	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.						
	5.1.1	Definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas	No		X	X	X	X
	5.1.2	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.	No		X	X	X	X
	6							
6 Organización de la Seguridad de la Información	6,1	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.						
	6.1.1	Se deberían definir y asignar todas las responsabilidades de la seguridad de la información.	No				X	
	6.1.2	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.	No				X	
	6.1.3	Se deberían mantener los contactos apropiados con las autoridades pertinentes.	No				X	
	6.1.4	Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	No				X	
	6.1.5	La seguridad de la información se debería tratar en la gestión de proyectos, independientemente del tipo de proyecto.	No				X	
	6,2	Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.						
	6.2.1	Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	No				X	
	6.2.2	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.	No				X	
	7							
7 Seguridad en los Recursos Humanos	7,1	Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.						
	7.1.1	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.	No		X			
	7.1.2	Los acuerdos contractuales con empleados y contratistas, deberían establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	No		X			
	7,2	Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.						
	7.2.1	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.	No				X	
	7.2.2	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.	No				X	
	7.2.3	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.	No		X			

ISO 27001:2013 Controles de Seguridad	Núm.	Descripción	Exclusión (Sí / No)	Justificación de exclusión	Controles seleccionados y razones de selección (justificación inclusión)			
					RL	OC	RN/MP	RVR
	7,3	Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación del contrato.						
	7.3.1	Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir.	No		X			
	8							
8 Gestión de Activos	8,1	Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.						
	8.1.1	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.	No				X	
	8.1.2	Los activos mantenidos en el inventario deberían tener un propietario.	No				X	
	8.1.3	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.	No				X	
	8.1.4	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.	No				X	
	8,2	Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.						
	8.2.1	La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	No				X	
	8.2.2	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.	No				X	
	8.2.3	Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	No				X	
	8,3	Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios.						
	8.3.1	Se deberían implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	No				X	
	8.3.2	Se debería disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	No				X	
	8.3.3	Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	No				X	
	9							
9 Control de	9,1	Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.						
	9.1.1	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.	No					X
	9.1.2	Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	No					X
	9,2	Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.						
	9.2.1	Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	No				X	
	9.2.2	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.	No				X	
	9.2.3	Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.	No					X
	9.2.4	La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal.	No				X	
	9.2.5	Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares.	No					X

ISO 27001:2013 Controles de Seguridad	Núm.	Descripción	Exclusión (Sí / No)	Justificación de exclusión	Controles seleccionados y razones de selección (justificación inclusión)			
					RL	OC	RN/MP	RVR
Acceso	9.2.6	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.	No					X
	9,3	Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.						
	9.3.1	Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	No				X	
	9,4	Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.						
	9.4.1	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.	No					X
	9.4.2	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.	No				X	
	9.4.3	Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.	No					X
	9.4.4	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.	No				X	
	9.4.5	Se debería restringir el acceso a los códigos fuente de los programas.	No				X	
	10							
10 Criptografía	10,1	Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.						
	10.1.1	Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	No				X	
	10.1.2	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.	No				X	
	11							
11 Seguridad Física y del Entorno	11,1	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.						
	11.1.1	Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o crítica, e instalaciones de manejo de información.	No				X	
	11.1.2	Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.	No					X
	11.1.3	Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	No			X		
	11.1.4	Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	No				X	
	11.1.5	Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras.	No				X	
	11.1.6	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.	No				X	
	11,2	Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.						
	11.2.1	Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.	No				X	
	11.2.2	Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	No					X
	11.2.3	El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño.	No				X	
	11.2.4	Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.	No					X
	11.2.5	Los equipos, información o software no se deberían retirar de su sitio sin autorización previa.	No				X	

ISO 27001:2013 Controles de Seguridad	Núm.	Descripción	Exclusión (Sí / No)	Justificación de exclusión	Controles seleccionados y razones de selección (justificación inclusión)			
					RL	OC	RN/MP	RVR
	11.2.6	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.	No				X	
	11.2.7	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.	No				X	
	11.2.8	Los usuarios deberían asegurarse de que a los equipos desatendidos se les dé protección apropiada.	No				X	
	11.2.9	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.	No				X	
	12							
12 Seguridad en las Operaciones	12,1	Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.						
	12.1.1	Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.	No				X	
	12.1.2	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.	No					X
	12.1.3	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.	No				X	
	12.1.4	Se deberían separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	No				X	
	12,2	Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.						
	12.2.1	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.	No				X	
	12,3	Objetivo: Proteger contra la perdida de datos.						
	12.3.1	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.	No				X	
	12,4	Objetivo: Registrar eventos y generar evidencia.						
	12.4.1	Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	No				X	
	12.4.2	Las instalaciones y la información de registro (logs) se deberían proteger contra alteración y acceso no autorizado.	No				X	
	12.4.3	Las actividades del administrador y del operador del sistema se deberían registrar, y los registros se deberían proteger y revisar con regularidad.	No				X	
	12.4.4	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.	No				X	
	12,5	Objetivo: Asegurar la integridad de los sistemas operacionales.						
	12.5.1	Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos.	No				X	
	12,6	Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.						
	12.6.1	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.	No				X	
	12.6.2	Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios.	No				X	
	12,7	Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.						

ISO 27001:2013 Controles de Seguridad	Núm.	Descripción	Exclusión (Sí / No)	Justificación de exclusión	Controles seleccionados y razones de selección (justificación inclusión)			
					RL	OC	RN/MP	RVR
	12.7.1	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.	No				X	
	13							
13 Seguridad en las Comunicaciones	13,1	Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.						
	13.1.1	Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.	No					X
	13.1.2	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.	No				X	
	13.1.3	Los grupos de servicios de información, usuarios y sistemas de información se deberían separar en las redes.	No				X	
	13,2	Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.						
	13.2.1	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.	No		X			
	13.2.2	Los acuerdos deberían tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.	No		X			
	13.2.3	Se debería proteger adecuadamente la información incluida en la mensajería electrónica.	No		X			
	13.2.4	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.	No		X			
	14							
14 Adquisición, Desarrollo y Mantenimiento de Sistemas	14,1	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.						
	14.1.1	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.	No					X
	14.1.2	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.	No				X	
	14.1.3	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.	No				X	
	14,2	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.						
	14.2.1	Se deberían establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.	No				X	
	14.2.2	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.	No				X	
	14.2.3	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.	No					X
	14.2.4	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.	No				X	
	14.2.5	Se deberían establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	No					X

ISO 27001:2013 Controles de Seguridad	Núm.	Descripción	Exclusión (Sí / No)	Justificación de exclusión	Controles seleccionados y razones de selección (justificación inclusión)			
					RL	OC	RN/MP	RVR
	14.2.6	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.	No				X	
	14.2.7	La organización debería supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	No				X	
	14.2.8	Durante el desarrollo se deberían llevar a cabo pruebas de funcionalidad de la seguridad.	No				X	
	14.2.9	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados.	No					X
	14,3	Objetivo: Asegurar la protección de los datos usados para pruebas.						
	14.3.1	Control: Los datos de ensayo se deberían seleccionar, proteger y controlar cuidadosamente.	No				X	
	15							
15 Relaciones con Proveedores	15,1	Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.						
	15.1.1	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.	No			X		
	15.1.2	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.	No			X		
	15.1.3	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.	No			X		
	15,2	Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.						
	15.2.1	Las organizaciones deberían hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	No					X
	15.2.2	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.	No			X		
	16							
16 Gestión de Incidentes de Seguridad de la Información	16,1	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.						
	16.1.1	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.	No					X
	16.1.2	Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible.	No					X
	16.1.3	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.	No				X	
	16.1.4	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	No				X	
	16.1.5	Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	No					X
	16.1.6	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.	No					X
	16.1.7	La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	No				X	
	17							

ISO 27001:2013 Controles de Seguridad	Núm.	Descripción	Exclusión (Sí / No)	Justificación de exclusión	Controles seleccionados y razones de selección (justificación inclusión)			
					RL	OC	RN/MP	RVR
17 Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio	17,1	Objetivo: La continuidad de seguridad de la información se debería incluir en los sistemas de gestión de la continuidad de negocio de la organización.						
	17.1.1	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	No				X	
	17.1.2	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	No				X	
	17.1.3	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 válidos y eficaces durante situaciones adversas.	No					X
	17,2	Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.						
	17.2.1	Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	No				X	
	18							
18 Cumplimiento	18,1	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.						
	18.1.1	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.	No		X			
	18.1.2	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	No		X			
	18.1.3	Los registros se deberían proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	No		X	X		
	18.1.4	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.	No		X			
	18.1.5	Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	No		X			
	18,2	Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.						
	18.2.1	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.	No					X
	18.2.2	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.	No					X
	18.2.3	Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	No					X

Elaboró: Carlos Javier Obañez Serna - Oficina de Seguridad de la Información

Aprobó: Hugo Alcides Perez Pinilla - Jefe Oficina de Seguridad de la Información