Políticas de Seguridad de la Información- Recomendadas por Logiscont

[2019]

1. CONTROL DE VERSIONES

Fuente de Cambio	Fecha de Solicitud del Cambio	Versión	Partes que Cambian	Descripción del Cambio	Fecha de Cambio
PSI-v0100		1.00	N/A		

Tabla de Contenido

2. INTRODUCCIÓN

Este documento es un conjunto de propuestas de políticas de seguridad de la información que sugieren como se debe manejar la seguridad en COOTRADIAN a partir de ellas se pueden desarrollar procedimientos detallados y guías de acción para casos de brechas y violaciones de seguridad.

Las políticas tratan los aspectos de manera genérica y dan base a las normas, las cuales hacen referencia específica a tecnologías, metodologías, procedimientos de implementación y otros aspectos de detalle. Asimismo, las políticas se proyectan para durar muchos años, a diferencia de las normas y procedimientos que pueden ir cambiando de acuerdo a las tecnologías y cambios en los procesos de negocios de la organización.

La importancia de las políticas radica en que, en primer lugar, son el punto de partida para establecer una infraestructura organizativa apropiada de seguridad, es decir, son los aspectos esenciales desde donde se derivan los otros aspectos de seguridad de la información. En segundo lugar, guían el proceso de selección e implantación de los productos de seguridad, y en tercer lugar, porque demuestran el apoyo de la Alta Dirección hacia los aspectos de seguridad de la información.

Además, las políticas pueden servir para evitar responsabilidades legales, ya que permiten aplicar controles para evitar contingencias de negligencia o violación de confidencialidad, fallas en el uso de medidas de seguridad, mala práctica, contra personas particulares u organizaciones que podrían reclamar por daños o perjuicios.

Se debe considerar la ***difusión de las políticas de seguridad*** de la información mediante diferentes tipos de documentos: los trabajadores podrían recibir un folleto que contiene las políticas de seguridad más importantes que ellos necesitan tener presente, el personal técnico podría recibir un documento más largo que proporcione más detalle y los contratistas pueden recibir un resumen de políticas confeccionado especialmente para ellos.

Una de las primeras acciones del Comité de Seguridad debería ser la revisión de estas recomendaciones. Este comité debería tener representantes de los distintos departamentos de la organización y en la evaluación debe considerar su viabilidad, análisis costo/beneficio y sus implicaciones. En todo caso, se debe tener en consideración que cualquier conjunto de políticas debe empezar por los aspectos esenciales, para luego ir ampliando con políticas adicionales.

Las políticas deben ***revisarse*** en forma periódica, preferiblemente cada año, para asegurarse de que todavía son pertinentes y efectivas. Es importante eliminar aquellas políticas que ya no son útiles o que ya no son aplicables. Este esfuerzo también ayudará a mejorar la credibilidad de las actividades de seguridad de la información dentro y fuera de la organización.

ISO 27002	POLITICAS COOTRADIAN	Descripción
5. Política de Seguridad		
5.1	**Política de la seguridad de la información**	
5.1.1	**Documento de política de la seguridad de la información**	
	Política 0501-001	Establecimiento de Políticas de Seguridad de la Información *La Alta Dirección de la organización se encargará de establecer, mantener y publicar las Políticas de Seguridad de la Información.*
5.1.2	**Revisión y evaluación**	
	Política 0501-002	Revisión de las Políticas de Seguridad de la Información *Las Políticas de Seguridad de la Información tendrán un propietario designado que será responsable de su mantenimiento y revisión de acuerdo a un **proceso definido**. En COOTRADIAN esta responsabilidad se delega en el Oficial de Seguridad de la Información.*
6. Aspectos Organizativos para la Seguridad		
6.1	**Organización para la seguridad de la información**	
6.1.1	**Comité Gerencial de Seguridad de la Información**	
6.1.1	Política 0601-001	Rol del Comité Gerencial de Seguridad de la Información *El comité gerencial de Seguridad de la Información se encargará de promover las iniciativas de Seguridad de la Información dentro de la organización, así como obtener los recursos necesarios para dichas actividades.*
6.1.2	**Coordinación de Seguridad de la Información**	
6.1.2	Política 0601-002	Rol de la alta dirección en la seguridad de la información *La Alta Dirección de la organización asignará una alta prioridad a la Seguridad de la Información en todas las actividades e iniciativas actuales y futuras.*
6.1.2	Política 0601-003	Actualizaciones sobre Seguridad de la Información para el Personal *La Alta Dirección se compromete a brindar a todo el personal, a través de las instancias correspondientes y de manera periódica, información relevante sobre Seguridad de la Información por diversos medios.*
6.1.3	**Asignación de responsabilidades sobre Seguridad de la Información**	

ISO 27002	POLITICAS COOTRADIAN	Descripción
6.1.3	Política 0601-004	Designación del Oficial de Seguridad de la Información (OSI). *Se designará al OSI que asuma la responsabilidad del desarrollo e implantación de la seguridad y respalde la identificación de las medidas de control. Sin embargo, la responsabilidad de proporcionar recursos e implantar las medidas de control permanecerá con los gerentes individuales y/o dueños de proceso.*
6.1.3	Política 0601-005	Administración de Sistemas *La gestión de los sistemas de información debe estar a cargo de un profesional o profesionales debidamente calificado(s), quien(es) será(n) responsable(s) de supervisar el funcionamiento y la seguridad de los sistemas. Debe(n) estar debidamente capacitado(s) y tener experiencia relevante en los sistemas y plataformas utilizadas por la organización. Además, debe(n) conocer y entender la gama de riesgos de Seguridad de la Información que requieren ser manejados.*
6.1.4	**Proceso de autorización de recursos para el tratamiento de la información**	
6.1.4	Política 0601-007	Especificación de los requisitos para nuevo equipamiento *Las requisiciones de compras significativas de nuevos equipos deben contar con un Expediente Técnico que detalle la especificación de los requerimientos del usuario, los requisitos de Seguridad de la Información, la prioridad, el cumplimiento de estándares técnicos y funcionales, y la relación con los objetivos a corto y largo plazo de la organización.*
6.1.4	Política 0601-008	Instalación de nuevo equipamiento *Todas las nuevas instalaciones de equipamiento, y sus respectivos requisitos de Seguridad de la Información, deben planificarse formalmente y notificarse a los interesados con la debida anticipación.*
6.1.4	Política 0601-009	Prueba de equipamiento y sistemas *Todo equipo debe probarse exhaustivamente y pasar por un proceso de aceptación formal de usuarios antes de ser transferido al entorno de producción.*

ISO 27002	POLITICAS COOTRADIAN	Descripción
6.1.4	Política 0601-010	Especificación de los requerimientos de usuario para software *Todos las solicitudes de desarrollo de sistemas nuevos o mejoras a los mismos deben presentarse a la gerencia mediante un documento de **"Especificaciones de requerimientos de usuario",** donde se define detalladamente los requerimientos técnicos y funcionales.*
6.1.4	Política 0601-011	Selección de paquetes de software comercial *La adquisición de software comercial debe hacerse, como regla general, a proveedores cuyo software esté debidamente probado en el mercado, y que cuente con el soporte adecuado.*
6.1.4	Política 0601-012	Selección de paquetes de software de ofimática *Todas los paquetes de software de oficina deben ser compatibles con el sistema operativo y plataforma de cómputo aprobados por la organización.*
6.1.5	**Asesoramiento de especialistas en seguridad de la información**	
6.1.5	Política 0601-013	Asesoría especializada en Seguridad de la Información *La institución buscará asesoría especializada sobre Seguridad de la Información de consultores internos o externos.*
6.1.6	**Cooperación entre organizaciones**	
6.1.6	Política 0601-014	Identificación de organizaciones relevantes *Se mantendrá un registro actualizado de todas las organizaciones relevantes que pudieran intervenir en casos de incidentes de seguridad, incluyendo los contactos responsables de coordinar dichos aspectos en tales organizaciones.*
6.1.7	**Revisión independiente de la seguridad de la información**	
6.1.7	Política 0601-015	Revisión periódica del documento de Políticas de Seguridad de la Información *El documento de Políticas de Seguridad de la Información será evaluado periódicamente por personas independientes o especialistas externos para garantizar que las prácticas organizacionales reflejan apropiadamente la política y que ésta es factible y eficaz.*
6.2	**Seguridad en los accesos de terceras personas**	
6.2.1	**Identificación de los riesgos por acceso de terceros**	

ISO 27002	POLITICAS COOTRADIAN	Descripción
6.2.1	Política 0602-001	Acceso de terceros *Se definirá y documentará formalmente los tipos de accesos de terceros a recursos de información de la organización, así como los motivos por los cuales se les puede otorgar dicho acceso.*
6.2.1	Política 0602-002	Permisos de acceso a terceros *Sólo se permitirá el acceso de terceros a información de la organización cuando dicha información esté aislada y que el riesgo de posibles accesos no autorizados esté debidamente controlado.*
6.2.2	**Requisitos de seguridad en contratos con terceros**	
6.2.2	Política 0602-003	Acuerdos de acceso a la información por terceros *Los acuerdos que permiten el acceso de terceros a recursos de tratamiento de información de la organización deberán estar basados en contratos formales que incluyan todos los requisitos de seguridad acordes con las políticas y normas de seguridad de la organización.*
6.2.2	Política 0602-004	Difusión de las políticas a contratistas y trabajadores temporales *Se entregará formalmente un **resumen de las Políticas de Seguridad** de la Información a todo contratista y/o trabajador temporal antes del inicio de sus servicios.*
6.2.2	Política 0602-005	Conformidad de trabajos hechos por terceros *Solamente las personas debidamente autorizadas expresamente pueden firmar la conformidad de trabajos hechos por terceros.*
6.2.2	Política 0602-006	Compra de software desarrollado por proveedores *El software desarrollado por terceros debe cumplir con las "Especificaciones de Requerimientos de Usuario" y ofrecer un soporte técnico apropiado. Tecnologías de la información debe garantizar la vigencia de los contratos de soporte de proveedores y sus respectivas actualizaciones.*
6.2.2	Política 0602-007	Brechas de confidencialidad de terceros *Las violaciones de confidencialidad de terceros deben ser reportadas al OSI tan pronto como sea posible.*

ISO 27002	POLITICAS COOTRADIAN	Descripción
6.2.2	Política 0602-008	Servicios externos de eliminación de material y equipo *Cualquier contratista usado para la eliminación externa de equipo y/o material obsoletos debe estar en capacidad de demostrar el cumplimiento de las Políticas de Seguridad de la Información de la organización.*
6.2.2	Política 0602-009	Soporte de software de aplicación *Todo software aplicativo debe tener un nivel apropiado de soporte técnico para garantizar que las operaciones de la organización no se vean perjudicadas, asegurándose que cualquier problema de software será manejado eficientemente en un tiempo razonable.*
7. Clasificación y control de Activos		
7.1	**Responsabilidad sobre los activos**	
7.1	Política 0701-001	Responsabilidad sobre los activos *Cada activo importante de información debe tener un propietario designado que será el responsable de establecer la seguridad de dicho activo y que se mantenga la protección adecuada.*
7.1	Política 0701-002	Defensa contra delitos informáticos *Los riesgos de los sistemas e información de la organización deben reducirse al mínimo fomentando la concientización y vigilancia del personal, e instalando sistemas y dispositivos de protección apropiados.*
7.1.1	**Inventario de activos**	
7.1.1	Política 0701-003	Mantenimiento del inventario de activos de información *La institución contará con un inventario formal de todos los activos de información, el cual estará actualizado de manera permanentemente.*
7.1.1	Política 0701-004	Gestión y uso de documentación de hardware *La documentación de hardware debe estar siempre actualizada y fácilmente accesible para el personal autorizado de soporte o mantenimiento.*

ISO 27002	POLITICAS COOTRADIAN	Descripción
7.1.1	Política 0701-005	Política de protección de marca *La entidad debe proteger sus marcas en las redes sociales, de manera que puedan seguir aprovechando la fuerza de estas redes con una cierta tranquilidad de espíritu.*
7.2	**Clasificación de la Información**	
7.2	Política 0702-001	Clasificación de Información *Todo activo de información: datos y documentos, debe clasificarse según su confidencialidad, valor para el negocio y sensibilidad.*
	Política 0702-002	Registro de activos de información *La organización debe mantener un registro actualizado de sus activos de información.*
7.2.1	**Guías de clasificación**	
7.2.1	Política 0702-003	Esquema de clasificación de activos de información *La institución contará con un esquema de clasificación de activos de información en función de su importancia, criticidad, integridad y disponibilidad para la organización. Cada propietario de activos de información será el responsable de definir y revisar periódicamente la clasificación de sus activos.*
7.2.1	Política 0702-004	Datos de beneficiarios, clientes y terceros *Se debe clasificar la información de contacto de beneficiarios, clientes y terceros como altamente confidencial y protegerla en consecuencia.*
7.2.1	Política 0702-005	Manejo de Información Financiera *La información financiera debe clasificarse como altamente confidencial y se deben tomar las medidas de seguridad necesarias (técnicas y administrativas) que protejan tal información de accesos no autorizados.*
7.2.2	**Marcado y tratamiento de la información**	
7.2.2	Política 0702-006	Etiquetado de información *Toda activo de información debe tener una etiqueta claramente visible a fin que los usuarios conozcan quien es el propietario y cuál es el nivel de clasificación designado.*

ISO 27002	POLITICAS COOTRADIAN	Descripción
7.2.2	Política 0702-007	Uso de nombres de archivos *Los nombres de archivos de datos de la organización deben tener un significado reconocible por los usuarios de dichos archivos.*
7.2.2	Política 0702-008	Indicación de niveles de seguridad en documentos *Dentro del encabezado y pie de página de todos los documentos se deberá indicar la clasificación del nivel de seguridad y el dueño del documento.*
7.2.2	Política 0702-009	Grabación periódica de datos por usuarios *A fin de prevenir daños o pérdida debido a malos funcionamientos del sistema o fallas de energía, los usuarios de sistemas de información que crean o modifican archivos de datos, deben grabar su trabajo de manera periódica usando las mejores prácticas.*
7.2.2	Política 0702-010	Gestión de borradores de informes *Los borradores de informes se deben actualizar solamente con autorización del dueño del documento. Las sucesivas versiones de borradores de informes no deben seguir en uso después de la elaboración de una versión final, se deben eliminar o archivar. Una sola versión del archivo debe conservarse para acceso de trabajo.*

8. Seguridad ligada al Personal		
8.1	**Seguridad en la definición del trabajo y los recursos**	
8.1.1	**Inclusión de la seguridad en las responsabilidades laborales**	
8.1.1	Política 0801-001	Inclusión de cláusulas en el contrato de trabajo ***El contrato de trabajo debe incluir cláusulas de cumplimiento de la Seguridad de la Información.***
8.1.1	Política 0801-002	Responsabilidad de los empleados sobre datos confidenciales *Todos los trabajadores que tengan acceso a información clasificada como confidencial deben firmar cláusulas de protección de la confidencialidad de dicha información, durante y después de la relación contractual con la organización.*
8.1.2	**Selección y política de personal**	

ISO 27002	POLITICAS COOTRADIAN	Descripción
8.1.2	Política 0801-003	Contratación de nuevo personal *Debe existir un mecanismo de verificación de identificación, referencias de nuevos trabajadores, el cual corresponderá al nivel de las responsabilidades que se le asignarán. En los casos de responsabilidades financieras, se hará una verificación del crédito y de ser necesarios pruebas de polígrafo.*
8.1.3	**Compromiso de Confidencialidad**	
8.1.3	Política 0801-004	Acuerdos de confidencialidad *En los casos donde la información esté clasificada como confidencial, se deben generar y suscribir "Acuerdos de confidencialidad" por los trabajadores o terceros que tengan acceso a dicha información.*
8.1.3	Política 0801-005	Confidencialidad de las contraseñas y números PIN *Las contraseñas otorgadas a los trabajadores son privadas y altamente confidenciales. La violación a dicha confidencialidad puede dar lugar a una acción disciplinaria.*
8.1.3	Política 0801-006	Respuesta a requerimientos telefónicos *Las solicitudes telefónicas de información confidencial se deben canalizar a la plana ejecutiva para su atención. Sólo personas autorizadas pueden divulgar información reservada, previa verificación de la identidad de la persona que recibirá dicha información.*
8.1.3	Política 0801-007	Compartir información confidencial con otros *Toda información que no sea de dominio público, sobre asuntos de la organización y a sus trabajadores, no debe divulgarse, así sea a miembros de la familia o personas cercanas.*
8.1.3	Política 0801-008	Declaraciones a medios de comunicación *Sólo personas expresamente autorizadas pueden dirigirse a medios de difusión sobre temas referidos a la organización.*
8.1.4	**Términos y condiciones de la relación laboral**	

ISO 27002	POLITICAS COOTRADIAN	Descripción
8.1.4	Política 0801-009	Conocimiento de obligaciones legales *Las responsabilidades legales de los trabajadores en el uso de sistemas de información y datos computarizados de la organización* ***deben ser incluidas dentro de la documentación clave de personal tales como cláusulas del Contrato de Trabajo y Reglamento Interno de Trabajo****. La Dirección de Personal debe garantizar que todos los empleados estén completamente enterados de dichas responsabilidades.*
8.1.4	Política 0801-010	Respeto de la privacidad en el trabajo *La organización respeta la privacidad del trabajador en su lugar de trabajo; sin embargo, esto no limitará el derecho de la organización a tener acceso a la información creada y almacenada en equipos de la organización.*
8.2	**Capacitación de Usuarios**	
8.2.1	**Capacitación en seguridad de la información**	
8.2.1	Política 0802-001	Capacitación en Seguridad de la Información a trabajadores *La capacitación en Seguridad de la Información se impartirá de manera individual, obligatoria y actualizada a todos los trabajadores.*
8.2.1	Política 0802-002	Capacitación en Seguridad de la Información al personal técnico *La capacitación del personal técnico en Seguridad de la Información deberá estar actualizada y acorde con la responsabilidad de configurar y mantener las protecciones requeridas por la organización. Se debe priorizar la capacitación al Departamento de TI.*
8.2.1	Política 0802-003	Capacitación en Seguridad de la Información a personal nuevo *El personal nuevo debe recibir capacitación básica en Seguridad de la Información como parte del proceso de inducción.*
8.2.1	Política 0802-004	Programas de concientización para el personal permanente. *Se debe concientizar en temas de seguridad de la información al personal permanente de la institución mediante información actualizada sobre amenazas existentes y las medidas de seguridad apropiadas.*

ISO 27002	POLITICAS COOTRADIAN	Descripción
8.3	**Respuesta ante incidentes y malos funcionamientos de la seguridad**	
8.3	Política 0803-001	Investigación de causas e impacto de incidentes *Los incidentes de Seguridad de la Información deben ser investigados apropiadamente por personal debidamente capacitado.*
8.3.1	**Reporte de incidentes de seguridad**	
8.3.1	Política 0803-002	Reporte de incidentes de Seguridad de la Información *Los incidentes, sospechas de incidentes y brechas de seguridad de la información deben reportarse al OSI lo más rápidamente posible para agilizar las actividades de identificación de daños, reparación y recuperación, así como facilitar la recolección de evidencias.*
8.3.1	Política 0803-003	Reporte de incidentes de Seguridad de la Información a autoridades externas *Sólo se deben comunicar los incidentes de Seguridad de la Información a autoridades externas siempre que sea necesario debido a requisitos legales o regulatorios.*
8.3.2	**Reporte de debilidades de seguridad**	
8.3.2	Política 0803-004	Notificación de debilidades de Seguridad de la Información *Las debilidades o sospechas de debilidades de Seguridad de la Información deben notificarse al OSI lo más rápidamente posible.*
8.3.3	**Reporte de fallas de software**	
	Política 0803-005	Reporte de fallas de software *Las fallas de software deben ser reportadas **mediante un procedimiento existente** para tal fin*.
8.3.4	**Aprendiendo de los incidentes**	
8.3.4	Política 0803-006	Revisión del registro de incidentes de Seguridad de la Información *Se debe crear y mantener un registro de incidentes, sospechas de incidentes, brechas y amenazas a la seguridad de la información y las acciones correctivas identificadas. El registro debe estudiarse regularmente para tomar medidas de reducción del riesgo y frecuencia de los incidentes de la seguridad de la información en la organización.*
8.3.5	**Proceso disciplinario**	

ISO 27002	POLITICAS COOTRADIAN	Descripción
8.3.5	Política 0803-007	Cumplimiento de las Políticas de Seguridad de la Información *Cualquier incidente de seguridad originado por un incumplimiento de dichas políticas, podrá dar lugar a una* ***acción disciplinaria.***
9. Seguridad Física y del Entorno		
9.1	**Áreas Seguras**	
9.1.1	**Perímetro de Seguridad Física**	
9.1.1	Política 0901-001	Seguridad de ambientes de cómputo *Los ambientes que contengan computadoras deben protegerse contra cualquier intrusión física.*
9.1.1	Política 0901-002	Gestión de repositorios de datos *Los locales donde se almacenan datos o información deben tener controles de acceso para reducir el riesgo de pérdida o daño a un nivel aceptable.*
9.1.2	**Controles físicos de ingreso**	
9.1.2	Política 0901-003	Protección de acceso físico *Se debe controlar el acceso físico a ambientes de alta seguridad mediante técnicas de identificación y autenticación. Se debe tener un sistema de control que monitoree todos los intentos de acceso. Se debe informar al personal con autorización de ingreso a tales áreas sobre los riesgos de seguridad inherentes.*
9.1.3	**Seguridad de oficinas, despachos y recursos**	
9.1.3	Política 0901-004	Configuración de oficinas *Las oficinas deben estar configuradas para minimizar los daños por incendio, inundación, explosión, disturbio y otras formas de desastres naturales o provocados, así como amenazas que procedan de lugares vecinos.*
9.1.3	Política 0901-005	Seguridad de oficinas *Se deben instalar sistemas de detección de intrusos y probarse regularmente para cubrir todas las puertas externas y las ventanas accesibles. Las ventanas y puertas deben permanecer cerradas cuando la oficina esté vacía, y las alarmas deben estar activadas.*

ISO 27002	POLITICAS COOTRADIAN	Descripción
9.1.3	Política 0901-006	Almacenamiento seguro *El material y equipo con información sensible o valiosa deben almacenarse con seguridad y según el nivel de clasificación de la información almacenada.*
9.1.3	Política 0901-007	Desconfiar de extraños en los locales de la organización *Todos los trabajadores deben conocer la necesidad de desconfiar de extraños en los ambientes de la organización.*
9.1.4	**El trabajo en las Áreas Seguras**	
9.1.4	Política 0901-008	Acceso de terceros a las áreas seguras *El personal de terceros sólo podrá acceder a áreas seguras cuando sea aprobado expresamente y su acceso se supervisará. No se permitirá la presencia de equipos de fotografía, vídeo, audio u otras formas de registro salvo autorización especial.*
9.1.5	**Áreas de acceso público, entrega y recepción**	
9.1.5	Política 0901-009	Controles en áreas de acceso público *Las áreas de acceso público, entrega y recepción deben tener controles apropiados y, de ser posible, aislarse de los recursos de tratamiento de información para evitar accesos no autorizados.*
9.2	**Seguridad de los Equipos**	
9.2.1	**Instalación y protección de equipos**	
9.2.1	Política 0902-001	Preparación de ambientes para cómputo *Los lugares elegidos para instalar computadoras y almacenar datos deben protegerse convenientemente contra intrusión física, hurto, incendio, inundación, temperatura y humedad excesivas, y otros peligros.*
9.2.2	**Suministro eléctrico**	
9.2.2	Política 0902-002	Suministro continuo de energía eléctrica a equipos críticos *Se debe instalar fuentes de alimentación continua (UPS) donde sea necesario para asegurar la continuidad del servicio durante interrupciones del suministro eléctrico.*

ISO 27002	POLITICAS COOTRADIAN	Descripción
9.2.2	Política 0902-003	Gestión y mantenimiento de generadores de reserva *Se deben usar generadores de reserva cuando sea necesario para asegurar la continuidad del servicio durante interrupciones del suministro eléctrico.*
9.2.3	**Seguridad del cableado**	
9.2.3	Política 0902-004	Instalación y mantenimiento de cableado de red *El cableado de red debe ser instalado y mantenido por profesionales calificados. Cualquier punto de red que no esté en uso debe ser sellado y su estado registrado.*
9.2.3	Política 0902-005	Seguridad del cableado *La seguridad del cableado de red debe ser revisada cada vez que se hagan mejoras, cambios de equipo o de ambientes.*
9.2.4	**Mantenimiento de equipos**	
9.2.4	Política 0902-006	Mantenimiento de equipos *Todo equipo de la organización debe tener mantenimiento apropiado a cargo de profesionales calificados, lo cual debe reflejarse en un documento formal.*
9.2.4	Política 0902-007	Limpieza de equipos *Deben implementarse procedimientos de limpieza de equipos que no comprometan la seguridad de la información, ni la integridad de los equipos. Los materiales y personal de limpieza deben estar aprobados para dicha función.*
9.2.4	Política 0902-008	Seguros de equipos *Todo equipo de tratamiento de la información de propiedad de la organización debe tener cobertura de seguro contra robo, daño o pérdida. Los equipos portátiles deben tener un seguro que cubra viajes nacionales y al exterior.*
9.2.5	**Seguridad de equipos fuera de los locales de la organización**	
9.2.5	Política 0902-009	Traslado de equipos *Todo movimiento de equipos entre locales de la organización debe ser estrictamente controlado por el personal responsable de dichos activos.*

ISO 27002	POLITICAS COOTRADIAN	Descripción
9.2.6	**Seguridad en el reuso o eliminación de equipos**	
9.2.6	Política 0902-010	Desecho de equipo obsoleto *Solo personal autorizado puede disponer de equipos de propiedad de la organización para su desecho, siempre y cuando se hayan controlado los riesgos de seguridad asociados a la información contenida en dicho equipo.*
9.3	**Controles Generales**	
9.3.1	**Política de puesto de trabajo despejado y bloqueo de pantalla**	
9.3.1	Política 0903-001	Política de escritorios limpios *Los trabajadores que manejan información deben mantener sus áreas de trabajo despejadas para reducir el riesgo de accesos no autorizados*
9.3.1	Política 0903-002	Impresión de documentos confidenciales *Se debe asegurar que una persona autorizada reciba la impresión de documentos confidenciales que se envían a una impresora de red, a fin de proteger la confidencialidad durante y después de la impresión.*
9.3.2	**Retiro de propiedad**	
9.3.2	Política 0903-003	Retiro de equipos *Solo se permite a personal autorizado retirar equipos de la organización, siendo dicho personal responsable de su seguridad.*
9.3.2	Política 0903-004	Bloqueo de Sesión *Los usuarios cuando se ausenten por más de un minuto de su puesto de trabajo deben bloquear su sesión en el computador.*

10. Gestión de Comunicaciones y Operaciones		
10.1	**Procedimientos y responsabilidades de operación**	
10.1.1	**Documentación de procedimientos operativos**	
10.1.1	Política 1001-001	Documentación de procedimientos operativos *Los procedimientos operativos deben especificar las instrucciones detalladas para la ejecución de cada tarea, incluyendo las actividades de administración de sistemas.* ***Dichos procedimientos deben estar documentados*** *formalmente.*

ISO 27002	POLITICAS COOTRADIAN	Descripción
10.1.1	Política 1001-002	Cronograma de operaciones *Los cronogramas de operaciones deben planearse y pasar por un proceso formal de autorización.*
10.1.2	**Control de cambios operacionales**	
10.1.2	Política 1001-003	Control de cambios operacionales *Los cambios operacionales deben probarse exhaustivamente y ser aprobados formalmente antes de ser puestos en producción.*
10.1.3	**Procedimientos de gestión de incidentes**	
10.1.3	Política 1001-004	Respuestas ante incidentes de Seguridad de la Información *El OSI debe responder rápidamente a cualquier incidente de Seguridad de la Información, coordinando la recolección de información y sugiriendo medidas a tomar donde sea necesario.*
10.1.3	Política 1001-005	Protección contra ataques de negación de servicio (DoS) *Se deben tener listos planes de acción contra ataques de negación del servicio (DoS) los cuales deben ser mantenidos y probados periódicamente para asegurarse de su eficacia.*
10.1.3	Política 1001-006	Análisis de incidentes de Seguridad de la Información ocasionados por fallas de sistemas *Los incidentes de seguridad de la información originados por fallas de hardware o software deben investigarse de manera apropiada por especialistas.*
10.1.3	Política 1001-007	Confidencialidad de los incidentes de Seguridad de la Información *La información relacionada a incidentes de seguridad de la información sólo puede ser divulgada por personas autorizadas.*

ISO 27002	POLITICAS COOTRADIAN	Descripción
10.1.4	**Segregación de funciones**	
10.1.4	Política 1001-008	Necesidad de control dual / segregación de funciones *Dondequiera que un incidente de seguridad de la información pueda ocasionar daño material o financiero a la organización, debe emplearse técnicas de control dual y segregación de funciones para mejorar el control de procedimientos de seguridad.*
10.1.5	**Separación de los recursos de desarrollo y de producción**	
10.1.5	Política 1001-009	Separación de funciones en desarrollo y producción *La gerencia debe asegurarse que una segregación de funciones apropiada se aplique a todas las áreas que se tienen que ver con el desarrollo, operaciones y administración de sistemas.*
10.1.6	**Gestión de servicios externos**	
10.1.6	Política 1001-010	Tercerización de operaciones *En el caso de tercerización de operaciones, se deben identificar los riesgos por anticipado e incorporar al contrato las medidas de seguridad apropiadas.*
10.2	**Planificación y Aceptación del Sistema**	
10.2.1	**Planificación de la capacidad**	
10.2.1	Política 1002-001	Planeamiento de capacidad y prueba de nuevos sistemas ***Para las pruebas de nuevos sistemas se deben aplicar criterios de capacidad, carga máxima y prueba de stress.*** *Debe demostrarse que sus niveles de rendimiento y resistencia cumplen o exceden las necesidades o requisitos técnicos de la organización.*
10.2.2	**Aceptación del sistema**	
10.2.2	Política 1002-002	Paralelo de sistemas *Los procedimientos de prueba de sistemas deben considerar un período de funcionamiento paralelo antes que el sistema nuevo o mejorado sea aceptado para su uso en producción. Los resultados del paralelo no deben revelar problemas o dificultades diferentes a los ya vistos durante la prueba de aceptación de usuario.*

ISO 27002	POLITICAS COOTRADIAN	Descripción
10.2.2	Política 1002-003	Elaboración de bases de datos *Antes de poner una base de datos en producción, se deben realizar pruebas exhaustivas de su funcionamiento, tanto a nivel lógico de su estructura, como de su eficiencia en un ambiente de producción.*
10.3	**Protección contra software malicioso**	
10.3.1	**Medidas y controles contra software malicioso**	
10.3.1	Política 1003-001	Defensa de la red contra ataques maliciosos *Todos los recursos activos de tratamiento de información: infraestructura de red, software base y de aplicación, deben configurarse y protegerse adecuadamente contra ataques físicos e intrusión.*
10.3.1	Política 1003-002	Defensa contra virus informáticos *Todas las PCs y servidores de la organización deben tener instalado un software antivirus. Igualmente, se debe mantener actualizado el archivo de firmas y escanear regularmente todos los equipos.*
10.3.1	Política 0003-002	Software antivirus *El software antivirus debe adquirirse de un proveedor reconocido, que tenga soporte técnico adecuado.*
10.3.1	Política 1003-003	Respuesta a incidentes de virus *Se debe desarrollar una estrategia integral y procedimientos de actuación para hacer frente a los virus informáticos, **lo cual incluirá procedimientos y responsabilidades de administración**, capacitación en el uso de software antivirus y recuperación después de los ataques de virus.*
10.3.1	Política 1003-004	Descargar archivos e Información de Internet *Se debe tener mucho cuidado al descargar información y archivos de Internet a fin de evitar el ingreso de código malicioso así como la descarga de material no apropiado.*
10.3.1	Política 1003-005	Certeza de orígenes de archivos *Los archivos electrónicos recibidos de remitentes desconocidos deben ser eliminados sin ser abiertos.*

ISO 27002	POLITICAS COOTRADIAN	Descripción
10.3.1	Política 1003-006	Instalación de software adicional *Está prohibido instalar software no autorizado en las computadoras de la organización, tales como protectores de pantalla, software demostrativo, manejadores de música, video, mensajería instantánea, etc., salvo autorización expresa de la gerencia.*
10.3.1	Política 1003-007	Manejo de rumores de virus *Debe existir un procedimiento formal de tratamiento de los rumores de virus y otros ataques.*
10.4	**Gestión interna de respaldo y recuperación**	
10.4.1	**Respaldo y recuperación de la información**	
10.4.1	Política 1004-001	Gestión de procedimientos de respaldo y recuperación *Se dará alta prioridad al respaldo de archivos de datos (backup) de la organización y la capacidad de restaurarlos. La gerencia de TI será responsable de que la frecuencia de tales operaciones y que los procedimientos aplicados se adecuan a las necesidades de la organización.*
10.4.1	Política 1004-002	Respaldo y recuperación de sistemas *Los dueños de sistemas de información deben asegurarse que los procedimientos de respaldo y recuperación de sistemas sean los adecuados y estén implementados y funcionando.*
10.4.1	Política 1004-003	Duración de los medios *Los medios usados para almacenar información deben corresponder a las necesidades de duración. El formato en el que se almacenan los datos debe ser evaluado cuidadosamente, especialmente donde hayan formatos propietarios.*
10.4.1	Política 1004-004	Caducidad de archivos electrónicos *El almacenamiento de datos electrónicos debe reflejar las necesidades de la organización y los dispositivos legales y regulatorios.*
10.4.2	**Diarios de operación**	

ISO 27002	POLITICAS COOTRADIAN	Descripción
10.4.2	Política 1004-005	Monitoreo de los logs de operaciones ***Los registros de log operacional deben ser revisados periódicamente por personal calificado*** *y las discrepancias con los procedimientos operacionales deben ser comunicadas al dueño del sistema de información.*
10.4.3	**Registro de fallas**	
10.4.3	Política 1004-006	**Registro y reporte de fallas de equipos** *Toda falla de equipos (incluyendo daño) debe anotarse en un registro especialmente designado para tal fin por el personal encargado de su mantenimiento.*
10.4.3	Política 1004-007	Registro y reporte de fallas de software *Se debe registrar y reportar formalmente toda falla de software a los responsables de soporte de software.*
10.5	**Gestión de Redes**	
10.5.1	**Controles de red**	
10.5.1	Política 1005-001	Gestión de redes ***Los administradores de redes deberán implantar los controles y medidas requeridas para conseguir y conservar la seguridad de los datos en las redes de computadoras****, así como la integridad de la red y protección de los servicios conectados contra accesos no autorizados.*
10.6	**Utilización y seguridad de medios**	
10.6.1	**Gestión de medios removibles**	
10.6.1	Política 1006-001	Uso de medios removibles de almacenamiento *Solamente el personal autorizado a instalar o a modificar el software podrá utilizar medios removibles para transferir datos de la organización. Cualquier otra persona requerirá autorización expresa.*

ISO 27002	POLITICAS COOTRADIAN	Descripción
10.6.2	**Eliminación de medios**	
10.6.2	Política 1006-002	Eliminación segura de documentos *Todos los documentos de naturaleza confidencial deben ser destruidos cuando ya no se requieren. El dueño del documento debe autorizar o realizar esta destrucción.*
10.6.2	Política 1006-003	Eliminación de Software *Sólo se debe eliminar un programa de software cuando se haya decidido que dicho programa ya no es necesario y que no se necesita tener acceso a sus archivos de datos mediante dicho programa.*
10.6.3	**Procedimientos de manejo de la información**	
10.6.3	Política 1006-004	Uso de buenas prácticas de gestión de información *Todos los usuarios deben proteger la confidencialidad, integridad y disponibilidad de los archivos durante la creación, almacenamiento, modificación, copiado y borrado/eliminación de archivos de datos.*
10.6.3	Política 1006-005	Comprobación de exactitud y validez de documentos *Se debe confirmar la validez e integridad de documentos, especialmente aquellos que comprometen u obligan a la organización.*
10.6.3	Política 1006-006	Dependencias entre documentos y archivos *Los documentos altamente sensibles o críticos no deben depender de la disponibilidad o integridad de archivos de datos sobre los que el autor no tenga control. Los documentos e informes importantes deben ser autónomos y contener toda la información necesaria.*
10.6.3	Política 1006-007	Fotocopiado de información confidencial *Los trabajadores deben conocer los riesgos de brechas de confidencialidad durante el fotocopiado/duplicación de documentos. Sólo se debe duplicar documentos confidenciales con la debida autorización del dueño del documento.*
10.6.3	Política 1006-008	Eliminación de archivos temporales (tmp) *Los archivos temporales en las computadoras de usuarios deben ser eliminados con regularidad para prevenir su posible mal uso por usuarios no autorizados.*

ISO 27002	POLITICAS COOTRADIAN	Descripción
10.6.4	**Seguridad de la documentación de sistemas**	
10.6.4	Política 1006-009	Gestión de documentación de sistemas *La documentación de sistemas es un requisito obligatorio para todo sistema de información de la organización. Dicha documentación debe mantenerse actualizada y disponible.*
10.7	**Intercambio de Información y software**	
10.7.1	**Acuerdos para intercambio de información y software**	
10.7.1	Política 1007-001	Envío de información a terceros *Antes de enviar información a terceros, se debe verificar que el receptor está autorizado a recibir dicha información y que las medidas adoptadas por los receptores aseguran la confidencialidad e integridad de la información que se envía.*
10.7.2	**Seguridad física de medios en tránsito**	
10.7.2	Política 1007-002	Transporte de documentos confidenciales *Las medidas de protección de la confidencialidad, integridad y disponibilidad en el transporte o transmisión de documentos confidenciales serán establecidas por los dueños de dichos documentos, quienes deberán asegurarse que tales medidas son las apropiadas.*
10.7.3	**Seguridad del correo electrónico**	
10.7.3	Política 1007-004	Envío de correo electrónico *Se debe utilizar el correo electrónico solamente para fines relacionados con la organización. Antes de adjuntar archivos a un mensaje de e-mail se debe verificar que la clasificación de información de dicho archivo permite su envío al destinatario previsto y también. Previamente se debe escanear y verificar que no exista virus u otro código malicioso.*
10.7.3	Política 1007-005	Recepción de correo erróneo *Los mensajes de correo electrónico no solicitado deben ser tratados con precaución y no ser respondidos.*
10.7.3	Política 1007-006	Recepción de correo no solicitado *Se debe verificar la identidad y la autenticidad del remitente de cualquier mensaje de correo electrónico no solicitado antes de abrirlo.*

ISO 27002	POLITICAS COOTRADIAN	Descripción
10.7.4	**Seguridad de los sistemas ofimáticos**	
10.7.4	Política 1007-007	Uso de equipos de fax y fax-módems *Sólo se puede enviar información confidencial por fax cuando no estén disponibles métodos más seguros de transmisión. El dueño de la información y el recipiente previsto deben autorizar las transmisiones por anticipado.*
10.7.4	Política 1007-008	Gestión de máquinas contestadoras y correo de voz *No se debe grabar información confidencial en contestadoras automáticas o sistemas de correo de voz.*
10.7.4	Política 1007-009	Información por teléfono *Se debe tener mucha precaución cuando se comunica información confidencial vía telefónica, verificando además la identidad de los destinatarios.*
10.7.4	Política 1007-010	Envío erróneo de información a terceros *Se debe comprobar cuidadosamente las direcciones de email y números de fax antes de enviar información, especialmente en los casos de información confidencial. La misma precaución debe aplicarse cuando existe la posibilidad que se divulguen las direcciones de E-mail u otra información de contacto.*
10.7.5	**Sistemas públicamente disponibles**	
10.7.5	Política 1007-011	Seguridad de sistemas públicamente disponibles *Se deben establecer controles en los sistemas públicamente disponibles de captura de información con la finalidad que la información confidencial se proteja durante su recogida y almacenamiento, y que el acceso a dicho sistema no permita accesos no autorizados a otras redes a las que está conectado el sistema.*
10.7.5	**Otras formas de intercambio de información**	
10.7.5	Política 1007-012	Transmisión e intercambio de datos *Solamente se puede transmitir datos o información confidenciales cuando la seguridad de los datos puede garantizarse razonablemente usando técnicas de encriptación.*

ISO 27002	POLITICAS COOTRADIAN	Descripción
11. Control de Accesos		
11.1	**Requisitos de negocio para el Control de Accesos**	
11.1	Política 1101-001	Control de distribución de información *Los datos e información deben protegerse mediante controles técnicos y administrativos a fin de asegurarse que están disponibles solo para personas autorizadas.*
11.1.1	**Política de control de accesos**	
11.1.1	Política 1101-002	Gestión de estándares de control de accesos *Los estándares de control de acceso de los sistemas de información deben establecerse de tal manera que prevengan accesos no autorizados y a la vez proporcionen acceso inmediato según los requerimientos de la organización.*
11.1.1	Política 1101-003	Establecimiento de una estructura de carpetas y datos para usuarios *Las estructuras de carpetas de datos de usuarios deben ser definidas por la Gerencia de Tecnologías de Información y los usuarios deben seguir dicha estructura. Las restricciones de acceso a tales carpetas se deben aplicar como convenga para restringir el acceso no autorizado.*
11.1.1	Política 1101-004	Protección de documentos con contraseñas *Se debe proteger la información confidencial usando, preferentemente, el control de acceso de la carpeta donde está situado el archivo correspondiente. No se recomienda el uso solamente de contraseñas para proteger documentos ya que es poco eficaz.*
11.1.1	Política 1101-005	Defensa contra ataques internos intencionales *Los estándares de control de acceso y de clasificación de datos deben ser revisados y actualizados periódicamente para reducir la incidencia y la posibilidad de ataques internos.*
11.1.1	Política 1101-006	Configuración de acceso a la Intranet/Extranet *Los responsables de configurar el acceso de la Intranet/Extranet deben asegurarse que la configuración del acceso replique, como mínimo, las restricciones de los sistemas convencionales de la organización.*

ISO 27002	POLITICAS COOTRADIAN	Descripción
11.1.1	Política 1101-007	Configuración de acceso a Internet *El personal encargado de configurar el acceso a Internet debe asegurarse que la red de la organización tenga la debida protección. Como mínimo se debe instalar un firewall debidamente configurado.*
11.1.1	Política 1101-008	Acceso a información sobre proyectos de la organización *Solamente personas autorizadas pueden tener acceso a datos confidenciales sobre proyectos de propiedad de la organización o gerenciados por sus trabajadores.*
11.2	**Gestión de Acceso de Usuarios**	
11.2	Política 1102-001	Gestión de Acceso de Usuarios *El acceso a los sistemas de información debe autorizarse por su dueño y tal acceso debe registrarse en una Lista de Control de Accesos. Estos registros deben considerarse como altamente confidenciales y ser debidamente protegidos.*
11.2	Política 1102-002	Inicio y fin de sesión *Los sistemas deben considerar el manejo de sesiones con los usuarios, las cuales se cerrarán después de un tiempo de no uso (time-out).*
11.2.1	**Registro de usuarios**	
11.2.1	Política 1102-003	Registro e identificador de usuarios *Se debe formalizar un procedimiento de registro de altas y bajas de usuarios para garantizar el acceso a los sistemas y servicios de información de la organización. Debe existir una gestión sobre el ciclo de vida de los usuarios.*
11.2.2	**Gestión de privilegios**	
11.2.2	Política 1102-004	Asignación de privilegios *La asignación de privilegios de acceso en los sistemas de la organización debe controlarse mediante un proceso formal de autorización, en el cual debe participar el dueño del sistema en cuestión.*
11.2.3	**Gestión de contraseñas de usuario**	

ISO 27002	POLITICAS COOTRADIAN	Descripción
11.2.3	Política 1102-005	Gestión de contraseñas *La selección, uso y gestión de contraseñas como medio principal para el control de acceso a los sistemas de la organización debe adecuarse a las mejores prácticas existentes. En particular, las contraseñas no deben ser compartidas con otra persona bajo ninguna circunstancia.*
11.2.4	**Revisión de los derechos de acceso de los usuarios**	
11.2.4	Política 1102-006	Manejo de renuncias de personal *En el caso de renuncias o ceses de personal, la Dirección de Personal debe considerar, conjuntamente con el OSI, si los derechos de acceso del personal saliente constituyen un riesgo inaceptable para la organización y, si es así, deben revocarse todos los derechos de acceso.*
11.2.4	Política 1102-007	Personal que trabajará en instituciones competidoras *Se debe anular los derechos de acceso a la información de la organización de manera inmediata a los trabajadores que se van a trabajar a una entidad competidora.*
11.3	**Responsabilidades de los Usuarios**	
11.3.1	**Uso de contraseñas**	
11.3.1	Política 1103-008	Responsabilidad de usuarios en el uso de contraseñas *Los usuarios deberán proteger sus contraseñas usando las mejores prácticas existentes, como por ejemplo: no se deben usar contraseñas fáciles de adivinar, como nombres, números de la placas de vehículos, fechas del nacimiento, o similares; la contraseña no debe almacenarse en teclas de función programables, debe ser cambiada si llega a ser conocida por personas no autorizadas, entre otras.*
11.3.2	**Equipo informático de usuario desatendido**	
11.3.2	Política 1103-009	Protección de computadoras desatendidas *Todos los usuarios de computadoras personales y laptops deben asegurarse que sus pantallas queden protegidas y no muestren información cuando estén desatendidas.*

ISO 27002	POLITICAS COOTRADIAN	Descripción
11.4	**Control de Acceso a la Red**	
11.4	Política 1104-001	Gestión de controles de acceso a la red *El acceso a los recursos de red debe controlarse estrictamente para evitar accesos no autorizados. El acceso a sistemas de cómputo y periféricos debe estar restringido por defecto y autorizarse expresamente.*
11.4	Política 1104-002	Configuración de redes *Las redes deben estar diseñadas y configuradas de tal manera que se restrinjan los accesos de acuerdo a reglas claramente definidas sin afectar la confiabilidad y el rendimiento.*
11.4	Política 1104-003	Gestión de seguridad de redes *El acceso a los recursos de la red de la organización debe controlarse estrictamente de acuerdo con la Lista de Control de Accesos aprobada, la cual debe estar actualizada permanentemente.*
11.4.1	**Política de uso de los servicios de la red**	
11.4.2	**Ruta forzosa**	
11.4.2	Política 1104-004	Establecimiento de rutas forzosas *La red debe estar configurada y equipada de tal manera que se puedan establecer rutas forzosas desde las estaciones de trabajo hacia los servidores de la organización.*
11.4.3	**Autenticación de usuarios para conexiones externas**	
11.4.3	Política 1104-005	Acceso remoto a la red *El acceso remoto a la red de la organización será permitido solamente cuando el usuario se identifique de manera segura, los datos que viajan por la red estén encriptados y los privilegios restringidos a la ocasión.*
11.4.4	**Autenticación de nodos de la red**	
11.4.4	Política 1104-006	Autenticación de dispositivos remotos *Las conexiones remotas a sistemas informáticos se deberán autenticar con la finalidad de reducir la amenaza de accesos no autorizados a las aplicaciones.*
11.4.5	**Protección a puertos de diagnóstico remoto**	

ISO 27002	POLITICAS COOTRADIAN	Descripción
11.4.5	Política 1104-007	Protección acceso a puertos de diagnóstico *Se deberá proteger, con un mecanismo de seguridad probado, el acceso a puertos de diagnóstico remoto para asegurar que sólo son accesibles tras un acuerdo formal del Departamento de TI con el personal de mantenimiento del hardware o software que solicita el acceso.*
11.5	**Control de acceso al sistema operativo**	
11.5	Política 1105-001	Control de acceso al Sistema Operativo *El acceso a comandos del sistema operativo debe restringirse para que solamente las personas autorizadas puedan ejecutar dichos comandos. Las funciones de administración de dichos sistemas deben requerir aprobación específica.*
11.5.1	**Identificación automática de terminales**	
11.5.1	Política 1105-002	Identificación automática de terminales o sesiones emuladas. *Se debe usar la identificación automática de terminales o sesiones emuladas para autenticar las conexiones a ubicaciones específicas y a equipos portátiles.*
11.5.2	**Procedimientos de conexión de terminales**	
11.5.2	Política 1105-003	Conexión al sistema informático *El procedimiento de conexión a los sistemas informáticos debe minimizar la posibilidad de accesos no autorizados.*
11.5.3	**Identificación y autenticación del usuario**	
11.5.3	Política 1105-004	Identificación del usuario *Todos los usuarios deberán disponer de un identificador único para su uso personal y exclusivo, a fin de vincular a los usuarios con la responsabilidad de sus acciones (Control No Repudio).*
11.6	**Control de Acceso a las aplicaciones**	
11.6.1	**Restricción de acceso a la información**	
11.6.1	Política 1106-001	Restricción de acceso *Los controles de acceso deben ser fijados de tal manera que se reduzcan al mínimo los riesgos de la seguridad de la información pero que a la vez no impidan la operatividad de la organización.*

ISO 27002	POLITICAS COOTRADIAN	Descripción
11.6.2	**Aislamiento de sistemas sensibles**	
11.6.2	Política 1106-002	Administración de acceso a sistemas altamente confidenciales *Los controles de acceso para sistemas de información altamente confidenciales deben ser fijados en concordancia con la clasificación de los activos de información a ser protegidos.*
11.7	**Seguimiento de accesos y usos del sistema**	
11.7.1	**Registro de incidentes**	
11.7.1	Política 1107-001	Registro de evidencias de incidentes *Se debe advertir a todos los empleados que en caso de incidentes de seguridad, es necesario registrar y conservar evidencias o pistas para uso del OSI.*
11.7.2	**Seguimiento del uso de los sistemas**	
11.7.2	Política 1107-002	Monitoreo de accesos y uso del sistema *Se debe registrar y supervisar el acceso a los sistemas para identificar su posible mala utilización.*
11.7.2	Política 1107-003	Integridad de las investigaciones de incidentes de Seguridad de la Información. *Se debe monitorear regularmente el uso de los sistemas de información, registrando e investigando todos los eventos inesperados. Tales registros también deben auditarse periódicamente de tal manera que sus resultados, sumados al historial de errores fortalezcan la investigación.*
11.7.3	**Sincronización de relojes**	
11.7.3	Política 1107-004	Sincronización de relojes del sistema *Los relojes del sistema se deben sincronizar regularmente, especialmente cuando hay diferentes plataformas de procesamiento.*
11.8	**Informática móvil y teletrabajo**	
11.8.1	**Informática móvil**	

ISO 27002	POLITICAS COOTRADIAN	Descripción
11.8.1	Política 1108-001	Uso de equipos portátiles de cómputo *Las personas que usan computadoras portátiles fuera de la organización deben conocer los riesgos de Seguridad de Información referidos a equipos portátiles e implementar las protecciones apropiadas para reducir al mínimo dichos riesgos.*
11.8.1	Política 1108-002	Uso de facilidades de centros empresariales *El personal que usa centros empresariales para trabajar asuntos de la organización es responsable de la seguridad y subsecuente remoción de toda información registrada por él en los sistemas de dicho centro.*
11.8.1	Política 1108-003	Respaldo de datos (backup) de equipos portátiles de cómputo *La información y datos almacenados en computadoras portátiles se deben respaldar regularmente (backup). Es responsabilidad del usuario asegurarse de que esto se realice de manera periódica.*
11.8.1	Política 1108-004	Viajes de trabajo *Los empleados que viajan por asuntos de la organización son responsables de la seguridad de la información en su poder.*
11.8.1	Política 1108-005	Correo electrónico corporativo en dispositivos móviles. *La posibilidad de sincronización de correo electrónico a dispositivos móviles se debe brindar previa autorización expresa y por escrito del dueño de proceso o gerente de área.*

12. Desarrollo y mantenimiento de Sistemas		
12.1	**Requisitos de seguridad de los sistemas**	
12.1	Política 1201-001	Implementación de software nuevo o mejorado *Toda implementación de software debe considerar una planificación adecuada para reducir los riesgos de seguridad de la información mediante la aplicación de los controles apropiados.*
12.1	Política 1201-002	Documentación de sistemas *Todos los sistemas deben tener documentación completa y actualizada. Ningún sistema debe pasar a producción si no tiene la documentación de soporte disponible.*

ISO 27002	POLITICAS COOTRADIAN	Descripción
12.1.1	**Análisis y especificación de los requisitos de seguridad**	
12.1.1	Política 1201-003	Justificación de desarrollo de nuevos sistemas *Todo desarrollo de software, dentro o fuera de la organización, debe contar con un sustento técnico-económico, un presupuesto adecuado y el compromiso de disponer de los recursos necesarios para solventar el proyecto de inicio a fin. El proceso de aprobación debe ser formal e incluir a la Alta Dirección.*
12.1.1	Política 1201-004	Desarrollo y mantenimiento de software *Las especificaciones técnicas y funcionales para el desarrollo y mantenimiento de un software deben contemplar formalmente los requerimientos de seguridad, incluyendo los controles técnicos de acceso, la asignación restringida de privilegios y otros requisitos que resulten convenientes para dicha aplicación.*
12.1.1	Política 1201-005	Interfases de software aplicativo *El desarrollo de interfases de sistemas es una tarea altamente especializada y por lo tanto sólo debe ser realizada por profesionales con la debida calificación y experiencia comprobada en el tema. Debe considerar sobremanera los aspectos de seguridad de los sistemas que son conectados y de las plataformas que intervienen.*
12.2	**Seguridad de las aplicaciones del sistema**	
12.2.1	**Validación de los datos de entrada**	
	Política 1202-001	Control de datos de entrada *Como parte del proceso de diseño, desarrollo y/o implementación de todo software en la institución debe realizarse, de manera obligatoria, el control de datos de entrada, considerando, como mínimo, los procedimientos de consistencia de datos, correspondencia a las autorizaciones y privilegios de usuario, y procedimientos de manejo de errores.*
12.2.2	**Control del proceso interno**	
	Política 1202-002	Control de datos en proceso *Todo sistema en producción debe contemplar el control de los datos en proceso. Dichos controles deberán ser diseñados conjuntamente con el dueño del sistema. Como mínimo se debe considerar controles externos de integridad de datos así como momentos de ejecución de programas.*
12.2.3	**Autenticación de mensajes**	

ISO 27002	POLITICAS COOTRADIAN	Descripción
	Política 1202-003	Autenticación de mensajes en intercambio de datos *Todo intercambio electrónico de información confidencial deberá tener implementado un procedimiento probado de autenticación de mensajes.*
12.2.4	**Validación de los datos de salida**	
	Política 1202-004	Control de datos de salida *Como parte del proceso de diseño, desarrollo y/o implementación de todo software en la institución debe existir, de manera obligatoria, un procedimiento para controlar los datos de salida, considerando, como mínimo, procedimientos de consistencia de datos de salida, correspondencia a las autorizaciones y privilegios de usuario, y procedimientos de manejo de errores.*
12.3	**Controles Criptográficos**	
12.3.1	**Política de uso de los controles criptográficos**	
	Política 1203-001	Uso de medidas criptográficas *La organización debe evaluar constantemente, mediante un análisis de riesgos, qué información requiere ser protegida con medidas criptográficas.*
12.3.2	**Cifrado**	
12.3.2	Política 1203-002	Uso de técnicas de encriptación *Las técnicas de encriptación a ser usadas en la organización deben considerar las regulaciones y restricciones nacionales e internacionales. Antes de la transmisión, se deben coordinar los procedimientos que utilizarán el emisor y el receptor.*
12.3.3	**Firmas digitales**	
12.3.3	Política 1203-003	Uso de firmas digitales en la organización *La conveniencia y viabilidad, así como los casos en los que se puede usar firmas digitales debe analizarse conjuntamente entre la parte técnica y legal de la organización, teniendo en cuenta toda la legislación relativa que describe las condiciones en las que una firma digital tiene validez legal.*

ISO 27002	POLITICAS COOTRADIAN	Descripción
12.4	**Seguridad de los archivos del sistema**	
12.4.1	**Control del software en producción**	
12.4.1	Política 1204-001	Gestión de operaciones y administración de sistemas *La operación y administración de sistemas de la organización debe llevarse a cabo siguiendo procedimientos diseñados y documentados detalladamente según las mejores prácticas y debidamente aprobados por los dueños de los sistemas.*
12.4.1	Política 1204-002	Gestión de bibliotecas de programas en producción *Las bibliotecas de programas que están en producción deben tener controles que impidan el acceso de personas no autorizadas, el cual se debe otorgar estrictamente por necesidad de uso. Los procedimientos de modificación deben estar formalmente autorizados por el dueño del sistema y prever el control dual.*
12.4.2	**Protección de los datos de prueba del sistema**	
12.4.2	Política 1204-003	Uso de datos para pruebas *Todo sistema de información debe tener un juego de datos de prueba que sea consistente y no contenga datos reales o confidenciales. Si no se puede evitar el uso de uso de datos reales confidenciales, éstos deben ser despersonalizados antes de ser usados.*
12.4.3	**Control de acceso a la biblioteca de programas fuente**	
12.4.3	Política 1204-004	Gestión de bibliotecas de programas fuente *Las bibliotecas de programas fuente deben tener controles que impidan el acceso de personas no autorizadas y manejarse con un adecuado control de versiones. Los procedimientos de uso de los programas fuente deben estar definidos formalmente de acuerdo a la metodología de desarrollo de sistemas de la organización.*
12.5	**Seguridad en los procesos de desarrollo y soporte**	
12.5.1	**Procedimientos de control de cambios**	
12.5.1	Política 1205-001	Gestión de procedimientos de control de cambios *Todo cambio a sistemas de información debe realizarse mediante procedimientos formales de control de cambios, y debe autorizarse y probarse exhaustivamente en un ambiente de prueba antes de pasarlo al ambiente de producción.*

ISO 27002	POLITICAS COOTRADIAN	Descripción
12.5.1	Política 1205-002	Control de versiones *Se deben aplicar procedimientos del control de versiones a todos los programas de software y procedimientos pertenecientes a la organización.*
12.5.1	Política 1205-003	Actualizaciones de software recomendadas por el proveedor *Solo de se debe actualizar el software a una nueva versión si se han evaluado adecuadamente las ventajas previstas, la necesidad de dicha actualización y las implicancias de dicha actualización así como sus riesgos.*
12.5.1	Política 1205-004	Reparaciones de emergencia al software. *En el caso que se requiera realizar reparaciones de emergencia al software aplicativo, será la gerencia quien tome la decisión al respecto, después de evaluar la necesidad e implicancias de dicha operación. En cualquier caso, la reparación deberá hacerse estrictamente de acuerdo a* ***procedimientos acordados de control de cambios****.*
12.5.2	**Revisión técnica de los cambios en el sistema operativo**	
12.5.2	Política 1205-005	Mejoras (upgrades) de software al sistema operativo *Toda decisión de instalar mejoras a sistemas operativos debe considerar los riesgos asociados y tener la adecuada planificación mediante el establecimiento de un proyecto formal que también considere el manejo de contingencias.*
12.5.3	**Restricciones en los cambios a los paquetes de software**	
	Política 1205-006	Cambios a paquetes de software *No se deben realizar modificaciones a los paquetes de software a menos que sea estrictamente necesario, en cuyo caso se deberá guardar el software original (sin cambios) y probar y documentar los cambios realizados.*
12.5.5	**Desarrollo externo del software**	
	Política 1205-007	Calidad de desarrollo externo *Todo desarrollo externo de software debe hacerse por empresas debidamente certificadas en dicha actividad y determinar los derechos de propiedad intelectual. Se debe tener acuerdos para manejar los posibles fallos del contratista.*

ISO 27002	POLITICAS COOTRADIAN	Descripción

13. Gestión de Incidentes en la Seguridad de Información		
13.1	**Reporte de eventos y debilidades de la Seguridad de la Información**	
13.1.1	**Reporte de Eventos**	
13.1.1	Política -1305-001	Procedimiento formal *Un procedimiento formal de reporte de eventos en la seguridad de la información debe ser establecido conjuntamente con una respuesta de incidencias y procedimientos de escalada, estableciendo las acciones que serán tomadas al recibir dicho reporte. Se debe establecer dentro de este reporte un punto de contacto que siempre esté disponible y que sea capaz de proveer respuestas adecuadas a tiempo.*
	Política -1305-002	Procedimiento del reporte *Los procedimientos de reporte del cual deben tener conocimiento los empleados, contratistas y terceros, deben incluir: procesos de retroalimentación que aseguren que los eventos sean notificados; formulario de reporte, el cual apoya la acción del reporte y ayuda al encargado del reporte a recordar las acciones necesarias cuando se produce un evento.*
13.1.1	Política -1305-003	Recolectando evidencias *Para ser capaz de tratar propiamente eventos e incidentes de la seguridad de información puede ser necesario recolectar evidencias lo más pronto posible después de la ocurrencia*
13.1.1	Política -1305-004	Respuesta del sistema *El mal funcionamiento u otro comportamiento anormal en el sistema puede ser un indicador de un ataque de seguridad o de una abertura en la seguridad, debiendo ser reportado como un evento de la seguridad de información.*
13.1.2	**Reporte de Debilidades**	
13.1.2	Política -1305-005	Mecanismo de reporte *El mecanismo del reporte debe ser fácil, accesible y disponible como sea posible. Deben ser informados que por ninguna circunstancia deben tratar de probar una debilidad sospechosa.*

ISO 27002	POLITICAS COOTRADIAN	Descripción
13.1.2	Política -1305-006	Probar debilidades *Probar las debilidades puede ser interpretado como un potencial mal uso del sistema y puede ocasionar un daño al sistema o servicio de información y resultar en responsabilidad legal para el individuo que realiza la prueba.*
13.2	**Gestión de las mejoras e incidentes de la Seguridad de Información**	
	Política -1305-007	Responsabilidades y procedimiento de las mejoras e incidentes de la seguridad de información. *Las responsabilidades y procedimientos deben establecerse para maniobrar los eventos y debilidades en la seguridad de información de una manera efectiva una vez que hayan sido reportados.*
13.2.1	**Responsabilidades y procedimientos**	
13.2.1	Política -1305-008	Monitoreo del sistema, alerta y vulnerabilidad *El monitoreo de los sistemas, alertas y vulnerabilidades deben ser utilizados para detectar los incidentes en la seguridad de información.*
13.2.1	Política -1305-009	Pautas para procedimientos de la gestión de incidentes en la seguridad de información *Los procedimientos deben ser establecidos para maniobrar diferentes tipos de incidentes en la seguridad de información como, las fallas y pérdidas de servicio en el sistema, código malicioso, negación de servicios, apertura de confidencialidad e integridad y el mal uso de los sistemas de información.*
13.2.2	**Recolección de evidencia**	
13.2.2	Política -1305-010	Acciones para recolectar evidencias *Cuando una acción o seguimiento contra una persona u organización, después de un incidente en la seguridad de información, implique acción legal, la evidencia debe ser recolectada, retenida y presentada para estar conforme con las reglas para la colocación de evidencia en la jurisdicción relevante.*
13.2.2	Política -1305-011	Acciones para los Procesos internos *Los procesos internos deben ser desarrollados y seguidos cuando se recolecte y presente evidencia para propósitos disciplinarios maniobrados dentro de la organización.*

ISO 27002	POLITICAS COOTRADIAN	Descripción
13.2.2	Política -1305-012	Admisibilidad de la evidencia *Para lograr admisibilidad de la evidencia, la organización debe asegurar que sus sistemas de información cumplen con cualquier estándar o código publicado de práctica para la producción de evidencia admisible.*
13.2.2	Política -1305-013	Integridad de material de evidencia *La integridad de todo material de evidencia debe ser protegida. Las copias deben ser supervisadas por personal confiable y se debe registrar la información de cuando y donde fue ejecutado el proceso de copia, quien realizo dicha actividad, y que herramientas y programas se utilizaron.*
14. Gestión de Continuidad del Negocio		
14.1	**Aspectos de la Gestión de Continuidad del Negocio**	
14.1.1	**Proceso de gestión de la continuidad del negocio**	
14.1.1	Política 1401-001	Gestión de continuidad del negocio *La gestión de la continuidad del negocio debe incorporarse en los procesos y estructura de la organización, asignando la responsabilidad de coordinación de este proceso al comité de seguridad de la información.*
	Política 1401-002	Proceso de continuidad del negocio *El proceso de continuidad del negocio debe incluir la identificación y priorización de los procesos críticos y el impacto de las interrupciones. Los planes y procesos de continuidad así definidos deben probarse y actualizarse periódicamente.*
14.1.1	Política 1401-003	Iniciativa para el Plan de Continuidad del Negocio *La gerencia debe tener la iniciativa en la realización del Plan de Continuidad del Negocio.*
14.1.1	Política 1401-004	Plan de recuperación de desastres *Los dueños de sistemas de información críticos deben asegurarse que sus sistemas cuentan con planes de recuperación de desastres probados y en funcionamiento.*
14.1.2	**Continuidad del negocio y análisis de impactos**	

ISO 27002	POLITICAS COOTRADIAN	Descripción
14.1.2	Política 1401-005	Análisis de impactos *Los dueños de los sistemas de información, conjuntamente con los responsables técnicos de su manejo y respaldados por la Alta Dirección, identificarán los eventos potencialmente causantes de interrupciones a procesos y/o servicios.*
14.1.2	Política 1401-006	Minimización de impacto de ataques informáticos *Se deben elaborar planes para minimizar los daños por posibles ataques informáticos, los que deberán ser mantenidos y probados periódicamente para asegurar su eficacia y que los tiempos de recuperación sean razonables.*
14.1.4	**Marco de planificación para la continuidad del negocio**	
	Política 1401-007	Responsabilidades de los Planes de Continuidad *La Alta Dirección será responsable de la existencia de un esquema único de planes de continuidad del negocio que garantice que los diferentes planes son consistentes entre sí y que cada plan tiene un dueño designado. Asimismo que los procedimientos de emergencia y los planes de respaldo manual y de reanudación estén bajo la responsabilidad de los dueños de los correspondientes recursos o procesos del negocio involucrados.*
	Política 1401-008	Activación de los Planes de Continuidad *Cada plan de continuidad del negocio debería especificar claramente las condiciones para su activación, los procedimientos de emergencia a llevar a cabo, los procedimientos de respaldo que permitirán operar, los procedimientos de reanudación en condiciones de normalidad así como las personas responsables de ejecutar cada etapa del plan.*
	Política 1401-009	Mantenimiento y concientización *Todo plan de continuidad debe tener un calendario de mantenimiento de pruebas del plan, así como prever actividades de concientización y capacitación diseñadas para asegurar que los procesos sean eficaces*
14.1.5	**Prueba, mantenimiento y reevaluación de los Planes de Continuidad**	

ISO 27002	POLITICAS COOTRADIAN	Descripción
14.1.5	Política 1401-010	Prueba del Plan de Continuidad del Negocio *El Plan de Continuidad del Negocio debe ser probado periódicamente para asegurarse que cada uno de los responsables de las diferentes acciones entiendan correctamente la ejecución del Plan.*
14.1.5	Política 1401-011	Mantenimiento y reevaluación del Plan de Continuidad del Negocio *El Plan de Continuidad del Negocio debe ser continuamente actualizado para reflejar los cambios en los recursos, procesos y servicios de la organización.*

15. Cumplimiento		
15.1	**Cumplimiento con requisitos legales**	
15.1.1	**Identificación de legislación aplicable**	
	Política 1501-001	Documentación de requisitos ***Cada dueño de sistema de información será responsable de documentar de forma explícita todos los requisitos legales, regulatorios y contractuales que sean importantes para su sistema.*** *Esta documentación estará disponible para uso legal y técnico del sistema.*
15.1.1	Política 1501-002	Cuidados contra denuncias de difamación y calumnias *A fin de evitar denuncias por difamación y/o calumnia, se prohíbe que los trabajadores realicen observaciones despectivas sobre otras personas u organizaciones usando el nombre y/o recursos de la organización.*
15.1.2	**Derechos de propiedad intelectual**	
	Política 1501-003	Responsabilidad de la Alta Dirección *La Alta Dirección es responsable de implantar los procedimientos apropiados de cumplimiento de las restricciones legales sobre uso de material protegido por derechos de propiedad intelectual.*
15.1.2	Política 1501-004	Responsabilidad de la Dirección de Personal *La Dirección de Personal ejecutará las acciones necesarias para que todos los trabajadores conozcan los principales aspectos de propiedad intelectual y licenciamiento de software que guarden relación con sus funciones.*

ISO 27002	POLITICAS COOTRADIAN	Descripción
15.1.2	Política 1501-005	Renovación de nombres de dominio de sitios Web *Se deben proteger y asegurar los nombres de dominio de Internet de forma similar a cualquier otro activo valioso de la organización.*
15.1.2	Política 1501-006	Propiedad intelectual de trabajos dentro de la organización *Los derechos de propiedad intelectual de trabajos llevados a cabo dentro de un contrato con la organización se protegerán mediante acuerdos formales.*
15.1.2.	Política 1501-007	Uso de software licenciado *Todo software que se utilice en la organización debe estar amparado en una Licencia de Usuario, cuyos términos se deben respetar estrictamente con la finalidad de cumplir con las leyes y asegurar el soporte continuo por parte de los proveedores.*
15.1.2	Política 1501-008	Uso de información protegida por derechos de autor (con copyright) de la Internet *Para utilizar información obtenida de la Internet o de otras fuentes electrónicas, se debe obtener la autorización del propietario de los derechos de autor.*
15.1.2	Política 1501-009	Envío electrónico de información protegida por derechos de autor (con copyright) *Para retransmitir información por Internet u otras fuentes electrónicas, se deben obtener la autorización del propietario de los derechos de autor.*
15.1.3	**Protección de los registros de la organización**	
15.1.3	Política 1501-010	Archivamiento de documentos *Se deben aplicar controles técnicos y administrativos para garantizar el cumplimiento de las consideraciones legales y regulatorias en el archivamiento de los registros de la organización.*
15.1.3	Política 1501-011	Conservación de información *Los registros e información creados y almacenados por sistemas de información de la organización deben conservarse por el tiempo que sea necesario para cumplir con los requisitos legales, sectoriales y los propios de la actividad de la organización.*

ISO 27002	POLITICAS COOTRADIAN	Descripción
15.1.3	Política 1501-012	Conservación o borrado de correo electrónico *Los mensajes de correo electrónico almacenados en sistemas de organización deben conservarse por el tiempo que sea necesario para cumplir con los requisitos legales, sectoriales y los propios de la actividad de la organización.*
15.1.4	**Protección de los datos y de la privacidad de la información personal**	
15.1.4	Política 1501-013	Confidencialidad de información de clientes *Se debe proteger la información de contacto de cliente y terceros de cualquier acceso no autorizado.*
15.1.4	Política 1501-014	Información confidencial de trabajadores *Sólo personas expresamente autorizadas podrán tener acceso a información personal sobre los trabajadores de la organización, al ser dicha información estrictamente confidencial.*
15.1.4	Política 1501-015	Gestión de datos de tarjetas débito y crédito de clientes *La información obtenida a partir del acceso a tarjetas débito y crédito de clientes debe procesarse de tal manera que dicha información esté protegida contra todas las formas conocidas de acceso no autorizado, para lo cual deben usarse controles técnicos y administrativos. Se deben considerar los requerimientos de la norma PCI-DSS.*
15.1.5	**Prevención del mal uso de los recursos de tratamiento de la información**	
15.1.5	Política 1501-016	Uso de fotocopiadoras con fines personales *Las fotocopiadoras o duplicadoras no deben usarse para uso personal. De manera excepcional, el supervisor inmediato puede dar permiso específico al empleado para su uso.*
15.1.5	Política 1501-017	Uso del correo para fines personales *El uso personal del correo electrónico (email) debe reducirse al mínimo. El correo postal sólo se debe utilizar para propósitos de la organización.*
15.1.5	Política 1501-018	Uso del teléfono para fines personales *Las llamadas telefónicas personales a través de sistemas telefónicos, incluidos los móviles, de la organización deben ser reducidas al mínimo.*

ISO 27002	POLITICAS COOTRADIAN	Descripción
15.1.5	Política 1501-019	Juegos en computadores *El uso de computadoras de la organización para juegos está estrictamente prohibido.*
15.1.7	**Recopilación de pruebas**	
15.1.7	Política 1501-020	Recolección de pruebas de delitos informáticos *La organización denunciará, con toda el peso de la ley, a autores de delitos informáticos. Se deben desarrollar procedimientos apropiados para asegurar la recolección y protección adecuada de evidencias.*
15.1.7	Política 1501-021	Recopilación de evidencias de brechas de Seguridad de la Información *Toda evidencia referente a brechas de seguridad de la información debe ser recopilada y remitida al OSI.*
15.2	**Revisiones de la Política de Seguridad y de la conformidad técnica**	
15.2.1	**Conformidad con la política de seguridad**	
15.2.1	Política 1502-001	Cumplimiento de las Políticas de Seguridad de la Información *El cabal cumplimiento de las Políticas de Seguridad de la Información de la organización por parte de los trabajadores es obligatorio. La supervisión de tal cumplimiento es responsabilidad de la Alta Dirección.*
15.2.2	**Comprobación de la conformidad técnica**	
	Política 1502-002	Examen y pruebas de conformidad *Se debe comprobar regularmente la conformidad técnica de las medidas de seguridad mediante el examen de los sistemas y pruebas de intrusión a diversos sistemas, realizables por profesionales independientes especialistas en el tema.*

ISO 27002	POLITICAS COOTRADIAN	Descripción
15.3	**Consideraciones sobre la auditoria de sistemas**	
15.3.1	**Controles de auditoria de sistemas**	
	Política 1502-003	Planificación de las actividades de auditoría *Para minimizar el riesgo de interrupción de los procesos de negocio, las actividades de auditoría se deberán planificar cuidadosamente, registrándose y supervisándose todos los accesos. Asimismo, todos los procedimientos, requisitos y responsabilidades deberán estar documentados.*