Controles de la Seguridad de la Información

(Responsabilidades ISO/IEC OFICIAL DE SEGURIDAD)

REQ	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
5	**Controles Organizacionales**	
5.1	Políticas para la seguridad de la información.	**Control** **La política de seguridad de la información y un conjunto de políticas temáticas especificas deben ser definidas, aprobadas por la dirección, publicadas, comunicadas y reconocidas por el personal pertinente y las partes interesadas relevantes, y revisadas a intervalos planificados y si se producen cambios significativos.**
5.2	Roles y responsabilidades en seguridad de la información.	**Control** **Todos los roles y responsabilidades de seguridad de la información deben definirse y asignarse de acuerdo con las necesidades de la organización.**
5.3	Segregación de tareas.	**Control** **Las funciones y areas de responsabilidad en conflicto deben segregarse.**
5.4	Responsabilidades de la Dirección.	**Control** **La dirección debe exigir a todo el personal que aplique la seguridad de la información de acuerdo con la política de seguridad de la información, las políticas temáticas y sus procedimientos específicos establecidos en la organización.**
5.5	Contacto con las autoridades.	**Control** **Deben establecerse y mantenerse los contactos adecuados con las autoridades pertinentes.**
5.6	Contacto con grupos de interés Especial.	**Control** **Deben establecerse y mantenerse los contactos apropiados con grupos de interés especial, u otros foros. y asociaciones profesionales especializados en seguridad.**
5.7	Inteligencia de amenazas.	**Control** **La información relativa a las amenazas a la seguridad de la información debe recopilarse y analizarse para producir información sobre amenazas.**
5.8	Seguridad de la información en la gestión de proyectos.	**Control** **La seguridad de la información debe integrarse en la gestión de proyectos.**
5.9	Inventario de información y otros activos asociados.	**Control** **Debe elaborarse y mantenerse un inventario de la información y otros activos asociados, incluyendo la identificación de sus propietarios.**

Atención a Clientes
Lic. Alejandra Morales / Ing Gerardo García
Dirección Comercial WST / Dirección Operaciones WST
55 6581 0662 / 55 6581 0123
licmorales@iso-irca.com / inggarcia@iso-irca.com

Controles de la Seguridad de la Información

(Responsabilidades ISO/IEC OFICIAL DE SEGURIDAD)

REQ	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
5.10	Uso aceptable de la información y activos asociados.	**Control** **Se deben identificar, documentar e implementar regias para el uso aceptable y procedimientos para el manejo de información y otros activos asociados.**
5.11	Devolución de activos.	**Control** **Todos los empleados y otras terceras partes, según procedan. deben devolver todos los activos de la organización en tu poder tras el cambio o la terminación de su trabajo, contrato o acuerdo.**
5.12	Clasificación de la información.	**Control** **La información debe clasificarse de acuerdo con las necesidades de seguridad de la información de la organización en función de la confidencialidad, integridad, disponibilidad y los requisitos pertinentes de las partes interesadas.**
5.13	Etiquetado de la información.	**Control** **Debe desarrollarse e implantarse un conjunto adecuado de procedimientos para etiquetar la información, de acuerdo con el esquema de clasificación adoptado por la organización.**
5.14	Transferencia de la información.	**Control** **Deben existir reglas, procedimientos o acuerdos de transferencia de información para todos los tipos de medios de transferencia dentro de la organización y entre la organización y otras partes.**
5.15	Control de acceso.	**Control** **Se deben establecer e implementar regias de control de acceso físico y lógico a la información y otros activos asociados, basadas en los requisitos de negocio y de seguridad dela información.**
5.16	Gestión de identidad.	**Control** **Se debe gestionar el ciclo de vida completo de las identidades.**
5.17	Información de autenticación.	**Control** **La aslgnaci6n y Gestión de la información de autenticación debe controlarse mediante un proceso formal de gestión. incluyendo el asesoramiento al personal sobre el tratamiento adecuado de la información de autenticación.**
5.18	Derechos de acceso	**Control** **Los derechos de acceso a la información y otros activos asociados deben aprovisionarse, revisarse, modificarse y eliminarse de conformidad con la política específica de la organización y las reglas sobre control de acceso.**

Atención a Clientes
Lic. Alejandra Morales / Ing Gerardo García
Dirección Comercial WST / Dirección Operaciones WST
55 6581 0662 / 55 6581 0123
licmorales@iso-irca.com / inggarcia@iso-irca.com

Controles de la Seguridad de la Información

(Responsabilidades ISO/IEC OFICIAL DE SEGURIDAD)

REQ	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
5.19	Seguridad de la información en las relaciones con los proveedores.	**Control** **Se deben identificar e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con el uso de los productos o servicios de proveedores.**
5.20	Abordar la seguridad de la información dentro de los acuerdos de proveedores.	**Control** **Deben establecerse y acordarse con cada proveedor los requisitos pertinentes de seguridad de la información en función del tipo de relación con el proveedor.**
5.21	Gestión de la seguridad de la información en la cadena de suministro de los TIC.	**Control** **Se deben definir e implementar procesos y procedimientos para hacer frente a los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de Tecnologías de la Información y de las Comunicaciones (TIC).**
5.22	Seguimiento, revisión y gestión del cambio de los servicios de proveedores.	**Control** **La organización debe supervisar, revisar, evaluar y gestionar regularmente los cambios en las prácticas de seguridad de la información y prestación de servicios de los proveedores.**
5.23	Seguridad de la información para el uso de servicios en la nube.	**Control** **Los procesos de adquisición, uso, gestión y finalización de los servicios en la nube deben establecerse de acuerdo con los requisitos de seguridad de la información de la organización.**
5.24	Planificación y preparación de la gestión de incidentes de seguridad de información	**Control** **La organización debe planificar y prepararse para gestionar los incidentes de seguridad de la información mediante la definición, el establecimiento y la comunicación de los procesos, roles y responsabilidades de gestión de los incidentes de seguridad de la información.**
5.25	Evaluación y decisión sobre los eventos de seguridad de información.	**Control** **La organización debe evaluar los eventos de seguridad de la información y decidir si deben ser catalogados como incidentes de seguridad de la información.**
5.26	Respuesta a incidentes de seguridad de la información.	**Control** **Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados.**
5.27	Aprender de los incidentes de seguridad de la información.	**Control** **El conocimiento adquirido a partir de los incidentes de seguridad de la información debe utilizarse para fortalecer y mejorar los controles de seguridad de la información.**

Atención a Clientes
Lic. Alejandra Morales / Ing Gerardo García
Dirección Comercial WST / Dirección Operaciones WST
55 6581 0662 / 55 6581 0123
licmorales@iso-irca.com / inggarcia@iso-irca.com

Controles de la Seguridad de la Información

(Responsabilidades ISO/IEC OFICIAL DE SEGURIDAD)

REQ	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
5.28	Recopilación de evidencias.	**Control** **La organización debe establecer e implementar procedimientos para la identificación, recogida, adquisición y preservación de evidencias relacionadas con eventos de seguridad de la información.**
5.29	Seguridad de la información durante la interrupción.	**Control** **La organización debe planificar cómo mantener la seguridad de la información a un nivel adecuado durante la Interrupción.**
5.30	Preparación para las TIC para la continuidad del negocio.	**Control** **La resiliencia de las TIC debe planificarse, implantarse, mantenerse y probarse en función de los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC.**
5.31	Identificación de requisitos legales, reglamentarios y contractuales.	**Control** **Los requisitos legales, estatuarios, reglamentarios y contractuales pertinentes para la seguridad de la información y el enfoque de la organización para cumplir con estos requisitos deben ser identificados, documentados y mantenerse actualizados.**
5.32	Derechos de propiedad intelectual (DPI).	**Control** **La organización debe implementar procedimientos apropiados para proteger los derechos de propiedad intelectual (DPI).**
5.33	Protección de los registros.	**Control** **Los registros deben ser protegidos contra la pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada.**
5.34	Privacidad y protección de datos de carácter personal (DCP).	**Control** **La organización debe identificar y cumplir con los requisitos relativos a la preservación de la privacidad y la protección de datos de carácter personal (DCP)de acuerdo con las leyes y regulaciones aplicables y los requisitos contractuales.**
5.35	Revisión independiente de la seguridad de la información.	**Control** **El enfoque de la organización para gestionar la seguridad de la información y su implementación, incluidos los procesos, la tecnología y las personas, debe revisarse de forma independiente a intervalos planificados o siempre que se produzcan cambios significativos.**
5.36	Cumplimiento de las políticas y normas de seguridad de la información.	**Control** **Debe comprobarse periódicamente el cumplimiento con la política de seguridad de la información, las políticas específicas, las reglas y las normas de la organización.**

Atención a Clientes
Lic. Alejandra Morales / Ing Gerardo García
Dirección Comercial WST / Dirección Operaciones WST
55 6581 0662 / 55 6581 0123
licmorales@iso-irca.com / inggarcia@iso-irca.com

Controles de la Seguridad de la Información

(Responsabilidades ISO/IEC OFICIAL DE SEGURIDAD)

REQ	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
5.37	Documentación de procedimientos operacionales.	**Control** **Deben documentarse los procedimientos operacionales de los medios de tratamiento de la información y ponerse a disposición de todos los usuarios que los necesiten.**
6	Personas	
6.1	Comprobación.	**Control** **La comprobación de los antecedentes de todos los candidatos al puesto de trabajo se debe llevar a cabo antes de unirse a la organización y de forma continua, de acuerdo con las leyes, reglamentos y éticas aplicables, y debe ser proporcional a los requisitos empresariales, la clasificación de la información a la que se acceden y los riesgos percibidos.**
6.2	Términos y condiciones de contracción.	**Control** **Los acuerdos contractuales de empleo deben indicar las responsabilidades del personal y de la organización en materia de seguridad de la información.**
6.3	Concienciación, educación y formación en seguridad de la información	**Control** **El personal de la organización y las partes interesadas pertinentes deben recibir una adecuada concienciación, educación y formación sobre seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización y de las políticas y los procedimientos específicos, según corresponda a su puesto de trabajo.**
6.4	Proceso disciplinario.	**Control** **Debe existir un proceso disciplinario formal que haya sido comunicado a los empleados y partes interesadas pertinentes, que recoja las acciones a tomar ante aquellos que hayan provocado alguna brecha de seguridad.**
6.5	Responsabilidad ante la finalización o cambio.	**Control** **Las responsabilidades y obligaciones en seguridad de la información que siguen vigentes después del cese o cambio de empleo se deben definir, hacer cumplir. y comunicar al personal pertinente y a otras partes interesadas.**
6.6	Acuerdos de confidencialidad o no divulgación.	**Control** **Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de protección de la información de la organización deben ser identificados, documentados, revisados regularmente y firmados por el personal y otras partes interesadas pertinentes.**

Atención a Clientes
Lic. Alejandra Morales / Ing Gerardo García
Dirección Comercial WST / Dirección Operaciones WST
55 6581 0662 / 55 6581 0123
licmorales@iso-irca.com / inggarcia@iso-irca.com

Controles de la Seguridad de la Información

(Responsabilidades ISO/IEC OFICIAL DE SEGURIDAD)

REQ	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
6.7	Teletrabajo.	**Control** **Se implementarán medidas de seguridad cuando el personal trabaje de forma remota para proteger la información a la que se acceda, procese o almacene fuera de las instalaciones de la organización.**
6.8	Notificación de los eventos de seguridad de la información.	**Control** **La organización debe proporcionar un mecanismo para que el personal notifique a tiempo eventos de seguridad de la Información observados o sospechosos a través de los canales apropiados.**
7	Infraestructura.	
7.1	Perímetro de seguridad física.	**Control** **Se deben definir y utilizar perímetros de seguridad para proteger áreas que contengan información y otros activos asociados.**
7.2	Controles físicos de entrada	**Control** **Las áreas seguras deben ser protegidas por controles de entrada y puntos de acceso adecuados.**
7.3	Seguridad de oficinas, despachos y recursos	**Control** **Para las oficinas, despachos y recursos, se debe diseñar y aplicar la seguridad física.**
7.4	Monitorización de la seguridad física.	**Control** **Las instalaciones deben ser monitorizadas continuamente para detectar cualquier acceso físico no autorizado.**
7.5	Protección contra las amenazas físicas y ambientales.	**Control** **Se debe diseñar e implementar una protección a las Infraestructuras contra las amenazas físicas y ambientales, como los desastres naturales y otras amenazas físicas intencionadas o no.**
7.6	El trabajo en areas seguras.	**Control** **Se debe diseñar e implementar procedimientos para trabajar en las áreas seguras.**
7.7	Puesto de trabajo despejado y pantalla limpia.	**Control** **Deben definirse y hacerse cumplir reglas de puesto de trabajo despejado de papeles y de medios de almacenamiento removibles, así como reglas de pantalla limpia para los recursos de tratamiento de la información.**
7.8	Emplazamiento y protección de equipos	**Control** **Los equipos deben situarse de forma protegida y segura.**

Atención a Clientes
Lic. Alejandra Morales / Ing Gerardo García
Dirección Comercial WST / Dirección Operaciones WST
55 6581 0662 / 55 6581 0123
licmorales@iso-irca.com / inggarcia@iso-irca.com

Controles de la Seguridad de la Información

(Responsabilidades ISO/IEC OFICIAL DE SEGURIDAD)

REQ	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
7.9	Seguridad de los equipos fuera de las instalaciones	**Control** **Los activos fuera de las instalaciones deben estar protegidos.**
7.10	Soportes de almacenamiento.	**Control** **Los soportes de almacenamiento deben gestionarse durante todo su ciclo de vida de adquisición, uso, trasporte y eliminación de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización.**
7.11	Instalaciones de suministro.	**Control** **Las instalaciones de procesamiento de información deben estar protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro.**
7.12	Seguridad del cableado.	**Control** **El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información debe estar protegido frente a interceptaciones, interferencias o daños.**
7.13	Mantenimiento de los equipos.	**Control** **Los equipos deben recibir un mantenimiento correcto que asegure la disponibilidad, integridad y confidencialidad de la información.**
7.14	Eliminación o reutilización segura de equipos.	**Control** **Todos los soportes de almacenamiento deben ser comprobados para confirmar que todo dato sensible y software bajo licencia, han sido eliminados o sobrescritos de manera segura. antes de deshacerse de ellos o reutilizarlos.**
8	Tecnología	
8.1	Dispositivos finales de usuario.	**Control** **La información almacenada, procesada o accesible a través de dispositivos finales de usuario debe protegerse.**
8.2	Gestión de privilegios de acceso.	**Control** **La asignación y el uso de derechos de acceso con privilegios deben restringirse y controlarse.**
8.3	Restricción del acceso a la información.	**Control** **Se debe restringir el acceso a la información y otros activos relacionados, de acuerdo con las políticas específicas de control de acceso definidas.**
8.4	Acceso al código fuente.	**Control** **Se debe gestionar adecuadamente el acceso de lectura y escritura al código fuente, a las herramientas de desarrollo y a las bibliotecas de software.**

Atención a Clientes
Lic. Alejandra Morales / Ing Gerardo García
Dirección Comercial WST / Dirección Operaciones WST
55 6581 0662 / 55 6581 0123
licmorales@iso-irca.com / inggarcia@iso-irca.com

Controles de la Seguridad de la Información

(Responsabilidades ISO/IEC OFICIAL DE SEGURIDAD)

REQ	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
8.5	Autenticación segura.	**Control** **Las tecnologías y procedimientos de autenticación segura deben implementarse en función de las restricciones de acceso a la información y la política específica sobre control de acceso.**
8.6	Gestión de capacidades.	**Control** **Se debe supervisar y ajustar la utilización de los recursos en consonancia con los requisitos de capacidad actuales y esperados.**
8.7	Controles contra el código Malicioso.	**Control** **Se debe implementar una protección contra el código malicioso, respaldada por una concienciación ademada al usuario.**
8.8	Gestión de vulnerabilidades técnicas.	**Control** **Se debe obtener información acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas.**
8.9	Gestión de la configuración.	**Control** **Se debe ser establecer, documentar, implementar, monitorizar y revisar las configuraciones de hardware, software, servicios y redes, incluyendo sus configuraciones de seguridad.**
8.10	Eliminación de la información.	**Control** **La información almacenada en los sistemas de información, en los dispositivos y cualquier otro medio de almacenamiento debe eliminarse cuando ya no sea necesaria.**
8.11	Enmascaramiento de datos.	**Control** **El enmascaramiento de datos debe utilizarse de acuerdo con la política específica del tema de la organización sobre et control de acceso, con otras políticas temáticas relacionadas, así como con los requisitos de negocio. teniendo en cuenta los requisitos legales aplicables.**
8.12	Prevención de fugas de datos.	**Control** **Se deben aplicar medidas de prevención de fugas de datos a sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información confidencial.**
8.13	Copias de seguridad de la información.	**Control** **Las copias de seguridad de la información, del software y de los sistemas deben mantenerse y probarse periódicamente de acuerdo con la política de copias de seguridad específica acordada.**

Atención a Clientes
Lic. Alejandra Morales / Ing Gerardo García
Dirección Comercial WST / Dirección Operaciones WST
55 6581 0662 / 55 6581 0123
licmorales@iso-irca.com / inggarcia@iso-irca.com

Controles de la Seguridad de la Información

(Responsabilidades ISO/IEC OFICIAL DE SEGURIDAD)

REQ	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
8.14	Redundancia recursos de tratamiento de la información.	**Control** **Los recursos de tratamiento de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.**
8.15	Registros de eventos	**Control** **Se deben generar, proteger, almacenar y analizar los registros de las actividades, excepciones, fallos y otros eventos relevantes.**
8.16	Seguimiento de actividades.	**Control** **Las redes, los sistemas y las aplicaciones deben monitorizarse en busca de comportamientos anómalos y se deben tomar medidas adecuadas para evaluar posibles incidentes de seguridad de la información.**
8.17	Sincronización de Reloj.	**Control** **Los relojes de los sistemas de procesamiento de información utilizados por la organizaci6n deben sincronizarse con fuentes de tiempo aprobadas.**
8.18	Uso de los programas de utilidad con privilegios.	**Control** **Se debe restringir y controlar rigurosamente el us0 de programas de utilidad que puedan ser capaces de invalidar los controles del sistema y de la aplicación.**
8.19	Instalación del software en sistemas en producción.	**Control** **Deben implementarse procedimientos y medidas para gestionar de forma segura la instalación de software en los sistemas en producción.**
8.20	Seguridad de redes.	**Control** **Las redes y los dispositivos de red deben estar protegidos, gestionados y controlados para proteger la información en los sistemas y aplicaciones.**
8.21	Seguridad de los servicios de red.	**Control** **Se deben identificar, implementar y monitorizar los mecanismos de seguridad, los niveles de severo y los requisitos de servicio de todos los servicios de red.**
8.22	Segregación en redes.	**Control** **Los grupos de servicios de información, de usuarios y de sistemas de información deben ser segregados en las redes de la organización.**

Atención a Clientes
Lic. Alejandra Morales / Ing Gerardo García
Dirección Comercial WST / Dirección Operaciones WST
55 6581 0662 / 55 6581 0123
licmorales@iso-irca.com / inggarcia@iso-irca.com

Controles de la Seguridad de la Información

(Responsabilidades ISO/IEC OFICIAL DE SEGURIDAD)

REQ	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
8.23	Filtrado de webs.	**Control** **El acceso a sitios web externos debe gestionarse para reducir la exposición a contenido malicioso.**
8.24	Uso de la criptografía.	**Control** **Deben definirse e implementarse reglas para el uso eficaz de la criptografía, incluida para la gestión de claves criptográficas.**
8.25	Seguridad en el ciclo de vida del desarrollo	**Control** **Se deben establecer y aplicar reglas para el desarrollo seguro de aplicaciones y sistemas.**
8.26	Requisitos de seguridad de las aplicaciones.	**Control** **Los requisitos de seguridad de la información deben identificarse, especificarse y aprobarse al desarrollar' o adquirir aplicaciones.**
8.27	Arquitectura segura de sistemas y principios de ingeniería.	**Control** **Los principios de ingeniería de sistemas seguros se deben establecer, documentar, mantener y aplicar a todas las actividades de desarrollo de sistemas de información.**
8.28	Codificación segura.	**Control** **Principios de codificaci6n segura deben aplicarse al desarrollo de software.**
8.29	Pruebas de seguridad en desarrollo y aceptación.	**Control** **Deben definirse e implementarse procesos de pruebas de seguridad en el ciclo de vida del desarrollo.**
8.30	Externalización del desarrollo.	**Control** **La organización debe controlar, monitorizar y revisar las actividades relativas al desarrollo externalizado de sistemas.**
8.31	Separación de los entornos de desarrollo. prueba y producción.	**Control** **Deben separarse y protegerse los entornos de desarrollo, prueba y producción.**
8.32	Gestión de cambios.	**Control** **Los cambios en las instalaciones de tratamiento de información y los sistemas de información deben estar sujetos a procedimientos de gestión de cambios.**
8.33	Datos de prueba.	**Control** **Los datos de prueba se deben seleccionar con cuidado y deben ser protegidos y controlados.**

Atención a Clientes
Lic. Alejandra Morales / Ing Gerardo García
Dirección Comercial WST / Dirección Operaciones WST
55 6581 0662 / 55 6581 0123
licmorales@iso-irca.com / inggarcia@iso-irca.com

REQ	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
8.34	Protección de los sistemas de información durante las pruebas de auditoría.	**Control** **Las pruebas de auditoría y otras actividades de aseguramiento en la evaluación de los sistemas en producción deben ser cuidadosamente planificadas y acordadas entre el evaluador y los gestores adecuados.**

Atención a Clientes
Lic. Alejandra Morales / Ing Gerardo García
Dirección Comercial WST / Dirección Operaciones WST
55 6581 0662 / 55 6581 0123
licmorales@iso-irca.com / inggarcia@iso-irca.com