

NORMA	BENEFICIO REQUISITOS EXIGIBLES	CONTROL	DESCRIPCIÓN DEL CONTROL	ETAPA DE OBTENCIÓN DEL DOCUMENTO DE REPORTE	RESPONSABLE DE OBTENER EL DOCUMENTO DE REPORTE	FÁBRICAS DE DESARROLLO	PROVEEDORES DE APLICACIONES, SOFTWARE O INFRAESTRUCTURA TI	PROVEEDORES DE REDES Y COMUNICACIONES	CALIFICADORAS DE VALORES	SERVICIOS DE AUDITORÍA, CONSULTORÍA, REVISORÍA	SERVICIOS JURIDICOS	SOPORTE UPS Y PLANTAS ELÉCTRICAS	PROVEEDORES DE MENSAJERÍA	COMPAÑÍAS DE SEGURIDAD PRIVADA	PROVEEDURA DE PRECIOS	CUSTODIO DE VALORES	FUENTE DE INFORMACIÓN FINANCIERA	INTERMEDIACIÓN DE VALORES (BROKER)
<b>A.5 Políticas de Seguridad</b>																		
Continuación de la descripción para la gestión de la seguridad de la información																		
2013	A.5.1.1	Política para la seguridad de la información	La Dirección debe definir, aprobar, publicar y comunicar a todos los empleados y a las partes externas pertinentes, un grupo de políticas para la seguridad de la información.	Previo al contrato	Supervisor de contrato													
2013	A.5.1.2	Revisión de las políticas para la seguridad de la información	Se debe revisar las políticas de seguridad de la información a intervalos planificados, o si se producen cambios significativos, para asegurar su conveniencia, suficiencia y eficiencia intercorreladas.	Previo al contrato	Supervisor de contrato													
<b>A.6 Organización de la Seguridad de la Información</b>																		
<b>A.6.1 Organización interna</b>																		
2013	A.6.1.1	Roles y Responsabilidades de Seguridad de la Información	Todas las responsabilidades de la seguridad de la información deben ser definidas y asignadas.	Previo al contrato	Supervisor de contrato													
2013	A.6.1.2	Segregación de deberes	Se debe asignar las funciones y las áreas de responsabilidad para reducir las oportunidades de modificaciones no autorizadas o no intencionales, o el uso inadecuado de los activos de la organización.	Previo al contrato	Supervisor de contrato													
2013	A.6.1.3	Contacto con las autoridades	Se deben mantener los contactos apropiados con las autoridades pertinentes.	Previo al contrato	Supervisor de contrato													
2013	A.6.1.4	Contacto con grupos de interés especial	Se deben mantener los contactos apropiados con los grupos especiales de interés u otros foros especiales en seguridad, así como asociaciones profesionales.	Previo al contrato	Supervisor de contrato													
2013	A.6.1.5	Seguridad de la información en la gestión de proyectos	Se deben abordar la seguridad de la información en la gestión de proyectos, sin importar el tipo de proyecto.	Previo al contrato	Supervisor de contrato													
<b>A.6.2 Dispositivos móviles y hardware</b>																		
2013	A.6.2.1	Política para dispositivos móviles	Se debe adoptar una política y medidas de apoyo a la seguridad para gestionar los riesgos asociados al uso de dispositivos móviles.	Previo al contrato	Supervisor de contrato													
2013	A.6.2.2	Teletrabajo	Se debe implementar una política y medidas de apoyo a la seguridad para proteger la información a la que se accede, procesa o almacena en los lugares de trabajo remoto.	Previo al contrato	Supervisor de contrato													
<b>A.7 Seguridad de los Recursos Humanos</b>																		
<b>A.7.1 Antes de asumir el empleo</b>																		
2013	A.7.1.1	Selección	Se debe realizar la verificación de antecedentes en todos los candidatos al empleo, de acuerdo a las leyes, regulaciones y normas éticas relevantes y en proporción a los requisitos del trabajo; la clasificación de la información a ser accedida y los riesgos pertinentes.	Previo al contrato	Supervisor de contrato													
2013	A.7.1.2	Términos y condiciones de empleo	Los acuerdos contractuales con los empleados y contratistas deben indicar sus responsabilidades y las de la organización en cuanto a seguridad de la información.	Previo al contrato	Supervisor de contrato	X	X	X	X	X	X	X	X	X	X	X	X	X
<b>A.7.2 Durante el empleo</b>																		
2013	A.7.2.1	Responsabilidades de la dirección	La dirección debe solicitar a todos los empleadores y contratistas que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	Previo al contrato	Supervisor de contrato													
2013	A.7.2.2	Concientización sobre la seguridad de la información y la formación	Todos los empleados de la organización, en donde sea pertinente, los contratistas deben recibir formación y actualización en conciencia y actualizaciones regulares en políticas y procedimientos organizacionales pertinentes para su función laboral.	Previo al contrato	Supervisor de contrato	X	X	X	X	X	X	X	X	X	X	X	X	X
2013	A.7.2.3	Proceso disciplinario	Debe existir un proceso disciplinario formal y conocido por los empleados para tomar acciones en contra de los empleados que hayan cometido una infracción a la seguridad de la información.	Previo al contrato	Supervisor de contrato													
<b>A.7.3 Terminación y cambio de empleo</b>																		
2013	A.7.3.1	Terminación o cambio de responsabilidades de empleo	Se debe definir y comunicar las responsabilidades y funciones de la seguridad de la información que siguen en vigor después de la desvinculación o cambio de relación laboral.	Previo al contrato	Supervisor de contrato	X	X	X	X	X	X	X	X	X	X	X	X	X
<b>A.8 Control de Activos</b>																		
<b>A.8.1 Responsabilidad de los activos</b>																		
2013	A.8.1.1	Inventario de Activos	Los Activos asociados a la información y a las instalaciones de procesamiento de la información deben ser identificados y se deben mantener y realizar un inventario de dichos activos.	Previo al contrato	Supervisor de contrato													
2013	A.8.1.2	Propietario de los activos	Los activos que se mantienen en inventario, deben pertenecer a un dueño.	Previo al contrato	Supervisor de contrato													
2013	A.8.1.3	Uso aceptable de los activos	Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con la información y las instalaciones de procesamiento de la información.	Previo al contrato	Supervisor de contrato													
2013	A.8.1.4	Devolución de los activos	Todos los empleados y usuarios de terceros partes deben devolver todos los activos pertenecientes a la organización que estén en su poder, como consecuencia de la finalización de la relación laboral, controlada o acordada.	Previo al contrato	Supervisor de contrato	X	X	X	X	X	X	X	X	X	X	X	X	X
<b>A.8.2 Clasificación de la información</b>																		
2013	A.8.2.1	Clasificación de la información	La información debe ser clasificada en términos de requisitos legales, valor, criticidad y sensibilidad para la divulgación o modificación sin autoridad.	Previo al contrato	Supervisor de contrato	X	X	X	X	X	X	X	X	X	X	X	X	X
2013	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 al esquema de clasificación adoptado por la organización.	Previo al contrato	Supervisor de contrato													
2013	A.8.2.3	Manejo de activos	Se deben desarrollar e implementar los procedimientos para el manejo de activos, de acuerdo al esquema de clasificación de información adoptado por la organización.	Previo al contrato	Supervisor de contrato													
<b>A.8.3 Manejo de medios</b>																		
2013	A.8.3.1	Gestión de medios removibles	Se deben implementar los procedimientos para la gestión de los medios removibles, de acuerdo al esquema de clasificación adoptado por la organización.	Previo al contrato	Supervisor de contrato													
2013	A.8.3.2	Disposición de los medios	Se deben eliminar los medios de forma segura y sin peligro cuando no se necesite más, usando procedimientos formales.	EN EL DESARROLLO DEL CONTRATO	Supervisor de contrato													
2013	A.8.3.3	Transferencia de medios físicos	Los medios que contengan información se deben proteger contra acceso no autorizado, uso inadecuado o cómputo, durante el transporte.	Previo al contrato	Supervisor de contrato	X	X	X	X	X	X	X	X	X	X	X	X	X
<b>A.9 Control de Acceso</b>																		
<b>A.9.1 Restricción del acceso para el control de acceso</b>																		
2013	A.9.1.1	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos del negocio y de seguridad.	Previo al contrato	Supervisor de contrato													
2013	A.9.1.2	Acceso a redes	Los usuarios solo deben tener acceso directo a la red y a los servicios de la red para los que han sido autorizados específicamente.	Previo al contrato	Supervisor de contrato													
<b>A.9.2 Gestión de accesos de usuarios</b>																		
2013	A.9.2.1	Registro y cancelación del registro de usuarios	Se debe implementar un proceso de registro y cancelación de registro de usuario para habilitar la asignación de derechos de acceso.	EN EL DESARROLLO DEL CONTRATO	Supervisor de contrato													
2013	A.9.2.2	Suministro de acceso de usuarios	Debe existir un procedimiento formal de asignación de acceso de usuario, para asignar o revocar los derechos de acceso para todos los tipos de usuarios, a todos los sistemas y servicios.	EN EL DESARROLLO DEL CONTRATO	Supervisor de contrato													
2013	A.9.2.3	Gestión de derechos de acceso privilegiado	Se debe restringir y controlar la asignación y uso de los derechos de acceso privilegiado.	EN EL DESARROLLO DEL CONTRATO	Supervisor de contrato													
2013	A.9.2.4	Gestión de información de autenticación secreta	Se debe controlar la asignación de información de autenticación secreta mediante un proceso de gestión formal.	EN EL DESARROLLO DEL CONTRATO	Supervisor de contrato													
2013	A.9.2.5	Revisión de los derechos de acceso de usuarios	Los propietarios de activos deben revisar los derechos de acceso de los usuarios de manera periódica.	EN EL DESARROLLO DEL CONTRATO	Supervisor de contrato													
2013	A.9.2.6	Revisión o ajuste de los derechos de acceso de información y las instalaciones de procesamiento de información	Se deben retirar los derechos de acceso de todos los empleados y usuarios externos a la información y a las instalaciones de procesamiento de información, una vez que termine su relación laboral, controlada o acordada, o se ajuste según el cambio.	EN EL DESARROLLO DEL CONTRATO	Supervisor de contrato													
<b>A.9.3 Responsabilidades de los usuarios</b>																		
2013	A.9.3.1	Uso de información de autenticación secreta	Se debe exigir a los usuarios el cumplimiento de las prácticas de la organización en el uso de la información de autenticación secreta.	EN EL DESARROLLO DEL CONTRATO	Supervisor de contrato													
<b>A.9.4 Control de acceso al sistema y aplicaciones</b>																		
2013	A.9.4.1	Restricciones de acceso a la información	Se debe restringir el acceso a la información y a las funciones del sistema de aplicaciones, de acuerdo con la política de control de acceso.	Previo al contrato	Supervisor de contrato													
2013	A.9.4.2	Procedimiento de ingreso seguro	Cuando lo exija la política de control de acceso, el acceso a los sistemas y aplicaciones debe ser controlado por un procedimiento de inicio de sesión seguro.	Previo al contrato	Supervisor de contrato													
2013	A.9.4.3	Sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas, deben ser interactivos y deben asegurar confiabilidad de calidad.	Previo al contrato	Supervisor de contrato													
2013	A.9.4.4	Uso de programas en entornos privilegiados	Se debe restringir y controlar estrictamente el uso de programas utilitarios que pueden estar en entornos privilegiados.	Previo al contrato	Supervisor de contrato													
2013	A.9.4.5	Control de acceso a código fuente de programas	Se debe restringir el acceso al código fuente de los programas.	Previo al contrato	Supervisor de contrato	X	X											
<b>A.10 Control de Criptografía</b>																		
<b>A.10.1 Controles criptográficos</b>																		
2013	A.10.1.1	Política de uso de controles criptográficos	Se deben desarrollar e implementar una política sobre el uso, protección y tiempo de vida de los claves criptográficas para la protección de la información.	Previo al contrato	Supervisor de contrato													
2013	A.10.1.2	Gestión de claves criptográficas	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las claves criptográficas durante toda su vida útil.	Previo al contrato	Supervisor de contrato	X	X											
<b>A.11 Seguridad Física y del entorno</b>																		
<b>A.11.1 Áreas seguras</b>																		
2013	A.11.1.1	Perímetro de seguridad física	Se deben definir y utilizar perímetros de seguridad para proteger a las áreas que contienen su información sensible o crítica y a las instalaciones de procesamiento de información.	Previo al contrato	Supervisor de contrato													
2013	A.11.1.2	Control de acceso físico	Las áreas seguras deben estar protegidas por controles de entrada apropiados que aseguren que solo se permite el acceso personal autorizado.	Previo al contrato	Supervisor de contrato													
2013	A.11.1.3	Seguridad de oficinas, recibos e instalaciones	Se debe diseñar y aplicar la seguridad física en oficinas, salas e instalaciones.	Previo al contrato	Supervisor de contrato													
2013	A.11.1.4	Protección contra las amenazas externas y ambientales	Se debe diseñar y aplicar la protección física contra daños por desastre natural ataque malicioso o accidentales.	Previo al contrato	Supervisor de contrato		X	X										
2013	A.11.1.5	Trabajo en áreas seguras	Se deben diseñar y aplicar procedimientos para trabajar en áreas seguras.	Previo al contrato	Supervisor de contrato	X												
2013	A.11.1.6	Áreas de despacho, carga	Se deben controlar los puntos de acceso tales como áreas de entrega y de carga y otros puntos donde las personas no autorizadas pueden acceder a las instalaciones, y si es posible aislarlas de las instalaciones de procesamiento de la información, para evitar el acceso no autorizado.	Previo al contrato	Supervisor de contrato													
<b>A.11.2 Equipos</b>																		



2013	A.15.2.2	Gestión de cambios en los servicios de los proveedores	Se deben gestionar los cambios al suministro del servicio por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas de seguridad de la información existentes, procedimientos y controles al considerar la criticidad de la información y la reevaluación de los riesgos.	Previo al contrato	Supervisor de contrato	X	X	X	X											
<b>A.16 Gestión de incidentes de seguridad de la información</b>																				
<b>A.16.1 Responsabilidades y roles en la seguridad de la información</b>																				
2013	A.16.1.1	Responsabilidades y procedimientos	Se deben establecer responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y metódica a los incidentes de seguridad de la información.	Previo al contrato	Supervisor de contrato	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
2013	A.16.1.2	Reporte de eventos de seguridad de la información	Se deben informar, lo antes posible, los eventos de seguridad de la información mediante canales de gestión apropiados.	Previo al contrato	Supervisor de contrato	X	X	X	X											
2013	A.16.1.3	Resolución de incidencias de seguridad de la información	Se debe requerir que los empleados y contratistas que usen los sistemas y servicios de información de la organización observen e informen cualquier debilidad en la seguridad de la información, en los sistemas o servicios observada o que se sospeche.	Previo al contrato	Supervisor de contrato	X	X													
2013	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 decidir si van a ser clasificados como incidentes de seguridad de la información.	Previo al contrato	Supervisor de contrato															
2013	A.16.1.5	Respuesta a incidentes de seguridad de la información	Los incidentes de seguridad de la información deben ser atendidos de acuerdo a los procedimientos documentados.	Previo al contrato	Supervisor de contrato															
2013	A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Se debe utilizar el conocimiento adquirido al analizar y resolver incidentes de seguridad de la información para reducir la probabilidad o el impacto de incidentes futuros.	Previo al contrato	Supervisor de contrato	X	X	X	X											
2013	A.16.1.7	Recopilación de evidencia	La organización debe definir y aplicar los procedimientos para la identificación, recolección, adquisición y conservación de información que pueda servir de evidencia.	Previo al contrato	Supervisor de contrato															
<b>A.17 Aspectos de la seguridad de la información de la gestión de continuidad del negocio</b>																				
<b>A.17.1 Continuidad de seguridad de la información</b>																				
2013	A.17.1.1	Planificación de la continuidad de la seguridad de la información	La organización debe determinar sus requerimientos de 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.	Previo al contrato	Supervisor de contrato	X	X	X	X											
2013	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 necesario de continuidad para la seguridad de la información durante una situación adversa.	Previo al contrato	Supervisor de contrato			X	X											
2013	A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	La organización debe verificar, de manera periódica, los controles de continuidad de la seguridad de la información definida e implementada para asegurar que son válidos y eficaces durante situaciones adversas.	Previo al contrato	Supervisor de contrato	X	X	X	X											
<b>A.17.2 Restauración</b>																				
2013	A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	Las instalaciones de procesamiento de la información deben ser implementadas con el nivel de redundancia suficiente para cumplir con los requisitos de disponibilidad.	Previo al contrato	Supervisor de contrato	X	X	X	X											
<b>A.18 Cumplimiento</b>																				
<b>A.18.1 Cumplimiento de requisitos legales y contractuales</b>																				
2013	A.18.1.1	Identificación de la legislación aplicable de los requisitos contractuales	Todos los requisitos estatutarios, regulatorios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben definir y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	Previo al contrato	Supervisor de contrato															
2013	A.18.1.2	Derechos de propiedad intelectual (DPI)	Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos regulatorios, regulatorios y contractuales relacionados a los derechos de propiedad intelectual y al uso de productos de software patentados.	Previo al contrato	Supervisor de contrato	X	X													
2013	A.18.1.3	Protección de registros	Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso sin autorización y emisión sin autorización, de acuerdo con los requisitos legislativos, regulatorios, contractuales y del negocio.	Previo al contrato	Supervisor de contrato	X	X													
2013	A.18.1.4	Privacidad y protección de datos personales	Se debe asegurar la privacidad y protección de la información de identificación personal, como se exige en la legislación y regulaciones pertinentes, donde corresponda.	Previo al contrato	Supervisor de contrato			X	X											
2013	A.18.1.5	Regeneración de controles criptográficos	Se debe utilizar controles criptográficos que cumplan con todos los acuerdos, leyes y regulaciones pertinentes.	Previo al contrato	Supervisor de contrato	X	X		X											
<b>A.18.2 Revisiones de seguridad de la información</b>																				
2013	A.18.2.1	Revisión de la implementación 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, objetivos de control, controles, políticas, procesos y procedimientos de seguridad de la información) se debe revisar en forma independiente, a intervalos planificados, cuando ocurran cambios identificables.	Previo al contrato	Supervisor de contrato															
2013	A.18.2.2	Cumplimiento con las políticas y normas de seguridad	Los gerentes deben revisar con regularidad el cumplimiento del procesamiento y los procedimientos de seguridad que están dentro de su área de responsabilidades, de acuerdo con las políticas de seguridad, normas y otros requisitos de seguridad pertinentes.	Previo al contrato	Supervisor de contrato	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
2013	A.18.2.3	Revisión del cumplimiento técnico	Se deben verificar regularmente los sistemas de información en cuanto a su cumplimiento con las políticas y normas de seguridad de la información de la organización.	Previo al contrato	Supervisor de contrato	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

**OBSERVACIONES**

En caso de requerir información adicional o de generarse alguna duda e inquietud, póngase en contacto con el Coordinador del Sistema de Gestión de seguridad de la Información (SGSI) al correo [sgsinfo@incoproveia.com.ec](mailto:sgsinfo@incoproveia.com.ec), que hace parte de la Gerencia de Riesgos.