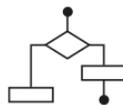




VIAJES CIRCULAR S.A.S

# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN



## Tabla de Contenido

<b>1. INTRODUCCIÓN</b>	<b>6</b>
<b>2. Política de Seguridad</b>	<b>8</b>
<b>3. Aspectos Organizativos para la Seguridad</b>	<b>8</b>
3.1 Organización para la seguridad de la información	8
3.1.1 Comité Gerencial de Seguridad de la Información	8
3.1.2 Coordinación de Seguridad de la Información	8
3.1.3 Asignación de responsabilidades sobre Seguridad de la Información	8
3.1.4 Proceso de autorización de recursos para el tratamiento de la información	9
3.1.5 Asesoramiento de especialistas en seguridad de la información	10
3.1.6 Cooperación entre organizaciones	10
3.2 Seguridad en los accesos de terceras personas	10
3.2.1 Identificación de los riesgos por acceso de terceros	10
3.2.2 Requisitos de seguridad en contratos con terceros	10
<b>4. Clasificación y control de Activos</b>	<b>11</b>
4.1 Responsabilidad sobre los activos	11
4.1.1 Inventario de activos	12
4.2 Clasificación de la Información	12
4.2.1 Guías de clasificación	12
4.2.2 Marcado y tratamiento de la información	13
<b>5. Seguridad ligada al Personal</b>	<b>13</b>
5.1 Seguridad en la definición del trabajo y los recursos	13
5.1.1 Inclusión de la seguridad en las responsabilidades laborales	13
5.1.2 Selección y política de personal	14
5.1.3 Compromiso de Confidencialidad	14
5.1.4 Términos y condiciones de la relación laboral	14
5.2 Capacitación de Usuarios	15
5.2.1 Capacitación en seguridad de la información	15
5.3 Respuesta ante incidentes y malos funcionamientos de la seguridad	15
5.3.1 Reporte de incidentes de seguridad	15
5.3.2 Reporte de debilidades de seguridad	16
5.3.3 Reporte de fallas de software	16
5.3.4 Aprendiendo de los incidentes	16
5.3.5 Proceso disciplinario	16

<b>6. Seguridad Física y del Entorno</b>	<b>16</b>
6.1 Áreas Seguras	16
6.1.1 Perímetro de Seguridad Física	16
6.1.2 Controles físicos de ingreso	17
6.1.3 Seguridad de oficinas, despachos y recursos	17
6.1.4 El trabajo en las Áreas Seguras	17
6.1.5 Áreas de acceso público, entrega y recepción	17
6.2 Seguridad de los Equipos	18
6.2.1 Instalación y protección de equipos	18
6.2.2 Suministro eléctrico	18
6.2.3 Seguridad del cableado	18
6.2.4 Mantenimiento de equipos	18
6.2.5 Seguridad de equipos fuera de los locales de la organización	19
6.2.6 Seguridad en el reúso o eliminación de equipos	19
6.3 Controles Generales	19
6.3.1 Política de puesto de trabajo despejado y bloqueo de pantalla	19
6.3.2 Retiro de propiedad	19
<b>7. Gestión de Comunicaciones y Operaciones</b>	<b>19</b>
7.1 Procedimientos y responsabilidades de operación	19
7.1.1 Documentación de procedimientos operativos	19
7.1.2 Control de cambios operacionales	20
7.1.3 Procedimientos de gestión de incidentes	20
7.1.4 Segregación de funciones	20
7.1.5 Separación de los recursos de desarrollo y de producción	20
7.1.6 Gestión de servicios externos	21
7.2 Planificación y Aceptación del Sistema	21
7.2.1 Planificación de la capacidad	21
7.2.2 Aceptación del sistema	21
7.3 Protección contra software malicioso	21
7.3.1 Medidas y controles contra software malicioso	21
7.4 Gestión interna de respaldo y recuperación	22
7.4.1 Respaldo y recuperación de la información	22
7.4.2 Diarios de operación	23
7.4.3 Registro de fallas	23
7.5 Gestión de Redes	23
7.5.1 Controles de red	23

7.6 Utilización y seguridad de medios	23
7.6.1 Gestión de medios removibles	23
7.6.3 Procedimientos de manejo de la información	24
7.6.4 Seguridad de la documentación de sistemas	25
7.7 Intercambio de Información y software	25
7.7.1 Acuerdos para intercambio de información y software	25
7.7.2 Seguridad física de medios en tránsito	25
7.7.3 Seguridad en Comercio Electrónico	25
7.7.4 Seguridad del correo electrónico	25
7.7.5 Seguridad de los sistemas ofimáticos	26
7.7.6 Sistemas públicamente disponibles	26
7.7.7 Otras formas de intercambio de información	26
<b>8. Control de Accesos</b>	<b>26</b>
8.1 Requisitos de negocio para el Control de Accesos	26
8.1.1 Política de control de accesos	27
8.2 Gestión de Acceso de Usuarios	28
8.2.1 Registro de usuarios	28
8.2.2 Gestión de privilegios	28
8.2.3 Gestión de contraseñas de usuario	28
8.2.4 Revisión de los derechos de acceso de los usuarios	28
8.3 Responsabilidades de los Usuarios	29
8.3.1 Uso de contraseñas	29
8.3.2 Equipo informático de usuario desatendido	29
8.4 Control de Acceso a la Red	29
8.4.1 Política de uso de los servicios de la red	29
8.4.2 Ruta forzosa	29
8.4.3 Autenticación de usuarios para conexiones externas	30
8.4.4 Autenticación de nodos de la red	30
8.4.5 Protección a puertos de diagnóstico remoto	30
8.5 Control de acceso al sistema operativo	30
8.5.1 Identificación automática de terminales	30
8.5.2 Procedimientos de conexión de terminales	30
8.6 Control de Acceso a las aplicaciones	31
8.6.1 Restricción de acceso a la información	31
8.6.2 Aislamiento de sistemas sensibles	31
8.7 Seguimiento de accesos y usos del sistema	31

8.7.1 Registro de incidentes	31
8.7.2 Seguimiento del uso de los sistemas	31
8.7.3 Sincronización de relojes	32
8.8 Informática móvil y teletrabajo	32
8.8.1 Informática móvil	32
<b>9. Desarrollo y mantenimiento de Sistemas</b>	<b>32</b>
9.1 Requisitos de seguridad de los sistemas	33
9.1.1 Análisis y especificación de los requisitos de seguridad	33
9.2 Seguridad de las aplicaciones del sistema	33
9.2.1 Validación de los datos de entrada	33
9.2.2 Control del proceso interno	34
9.2.3 Validación de los datos de salida	34
9.3 Seguridad de los archivos del sistema	34
9.3.1 Control del software en producción	34
9.3.2 Protección de los datos de prueba del sistema	34
9.3.3 Control de acceso a la biblioteca de programas fuente	34
9.4 Seguridad en los procesos de desarrollo y soporte	35
9.4.1 Procedimientos de control de cambios	35
9.4.2 Desarrollo externo del software	35
<b>10. Gestión de Incidentes en la Seguridad de Información</b>	<b>35</b>
10.1.1 Reporte de Eventos	35
10.1.2 Reporte de Debilidades	36
10.2 Gestión de las mejoras e incidentes de la Seguridad de Información	36
10.2.1 Responsabilidades y procedimientos	36
10.2.2 Recolección de evidencia	37
<b>11. Gestión de Continuidad del Negocio</b>	<b>37</b>
11.1 Aspectos de la Gestión de Continuidad del Negocio	37
11.1.1 Proceso de gestión de la continuidad del negocio	37
11.1.2 Continuidad del negocio y análisis de impactos	38
11.1.4 Marco de planificación para la continuidad del negocio	38
11.1.5 Prueba, mantenimiento y reevaluación de los Planes de Continuidad	39
<b>12. Cumplimiento</b>	<b>39</b>
12.1 Cumplimiento con requisitos legales	39
12.1.1 Identificación de legislación aplicable	39
12.1.2 Derechos de propiedad intelectual	40
12.1.3 Protección de los registros de la organización	41

12.1.4	Protección de los datos y de la privacidad de la información personal	41
12.1.5	Prevención del mal uso de los recursos de tratamiento de la información	42
12.1.7	Recopilación de pruebas	42
12.2	Revisiones de la Política de Seguridad y de la conformidad técnica	42
12.2.1	Conformidad con la política de seguridad	42
12.2.2	Comprobación de la conformidad técnica	43
12.3	Consideraciones sobre la auditoría de sistemas	43
12.3.1	Controles de auditoría de sistemas	43

## 1. INTRODUCCIÓN

Este contiene las políticas de seguridad de la información de Viajes Circular, 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. Así mismo 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.

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.

2. Política de Seguridad		
<b>2.1 Política de la seguridad de la información</b>		
<b>2.1.1 Documento de política de la seguridad de la información</b>		
	Política 0201-001	<p>Establecimiento de Políticas de Seguridad de la Información</p> <p>La Alta Dirección de la organización se encargará de establecer, mantener y publicar las Políticas de Seguridad de la Información.</p>
<b>2.1.2 Revisión y evaluación</b>		
	Política 0201-002	<p>Revisión de las Políticas de Seguridad de la Información</p> <p>Las Políticas de Seguridad de la Información tendrán un propietario designado que será responsable de su mantenimiento y revisión de acuerdo a un <b>proceso definido</b>. En CVU esta responsabilidad se delega en el Oficial de Seguridad de la Información.</p>
3. Aspectos Organizativos para la Seguridad		
<b>3.1 Organización para la seguridad de la información</b>		
<b>3.1.1 Comité Gerencial de Seguridad de la Información</b>		
3.1.1	Política 0301-001	<p>Rol del Comité Gerencial de Seguridad de la Información</p> <p>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.</p>
<b>3.1.2 Coordinación de Seguridad de la Información</b>		
3.1.2	Política 0301-002	<p>Rol de la alta dirección en la seguridad de la información</p> <p>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.</p>
3.1.2	Política 0301-003	<p>Actualizaciones sobre Seguridad de la Información para el Personal</p> <p>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.</p>
<b>3.1.3 Asignación de responsabilidades sobre Seguridad de la Información</b>		
3.1.3	Política 0301-004	<p>Designación del Oficial de Seguridad de la Información (OSI).</p> <p>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.</p>

3.1.3	Política 0301-005	<p>Administración de Sistemas</p> <p>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.</p>
3.1.3	Política 0301-006	<p>Responsabilidad de Proveedor(es) de servicios para transacciones con tarjeta de crédito</p> <p>Durante la relación comercial acepta(n) responsabilizarse de la seguridad de los datos del titular(es) de tarjeta, que posee, almacena, procesa o transmite en nombre del CLIENTE, o en la medida en que su gestión o servicio pueda afectar la seguridad del entorno de datos de los tarjetahabientes, bajo las condiciones descritas en el contrato para la prestación del servicio y las responsabilidades allí señaladas.</p>
<b>3.1.4 Proceso de autorización de recursos para el tratamiento de la información</b>		
3.1.4	Política 0301-007	<p>Especificación de los requisitos para nuevo equipamiento</p> <p>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.</p>
3.1.4	Política 0301-008	<p>Instalación de nuevo equipamiento</p> <p>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.</p>
3.1.4	Política 0301-009	<p>Prueba de equipamiento y sistemas</p> <p>Todo equipo debe probarse exhaustivamente y pasar por un proceso de aceptación formal de usuarios antes de ser transferido al entorno de producción.</p>
3.1.4	Política 0301-010	<p>Especificación de los requerimientos de usuario para software</p> <p>Todos las solicitudes de desarrollo de sistemas nuevos o mejoras a los mismos deben presentarse a la gerencia mediante un documento de <b>“Especificaciones de requerimientos de usuario”</b>, donde se define detalladamente los requerimientos técnicos y funcionales.</p>
3.1.4	Política 0301-011	<p>Selección de paquetes de software comercial</p>

		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.
3.1.4	Política 0301-012	<p>Selección de paquetes de software de ofimática</p> <p>Todas los paquetes de software de oficina deben ser compatibles con el sistema operativo y plataforma de cómputo aprobados por la organización.</p>
<b>3.1.5 Asesoramiento de especialistas en seguridad de la información</b>		
3.1.5	Política 0501-013	<p>Asesoría especializada en Seguridad de la Información</p> <p>La institución buscará asesoría especializada sobre Seguridad de la Información de consultores internos o externos.</p>
<b>3.1.6 Cooperación entre organizaciones</b>		
3.1.6	Política 0501-014	<p>Identificación de organizaciones relevantes</p> <p>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.</p>
<b>3.2 Seguridad en los accesos de terceras personas</b>		
<b>3.2.1 Identificación de los riesgos por acceso de terceros</b>		
3.2.1	Política 0202-001	<p>Acceso de terceros</p> <p>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.</p>
3.2.1	Política 0202-002	<p>Permisos de acceso a terceros</p> <p>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 controlados.</p>
<b>3.2.2 Requisitos de seguridad en contratos con terceros</b>		
3.2.2	Política 0202-003	<p>Acuerdos de acceso a la información por terceros</p> <p>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 acordados con las políticas y normas de seguridad de la organización.</p>
3.2.2	Política 0202-004	<p>Difusión de las políticas a contratistas y trabajadores temporales</p>

		Se entregará formalmente un <b>resumen de las Políticas de Seguridad</b> de la Información a todo contratista y/o trabajador temporal antes del inicio de sus servicios.
3.2.2	Política 0202-005	<p>Conformidad de trabajos hechos por terceros</p> <p>Solamente las personas debidamente autorizadas expresamente pueden firmar la conformidad de trabajos hechos por terceros.</p>
3.2.2	Política 0202-006	<p>Compra de software desarrollado por proveedores</p> <p>El software desarrollado por terceros, debe cumplir con las “Especificaciones de Requerimientos de Usuario” y ofrecer un soporte técnico apropiado. Las Tecnologías de la información deben garantizar la vigencia de los contratos de soporte de proveedores y sus respectivas actualizaciones.</p>
3.2.2	Política 0202-007	<p>Brechas de confidencialidad de terceros</p> <p>Las violaciones de confidencialidad de terceros deben ser reportadas al OSI tan pronto como sea posible.</p>
3.2.2	Política 0202-008	<p>Servicios externos de eliminación de material y equipo</p> <p>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.</p>
3.2.2	Política 0202-009	<p>Soporte de software de aplicación</p> <p>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.</p>

## 4. Clasificación y control de Activos

### 4.1 Responsabilidad sobre los activos

4.1	Política 0401-001	<p>Responsabilidad sobre los activos</p> <p>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.</p>
4.1	Política 0401-002	<p>Defensa contra delitos informáticos</p> <p>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.</p>

<b>4.1.1 Inventario de activos</b>		
4.1.1	Política 0401-003	<p>Mantenimiento del inventario de activos de información</p> <p>La institución contará con un inventario formal de todos los activos de información, el cual estará actualizado de manera permanentemente.</p>
4.1.1	Política 0401-004	<p>Gestión y uso de documentación de hardware</p> <p>La documentación de hardware debe estar siempre actualizada y fácilmente accesible para el personal autorizado de soporte o mantenimiento.</p>
4.1.1	Política 0401-005	<p>Política de protección de marca</p> <p>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.</p>
<b>4.2 Clasificación de la Información</b>		
4.2	Política 0402-001	<p>Clasificación de Información</p> <p>Todo activo de información: datos y documentos, debe clasificarse según su confidencialidad, valor para el negocio y sensibilidad.</p>
4.2	Política 0402-002	<p>Registro de activos de información</p> <p>La organización debe mantener un registro actualizado de sus activos de información.</p>
<b>4.2.1 Guías de clasificación</b>		
4.2.1	Política 0402-003	<p>Esquema de clasificación de activos de información</p> <p>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.</p>
4.2.1	Política 0402-004	<p>Datos de beneficiarios, clientes y terceros</p> <p>Se debe clasificar la información de contacto de beneficiarios, clientes y terceros como altamente confidencial y protegerla en consecuencia.</p>
4.2.1	Política 0402-005	<p>Manejo de Información Financiera</p> <p>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.</p>

<b>4.2.2 Marcado y tratamiento de la información</b>		
4.2.2	Política 0402-006	<p>Etiquetado de información</p> <p>Todo 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.</p>
4.2.2	Política 0402-007	<p>Uso de nombres de archivos</p> <p>Los nombres de archivos de datos de la organización deben tener un significado reconocible por los usuarios de dichos archivos.</p>
4.2.2	Política 0402-008	<p>Indicación de niveles de seguridad en documentos</p> <p>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.</p>
4.2.2	Política 0402-009	<p>Grabación periódica de datos por usuarios</p> <p>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.</p>
4.2.2	Política 0402-010	<p>Gestión de borradores de informes</p> <p>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.</p>

## 5. Seguridad ligada al Personal

### 5.1 Seguridad en la definición del trabajo y los recursos

#### 5.1.1 Inclusión de la seguridad en las responsabilidades laborales

5.1.1	Política 0501-001	<p>Inclusión de cláusulas en el contrato de trabajo</p> <p>El contrato de trabajo debe incluir cláusulas de cumplimiento de la Seguridad de la Información.</p>
5.1.1	Política 0501-002	<p>Responsabilidad de los empleados sobre datos confidenciales</p> <p>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.</p>

<b>5.1.2 Selección y política de personal</b>		
5.1.2	Política 0501-003	<p>Contratación de nuevo personal</p> <p>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.</p>
<b>5.1.3 Compromiso de Confidencialidad</b>		
5.1.3	Política 0501-004	<p>Acuerdos de confidencialidad</p> <p>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.</p>
5.1.3	Política 0501-005	<p>Confidencialidad de las contraseñas y números PIN</p> <p>Las contraseñas otorgadas a los trabajadores son privadas y confidenciales. La violación a dicha confidencialidad puede dar lugar a una acción disciplinaria.</p>
5.1.3	Política 0501-006	<p>Respuesta a requerimientos telefónicos</p> <p>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.</p>
5.1.3	Política 0501-007	<p>Compartir información confidencial con otros</p> <p>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.</p>
5.1.3	Política 0501-008	<p>Declaraciones a medios de comunicación</p> <p>Sólo personas expresamente autorizadas pueden dirigirse a medios de difusión sobre temas referidos a la organización.</p>
<b>5.1.4 Términos y condiciones de la relación laboral</b>		
5.1.4	Política 0501-009	<p>Conocimiento de obligaciones legales</p> <p>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.</p>

5.1.4	Política 0501-010	<p>Respeto de la privacidad en el trabajo</p> <p>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.</p>
<b>5.2 Capacitación de Usuarios</b>		
<b>5.2.1 Capacitación en seguridad de la información</b>		
5.2.1	Política 0502-001	<p>Capacitación en Seguridad de la Información a trabajadores</p> <p>La capacitación en Seguridad de la Información se impartirá de manera obligatoria y actualizada a todos los trabajadores.</p>
5.2.1	Política 0502-002	<p>Capacitación en Seguridad de la Información al personal técnico</p> <p>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.</p>
5.2.1	Política 0502-003	<p>Capacitación en Seguridad de la Información a personal nuevo</p> <p>El personal nuevo debe recibir capacitación básica en Seguridad de la Información como parte del proceso de inducción.</p>
5.2.1	Política 0502-004	<p>Programas de concientización para el personal permanente.</p> <p>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.</p>
<b>5.3 Respuesta ante incidentes y malos funcionamientos de la seguridad</b>		
5.3	Política 0503-001	<p>Investigación de causas e impacto de incidentes</p> <p>Los incidentes de Seguridad de la Información deben ser investigados apropiadamente por personal debidamente capacitado.</p>
<b>5.3.1 Reporte de incidentes de seguridad</b>		
5.3.1	Política 0503-002	<p>Reporte de incidentes de Seguridad de la Información</p> <p>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.</p>

5.3.1	Política 0503-003	<p>Reporte de incidentes de Seguridad de la Información a autoridades externas</p> <p>Sólo se deben comunicar los incidentes de Seguridad de la Información a autoridades externas siempre que sea necesario debido a requisitos legales o regulatorios.</p>
<b>5.3.2 Reporte de debilidades de seguridad</b>		
5.3.2	Política 0503-004	<p>Notificación de debilidades de Seguridad de la Información</p> <p>Las debilidades o sospechas de debilidades de Seguridad de la Información deben notificarse al OSI lo más rápidamente posible.</p>
<b>5.3.3 Reporte de fallas de software</b>		
	Política 0503-005	<p>Reporte de fallas de software</p> <p>Las fallas de software deben ser reportadas mediante un procedimiento existente para tal fin.</p>
<b>5.3.4 Aprendiendo de los incidentes</b>		
5.3.4	Política 0503-006	<p>Revisión del registro de incidentes de Seguridad de la Información</p> <p>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.</p>
<b>5.3.5 Proceso disciplinario</b>		
5.3.5	Política 0503-007	<p>Cumplimiento de las Políticas de Seguridad de la Información</p> <p>Cualquier incidente de seguridad originado por un incumplimiento de dichas políticas, podrá dar lugar a una acción disciplinaria.</p>

## 6. Seguridad Física y del Entorno

### 6.1 Áreas Seguras

#### 6.1.1 Perímetro de Seguridad Física

6.1.1	Política 0601-001	<p>Seguridad de ambientes de cómputo</p> <p>Los ambientes que contengan computadoras deben protegerse contra cualquier intrusión física.</p>
6.1.1	Política 0601-002	<p>Gestión de repositorios de datos</p> <p>Las áreas donde se almacenan datos o información deben tener controles de acceso para reducir el riesgo de pérdida o daño a un nivel aceptable.</p>

<b>6.1.2 Controles físicos de ingreso</b>		
6.1.2	Política 0601-003	<p>Protección de acceso físico</p> <p>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.</p>
<b>6.1.3 Seguridad de oficinas, despachos y recursos</b>		
6.1.3	Política 0601-004	<p>Configuración de oficinas</p> <p>Las oficinas deben estar configuradas para minimizar los daños por incendio, inundación, explosión, disturbios y otras formas de desastres naturales o provocados, así como amenazas que procedan de lugares vecinos.</p>
6.1.3	Política 0601-005	<p>Seguridad de oficinas</p> <p>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.</p>
6.1.3	Política 0601-006	<p>Almacenamiento seguro</p> <p>El material y equipo con información sensible o valiosa deben almacenarse con seguridad y según el nivel de clasificación de la información almacenada.</p>
6.1.3	Política 0601-007	<p>Desconfiar de extraños en las áreas de la organización</p> <p>Todos los trabajadores deben conocer la necesidad de desconfiar de extraños en los ambientes de la organización.</p>
<b>6.1.4 El trabajo en las Áreas Seguras</b>		
6.1.4	Política 0601-008	<p>Acceso de terceros a las áreas seguras</p> <p>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.</p>
<b>6.1.5 Áreas de acceso público, entrega y recepción</b>		
6.1.5	Política 0601-009	<p>Controles en áreas de acceso público</p> <p>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.</p>

<b>6.2 Seguridad de los Equipos</b>		
<b>6.2.1 Instalación y protección de equipos</b>		
6.2.1	Política 0602-001	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.
<b>6.2.2 Suministro eléctrico</b>		
6.2.2	Política 0602-002	Suministro continuo de energía eléctrica a equipos críticos  Se deben instalar fuentes de alimentación continua (UPS) donde sea necesario para asegurar la continuidad del servicio durante interrupciones del suministro eléctrico.
6.2.2	Política 0602-003	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.
<b>6.2.3 Seguridad del cableado</b>		
6.2.3	Política 0602-004	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.
6.2.3	Política 0602-005	Seguridad del cableado  La seguridad del cableado de red debe ser revisada cada vez que se hagan mejoras, cambios de equipo o de ambientes.
<b>6.2.4 Mantenimiento de equipos</b>		
6.2.4	Política 0602-006	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.
6.2.4	Política 0602-007	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.

6.2.4	Política 0602-008	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.
<b>6.2.5 Seguridad de equipos fuera de los locales de la organización</b>		
6.2.5	Política 0602-009	Traslado de equipos  Todo movimiento de equipos entre locales de la organización debe ser estrictamente controlado por el personal responsable de dichos activos.
<b>6.2.6 Seguridad en el reúso o eliminación de equipos</b>		
6.2.6	Política 0602-010	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.
<b>6.3 Controles Generales</b>		
<b>6.3.1 Política de puesto de trabajo despejado y bloqueo de pantalla</b>		
6.3.1	Política 0603-001	Política de escritorios limpios  Los trabajadores que manejan información deben mantener sus áreas de trabajo despejadas para reducir el riesgo de accesos no autorizados
6.3.1	Política 0603-002	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.
<b>6.3.2 Retiro de propiedad</b>		
6.3.2	Política 0603-003	Retiro de equipos  Solo se permite a personal autorizado retirar equipos de la organización, siendo dicho personal responsable de su seguridad.
<b>7. Gestión de Comunicaciones y Operaciones</b>		
<b>7.1 Procedimientos y responsabilidades de operación</b>		
<b>7.1.1 Documentación de procedimientos operativos</b>		
7.1.1	Política 0701-001	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.
7.1.1	Política 0701-002	<p>Cronograma de operaciones</p> <p>Los cronogramas de operaciones deben planearse y pasar por un proceso formal de autorización.</p>
<b>7.1.2 Control de cambios operacionales</b>		
7.1.2	Política 0701-003	<p>Control de cambios operacionales</p> <p>Los cambios operacionales deben probarse exhaustivamente y ser aprobados formalmente antes de ser puestos en producción.</p>
<b>7.1.3 Procedimientos de gestión de incidentes</b>		
7.1.3	Política 0701-004	<p>Respuestas ante incidentes de Seguridad de la Información</p> <p>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.</p>
7.1.3	Política 0701-005	<p>Protección contra ataques de negación de servicio (DoS)</p> <p>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.</p>
7.1.3	Política 0701-006	<p>Análisis de incidentes de Seguridad de la Información ocasionados por fallas de sistemas</p> <p>Los incidentes de seguridad de la información originados por fallas de hardware o software deben investigarse de manera apropiada por especialistas.</p>
7.1.3	Política 0701-007	<p>Confidencialidad de los incidentes de Seguridad de la Información</p> <p>La información relacionada a incidentes de seguridad de la información sólo puede ser divulgada por personas autorizadas.</p>
<b>7.1.4 Segregación de funciones</b>		
7.1.4	Política 0701-008	<p>Necesidad de control dual / segregación de funciones</p> <p>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.</p>
<b>7.1.5 Separación de los recursos de desarrollo y de producción</b>		
7.1.5	Política 0701-009	Separación de funciones en desarrollo y producción

		La gerencia debe asegurarse que una segregación de funciones apropiada se aplique a todas las áreas que tienen que ver con el desarrollo, operaciones y administración de sistemas.
<b>7.1.6 Gestión de servicios externos</b>		
7.1.6	Política 0701-010	<p>Tercerización de operaciones</p> <p>En el caso de tercerización de operaciones, se deben identificar los riesgos por anticipado e incorporar al contrato las medidas de seguridad apropiadas.</p>
<b>7.2 Planificación y Aceptación del Sistema</b>		
<b>7.2.1 Planificación de la capacidad</b>		
7.2.1	Política 0702-001	<p>Planeamiento de capacidad y prueba de nuevos sistemas</p> <p>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.</p>
<b>7.2.2 Aceptación del sistema</b>		
7.2.2	Política 0702-002	<p>Paralelo de sistemas</p> <p>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.</p>
7.2.2	Política 0702-003	<p>Elaboración de bases de datos</p> <p>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.</p>
<b>7.3 Protección contra software malicioso</b>		
<b>7.3.1 Medidas y controles contra software malicioso</b>		
7.3.1	Política 0703-001	<p>Defensa de la red contra ataques maliciosos</p> <p>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.</p>
7.3.1	Política 0703-002	<p>Defensa contra virus informáticos</p> <p>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.</p>

7.3.1	Política 0703-002	Software antivirus  El software antivirus debe adquirirse de un proveedor reconocido, que tenga soporte técnico adecuado.
7.3.1	Política 0703-003	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.
7.3.1	Política 0703-004	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.
7.3.1	Política 0703-005	Certeza de orígenes de archivos  Los archivos electrónicos recibidos de remitentes desconocidos deben ser eliminados sin ser abiertos.
7.3.1	Política 0703-006	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.
7.3.1	Política 0703-007	Manejo de rumores de virus  Debe existir un procedimiento formal de tratamiento de los rumores de virus y otros ataques.
<b>7.4 Gestión interna de respaldo y recuperación</b>		
<b>7.4.1 Respaldo y recuperación de la información</b>		
7.4.1	Política 0704-001	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 adecuen a las necesidades de la organización.
7.4.1	Política 0704-002	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.

7.4.1	Política 0704-003	<p>Duración de los medios</p> <p>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 haya formatos propietarios.</p>
7.4.1	Política 0704-004	<p>Caducidad de archivos electrónicos</p> <p>El almacenamiento de datos electrónicos debe reflejar las necesidades de la organización y los dispositivos legales y regulatorios.</p>
<b>7.4.2 Diarios de operación</b>		
7.4.2	Política 0704-005	<p>Monitoreo de los logs de operaciones</p> <p>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.</p>
<b>7.4.3 Registro de fallas</b>		
7.4.3	Política 0704-006	<p>Registro y reporte de fallas de equipos</p> <p>Toda falla de equipos (incluyendo daño) debe anotarse en un registro especialmente designado para tal fin por el personal encargado de su mantenimiento.</p>
7.4.3	Política 0704-007	<p>Registro y reporte de fallas de software</p> <p>Se debe registrar y reportar formalmente toda falla de software a los responsables de soporte de software.</p>
<b>7.5 Gestión de Redes</b>		
<b>7.5.1 Controles de red</b>		
7.5.1	Política 0705-001	<p>Gestión de redes</p> <p><b>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</b>, así como la integridad de la red y protección de los servicios conectados contra accesos no autorizados.</p>
<b>7.6 Utilización y seguridad de medios</b>		
<b>7.6.1 Gestión de medios removibles</b>		
7.6.1	Política 0706-001	<p>Uso de medios removibles de almacenamiento</p> <p>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.</p>

<b>7.6.2 Eliminación de medios</b>		
7.6.2	Política 0706-002	<p>Eliminación segura de documentos</p> <p>Todos los documentos de naturaleza confidencial deben ser destruidos cuando ya no se requieren. El dueño del documento debe autorizar o realizar esta destrucción.</p>
	Política 0706-003	<p>Tratamiento de Información de datos de tarjetahabientes.</p> <p>Todo archivo físico y/o digital con información histórica de tarjeta habientes debe ser destruido y/o eliminado.</p> <p>En consecuencia del punto anterior a partir de la fecha no se acepta almacenamiento por medios físicos y/o digitales de datos relacionados con la tarjeta del cliente.</p>
7.6.2	Política 0706-004	<p>Eliminación de Software</p> <p>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.</p>
<b>7.6.3 Procedimientos de manejo de la información</b>		
7.6.3	Política 0706-005	<p>Uso de buenas prácticas de gestión de información</p> <p>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.</p>
7.6.3	Política 0706-006	<p>Comprobación de exactitud y validez de documentos</p> <p>Se debe confirmar la validez e integridad de documentos, especialmente aquellos que comprometen y obligan a la organización.</p>
7.6.3	Política 0706-007	<p>Dependencias entre documentos y archivos</p> <p>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.</p>
7.6.3	Política 0706-008	<p>Fotocopiado de información confidencial</p> <p>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.</p>

7.6.3	Política 0706-009	<p>Eliminación de archivos temporales (tmp)</p> <p>Los archivos temporales en las computadoras de los usuarios, deben ser eliminados con regularidad para prevenir su posible mal uso por usuarios no autorizados.</p>
<b>7.6.4 Seguridad de la documentación de sistemas</b>		
7.6.4	Política 0706-010	<p>Gestión de documentación de sistemas</p> <p>La documentación de sistemas es un requisito obligatorio para todo sistema de información de la organización. Dicha documentación debe mantenerse actualizada y disponible.</p>
<b>7.7 Intercambio de Información y software</b>		
<b>7.7.1 Acuerdos para intercambio de información y software</b>		
7.7.1	Política 0707-001	<p>Envío de información a terceros</p> <p>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.</p>
<b>7.7.2 Seguridad física de medios en tránsito</b>		
7.7.2	Política 0707-002	<p>Transporte de documentos confidenciales</p> <p>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.</p>
<b>7.7.3 Seguridad en Comercio Electrónico</b>		
7.7.3	Política 0707-003	<p>Desarrollo y mantenimiento de sitios Web</p> <p>Solamente personal debidamente calificado y autorizado participará en el desarrollo y mantenimiento de sitios Web de la organización.</p>
<b>7.7.4 Seguridad del correo electrónico</b>		
7.7.4	Política 0707-004	<p>Envío de correo electrónico</p> <p>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.</p>
7.7.4	Política 0707-005	<p>Recepción de correo erróneo</p>

		Los mensajes de correo electrónico no solicitados, deben ser tratados con precaución y no ser respondidos.
7.7.4	Política 0707-006	<p>Recepción de correo no solicitado</p> <p>Se debe verificar la identidad y la autenticidad del remitente de cualquier mensaje de correo electrónico no solicitado antes de abrirlo.</p>
<b>7.7.5 Seguridad de los sistemas ofimáticos</b>		
7.7.5	Política 0707-007	<p>Gestión de máquinas contestadoras y correo de voz</p> <p>No se debe grabar información confidencial en contestadoras automáticas o sistemas de correo de voz.</p>
7.7.5	Política 0707-008	<p>Información por teléfono</p> <p>Se debe tener mucha precaución cuando se comunica información confidencial vía telefónica, verificando además la identidad de los destinatarios.</p>
7.7.5	Política 0707-009	<p>Envío erróneo de información a terceros</p> <p>Se debe comprobar cuidadosamente las direcciones de email antes de enviar información, especialmente en los casos de información confidencial. La misma precaución debe aplicarse cuando existe la posibilidad de que se divulguen las direcciones de E-mail u otra información de contacto.</p>
<b>7.7.6 Sistemas públicamente disponibles</b>		
7.7.6	Política 0707-010	<p>Seguridad de sistemas públicamente disponibles</p> <p>Se deben establecer controles en los sistemas públicos 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.</p>
<b>7.7.7 Otras formas de intercambio de información</b>		
7.7.7	Política 0707-011	<p>Transmisión e intercambio de datos</p> <p>Solamente se puede transmitir datos o información confidenciales cuando la seguridad de los datos puede garantizarse razonablemente usando técnicas de encriptación.</p>

## 8. Control de Accesos

### 8.1 Requisitos de negocio para el Control de Accesos

8.1	Política 0801-001	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.
<b>8.1.1 Política de control de accesos</b>		
8.1.1	Política 0801-002	<p>Gestión de estándares de control de accesos</p> <p>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 proporcionan acceso inmediato según los requerimientos de la organización.</p>
8.1.1	Política 0801-003	<p>Establecimiento de una estructura de carpetas y datos para usuarios</p> <p>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.</p>
8.1.1	Política 0801-004	<p>Protección de documentos con contraseñas</p> <p>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.</p>
8.1.1	Política 0801-005	<p>Defensa contra ataques internos intencionales</p> <p>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.</p>
8.1.1	Política 0801-006	<p>Configuración de acceso a la Intranet/Extranet</p> <p>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.</p>
8.1.1	Política 0801-007	<p>Configuración de acceso a Internet</p> <p>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.</p>
8.1.1	Política 0801-008	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.
<b>8.2 Gestión de Acceso de Usuarios</b>		
8.2	Política 0802-001	<p>Gestión de Acceso de Usuarios</p> <p>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.</p>
8.2	Política 0802-002	<p>Inicio y fin de sesión</p> <p>Los sistemas deben considerar el manejo de sesiones con los usuarios, las cuales se cerrarán después de un tiempo de no uso (time-out).</p>
<b>8.2.1 Registro de usuarios</b>		
8.2.1	Política 0802-003	<p>Registro e identificador de usuarios</p> <p>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.</p>
<b>8.2.2 Gestión de privilegios</b>		
8.2.2	Política 0802-004	<p>Asignación de privilegios</p> <p>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.</p>
<b>8.2.3 Gestión de contraseñas de usuario</b>		
8.2.3	Política 0802-005	<p>Gestión de contraseñas</p> <p>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.</p>
<b>8.2.4 Revisión de los derechos de acceso de los usuarios</b>		
8.2.4	Política 0802-006	<p>Manejo de renuncias de personal</p> <p>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</p>

		personal saliente constituyen un riesgo inaceptable para la organización y, si es así, deben revocarse todos los derechos de acceso.
8.2.4	Política 0802-007	<p>Personal que trabajará en instituciones competidoras</p> <p>Se deben 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.</p>
<b>8.3 Responsabilidades de los Usuarios</b>		
<b>8.3.1 Uso de contraseñas</b>		
8.3.1	Política 0803-008	<p>Responsabilidad de usuarios en el uso de contraseñas</p> <p>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.</p>
<b>8.3.2 Equipo informático de usuario desatendido</b>		
8.3.2	Política 0803-009	<p>Protección de computadoras desatendidas</p> <p>Todos los usuarios de computadoras personales y laptops deben asegurarse que sus pantallas queden protegidas y no muestren información cuando estén desatendidas.</p>
<b>8.4 Control de Acceso a la Red</b>		
8.4	Política 0804-001	<p>Gestión de controles de acceso a la red</p> <p>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.</p>
8.4	Política 0804-002	<p>Configuración de redes</p> <p>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.</p>
8.4	Política 0804-003	<p>Gestión de seguridad de redes</p> <p>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.</p>
<b>8.4.1 Política de uso de los servicios de la red</b>		
<b>8.4.2 Ruta forzosa</b>		
8.4.2	Política 0804-004	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.
<b>8.4.3 Autenticación de usuarios para conexiones externas</b>		
8.4.3	Política 0804-005	<p>Acceso remoto a la red</p> <p>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.</p>
<b>8.4.4 Autenticación de nodos de la red</b>		
8.4.4	Política 0804-006	<p>Autenticación de dispositivos remotos</p> <p>Las conexiones remotas a sistemas informáticos se deberán autenticar con la finalidad de reducir la amenaza de accesos no autorizados a las aplicaciones.</p>
<b>8.4.5 Protección a puertos de diagnóstico remoto</b>		
8.4.5	Política 0804-007	<p>Protección acceso a puertos de diagnóstico</p> <p>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.</p>
<b>8.5 Control de acceso al sistema operativo</b>		
8.5	Política 0805-001	<p>Control de acceso al Sistema Operativo</p> <p>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.</p>
<b>8.5.1 Identificación automática de terminales</b>		
8.5.1	Política 0805-002	<p>Identificación automática de terminales o sesiones emuladas.</p> <p>Se debe usar la identificación automática de terminales o sesiones emuladas para autenticar las conexiones a ubicaciones específicas y a equipos portátiles.</p>
<b>8.5.2 Procedimientos de conexión de terminales</b>		
8.5.2	Política 0805-003	<p>Conexión al sistema informático</p>

		El procedimiento de conexión a los sistemas informáticos debe minimizar la posibilidad de accesos no autorizados.
<b>8.5.3 Identificación y autenticación del usuario</b>		
8.5.3	Política 0805-004	<p>Identificación del usuario</p> <p>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).</p>
<b>8.6 Control de Acceso a las aplicaciones</b>		
<b>8.6.1 Restricción de acceso a la información</b>		
8.6.1	Política 0806-001	<p>Restricción de acceso</p> <p>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.</p>
<b>8.6.2 Aislamiento de sistemas sensibles</b>		
8.6.2	Política 0806-002	<p><b>Administración de acceso a sistemas altamente confidenciales</b></p> <p>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.</p>
<b>8.7 Seguimiento de accesos y usos del sistema</b>		
<b>8.7.1 Registro de incidentes</b>		
8.7.1	Política 0807-001	<p>Registro de evidencias de incidentes</p> <p>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.</p>
<b>8.7.2 Seguimiento del uso de los sistemas</b>		
8.7.2	Política 0807-002	<p>Monitoreo de accesos y uso del sistema</p> <p>Se debe registrar y supervisar el acceso a los sistemas para identificar su posible mala utilización.</p>
8.7.2	Política 0807-003	<p>Integridad de las investigaciones de incidentes de Seguridad de la Información.</p>

		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.
<b>8.7.3 Sincronización de relojes</b>		
8.7.3	Política 0807-004	<p>Sincronización de relojes del sistema</p> <p>Los relojes del sistema se deben sincronizar regularmente, especialmente cuando hay diferentes plataformas de procesamiento.</p>
<b>8.8 Informática móvil y teletrabajo</b>		
<b>8.8.1 Informática móvil</b>		
8.8.1	Política 0808-001	<p>Uso de equipos portátiles de cómputo</p> <p>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.</p>
8.8.1	Política 0808-002	<p>Uso de facilidades de centros empresariales</p> <p>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.</p>
8.8.1	Política 0808-003	<p>Respaldo de datos (backup) de equipos portátiles de cómputo</p> <p>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.</p>
8.8.1	Política 0808-004	<p>Viajes de trabajo</p> <p>Los empleados que viajan por asuntos de la organización son responsables de la seguridad de la información en su poder.</p>
8.8.1	Política 0808-005	<p>Correo electrónico corporativo en dispositivos móviles.</p> <p>La posibilidad de sincronización de correo electrónico a dispositivos móviles se debe brindar previa autorización expresa y por escrito del dueño del proceso o gerente de área.</p>

--

<b>9.1 Requisitos de seguridad de los sistemas</b>		
9.1	Política 0901-001	<p>Implementación de software nuevo o mejorado</p> <p>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.</p>
9.1	Política 0901-002	<p>Documentación de sistemas</p> <p>Todos los sistemas deben tener documentación completa y actualizada. Ningún sistema debe pasar a producción si no tiene la documentación de soporte disponible.</p>
<b>9.1.1 Análisis y especificación de los requisitos de seguridad</b>		
9.1.1	Política 0901-003	<p>Justificación de desarrollo de nuevos sistemas</p> <p>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.</p>
9.1.1	Política 0901-004	<p>Desarrollo y mantenimiento de software</p> <p>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.</p>
9.1.1	Política 0901-005	<p>Interfaces de software aplicativo</p> <p>El desarrollo de interfaces de sistemas es una tarea altamente especializada y por lo tanto sólo debe ser realizada por profesionales con la debida cualificación y experiencia comprobada en el tema. Debe considerar sobremana los aspectos de seguridad de los sistemas que están conectados y de las plataformas que intervienen.</p>
<b>9.2 Seguridad de las aplicaciones del sistema</b>		
<b>9.2.1 Validación de los datos de entrada</b>		
	Política 0902-001	<p>Control de datos de entrada</p> <p>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.</p>

<b>9.2.2 Control del proceso interno</b>		
	Política 0902-002	<p>Control de datos en proceso</p> <p>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.</p>
<b>9.2.3 Validación de los datos de salida</b>		
	Política 0902-004	<p>Control de datos de salida</p> <p>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.</p>
<b>9.3 Seguridad de los archivos del sistema</b>		
<b>9.3.1 Control del software en producción</b>		
9.3.1	Política 0904-001	<p>Gestión de operaciones y administración de sistemas</p> <p>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.</p>
9.3.1	Política 0904-002	<p>Gestión de bibliotecas de programas en producción</p> <p>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.</p>
<b>9.3.2 Protección de los datos de prueba del sistema</b>		
9.3.2	Política 0904-003	<p>Uso de datos para pruebas</p> <p>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 datos reales confidenciales, éstos deben ser despersonalizados antes de ser usados.</p>
<b>9.3.3 Control de acceso a la biblioteca de programas fuente</b>		
9.3.3	Política 0904-004	<p>Gestión de bibliotecas de programas fuente</p> <p>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</p>

		estar definidos formalmente de acuerdo a la metodología de desarrollo de sistemas de la organización.
<b>9.4 Seguridad en los procesos de desarrollo y soporte</b>		
<b>9.4.1 Procedimientos de control de cambios</b>		
9.4.1	Política 0905-001	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.
9.4.1	Política 0905-002	Control de versiones  Se deben aplicar procedimientos del control de versiones a todos los programas de software y procedimientos pertenecientes a la organización.
9.4.1	Política 0905-003	Actualizaciones de software recomendadas por el proveedor  Solo 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.
9.4.1	Política 0905-004	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 <b>procedimientos acordados de control de cambios</b> .
<b>9.4.2 Desarrollo externo del software</b>		
	Política 0905-007	Calidad de desarrollo externo  Todo desarrollo externo de software debe determinar los derechos de propiedad intelectual. Se debe tener acuerdos para manejar los posibles fallos del contratista.
<b>10. Gestión de Incidentes en la Seguridad de Información</b>		
<b>10.1 Reporte de eventos y debilidades de la Seguridad de la Información</b>		
<b>10.1.1 Reporte de Eventos</b>		
10.1.1	Política -1005-001	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

		<p>reporte un punto de contacto que siempre esté disponible y que sea capaz de proveer respuestas adecuadas a tiempo.</p>
	Política -1005-002	<p>Procedimiento del reporte</p> <p>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.</p>
10.1.1	Política -1005-003	<p>Recolectando evidencias</p> <p>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</p>
10.1.1	Política -1005-004	<p>Respuesta del sistema</p> <p>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.</p>
<b>10.1.2 Reporte de Debilidades</b>		
10.1.2	Política -1005-005	<p>Mecanismo de reporte</p> <p>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.</p>
10.1.2	Política -1005-006	<p>Probar debilidades</p> <p>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.</p>
<b>10.2 Gestión de las mejoras e incidentes de la Seguridad de Información</b>		
	Política -1005-007	<p>Responsabilidades y procedimiento de las mejoras e incidentes de la seguridad de información.</p> <p>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.</p>
<b>10.2.1 Responsabilidades y procedimientos</b>		
10.2.1	Política -1005-008	<p>Monitoreo del sistema, alerta y vulnerabilidad</p>

		El monitoreo de los sistemas, alertas y vulnerabilidades deben ser utilizados para detectar los incidentes en la seguridad de información.
10.2.1	Política -1005-009	<p>Pautas para procedimientos de la gestión de incidentes en la seguridad de información</p> <p>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.</p>
<b>10.2.2 Recolección de evidencia</b>		
10.2.2	Política -1005-010	<p>Acciones para recolectar evidencias</p> <p>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.</p>
10.2.2	Política -1005-011	<p>Acciones para los Procesos internos</p> <p>Los procesos internos deben ser desarrollados y seguidos cuando se recolecta y presenta evidencia para propósitos disciplinarios maniobrados dentro de la organización.</p>
10.2.2	Política -1005-012	<p>Admisibilidad de la evidencia</p> <p>Para lograr admisibilidad de la evidencia, la organización debe asegurar que sus sistemas de información cumplan con cualquier estándar o código publicado de práctica para la producción de evidencia admisible.</p>
10.2.2	Política -1005-013	<p>Integridad de material de evidencia</p> <p>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 realizó dicha actividad, y que herramientas y programas se utilizaron.</p>

## 11. Gestión de Continuidad del Negocio

### 11.1 Aspectos de la Gestión de Continuidad del Negocio

#### 11.1.1 Proceso de gestión de la continuidad del negocio

11.1.1	Política 1101-001	<p>Gestión de continuidad del negocio</p> <p>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.</p>
	Política 1101-002	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.
11.1.1	Política 1101-003	<p>Iniciativa para el Plan de Continuidad del Negocio</p> <p>La gerencia debe tener la iniciativa en la realización del Plan de Continuidad del Negocio.</p>
11.1.1	Política 1101-004	<p>Plan de recuperación de desastres</p> <p>Los dueños de sistemas de información críticos deben asegurarse que sus sistemas cuentan con planes de recuperación de desastres probados y en funcionamiento.</p>
<b>11.1.2 Continuidad del negocio y análisis de impactos</b>		
11.1.2	Política 1101-005	<p>Análisis de impactos</p> <p>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.</p>
11.1.2	Política 1101-006	<p>Minimización de impacto de ataques informáticos</p> <p>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.</p>
<b>11.1.4 Marco de planificación para la continuidad del negocio</b>		
	Política 1101-007	<p>Responsabilidades de los Planes de Continuidad</p> <p>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.</p>
	Política 1101-008	<p>Activación de los Planes de Continuidad</p> <p>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.</p>

	Política 1101-009	<p>Mantenimiento y concientización</p> <p>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.</p>
	Política 1101-010	<p>Se debe proteger la integridad de las personas, empleados y clientes, y bienes de la entidad en forma adecuada, realizando una buena administración de los incidentes.</p>
	Política 1101-011	<p>Se debe garantizar que los empleados, se encuentren protegidos, sepan dónde ir, qué hacer, qué recursos necesitan en situaciones de crisis, minimizando así la toma de decisiones inadecuadas y evitar cometer errores durante la crisis.</p>
	Política 1101-012	<p>El plan de continuidad de negocio está orientado a la protección de las personas, así como al restablecimiento oportuno de los procesos, servicios críticos e infraestructura, frente a eventos de interrupción o desastre.</p>
	Política 1101-013	<p>Los procesos / servicios críticos de la organización que sean desarrollados por terceros contratados deben disponer de planes de continuidad, para lo cual el funcionario interventor del contrato debe solicitar este documento y remitir a la Oficina de Riesgos, donde se analizará la cobertura del mismo. Adicionalmente, se debe verificar que los planes, en lo que corresponden a los servicios convenidos, funcionen en las condiciones esperadas, donde la Oficina de Riesgos debe coordinar con el área responsable del contrato la ejecución de pruebas a dicho plan.</p>
	Política 1101-014	<p>La Junta Directiva de CVU y VC, establecerá el Comité de Crisis y el Comité de Continuidad, con sus respectivos delegados y backups, los cuales tienen la responsabilidad de activar y administrar el Plan de Continuidad del Negocio.</p>
<b>11.1.5 Prueba, mantenimiento y reevaluación de los Planes de Continuidad</b>		
11.1.5	Política 1101-015	<p>Prueba del Plan de Continuidad del Negocio</p> <p>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.</p>
11.1.5	Política 1101-016	<p>Mantenimiento y reevaluación del Plan de Continuidad del Negocio</p> <p>El Plan de Continuidad del Negocio debe ser continuamente actualizado para reflejar los cambios en los recursos, procesos y servicios de la organización.</p>
<b>12. Cumplimiento</b>		
<b>12.1 Cumplimiento con requisitos legales</b>		
<b>12.1.1 Identificación de legislación aplicable</b>		

	Política 1201-001	<p>Documentación de requisitos</p> <p><b>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.</b> Esta documentación estará disponible para uso legal y técnico del sistema.</p>
12.1.1	Política 1201-002	<p>Cuidados contra denuncias de difamación y calumnias</p> <p>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.</p>
<b>12.1.2 Derechos de propiedad intelectual</b>		
	Política 1201-003	<p>Responsabilidad de la Alta Dirección</p> <p>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.</p>
12.1.2	Política 1201-004	<p>Responsabilidad de la Dirección de Personal</p> <p>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.</p>
12.1.2	Política 1201-005	<p>Renovación de nombres de dominio de sitios Web</p> <p>Se deben proteger y asegurar los nombres de dominio de Internet de forma similar a cualquier otro activo valioso de la organización.</p>
12.1.2	Política 1201-006	<p>Propiedad intelectual de trabajos dentro de la organización</p> <p>Los derechos de propiedad intelectual de trabajos llevados a cabo dentro de un contrato con la organización se protegerán mediante acuerdos formales.</p>
12.1.2.	Política 1201-007	<p>Uso de software licenciado</p> <p>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.</p>
12.1.2	Política 1201-008	<p>Uso de información protegida por derechos de autor (con copyright) de la Internet</p>

		Para utilizar información obtenida de la Internet o de otras fuentes electrónicas, se debe obtener la autorización del propietario de los derechos de autor.
12.1.2	Política 1201-009	<p>Envío electrónico de información protegida por derechos de autor (con copyright)</p> <p>Para retransmitir información por Internet u otras fuentes electrónicas, se debe obtener la autorización del propietario de los derechos de autor.</p>
<b>12.1.3 Protección de los registros de la organización</b>		
12.1.3	Política 1201-010	<p>Archivamiento de documentos</p> <p>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.</p>
12.1.3	Política 1201-011	<p>Conservación de información</p> <p>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.</p>
12.1.3	Política 1201-012	<p>Conservación o borrado de correo electrónico</p> <p>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.</p>
<b>12.1.4 Protección de los datos y de la privacidad de la información personal</b>		
12.1.4	Política 1201-013	<p>Confidencialidad de información de clientes</p> <p>Se debe proteger la información de contacto de cliente y terceros de cualquier acceso no autorizado.</p>
12.1.4	Política 1201-014	<p>Información confidencial de trabajadores</p> <p>Sólo personas expresamente autorizadas podrán tener acceso a información personal sobre los trabajadores de la organización, al ser dicha información estrictamente confidencial.</p>
12.1.4	Política 1201-015	<p>Gestión de datos de tarjetas de crédito de clientes</p>

		La información obtenida a partir del acceso a tarjetas de crédito de clientes debe utilizarse de tal manera que dicha información esté protegida contra todas las formas conocidas de acceso no autorizado, para lo cual deben usarse controles administrativos.
<b>12.1.5 Prevención del mal uso de los recursos de tratamiento de la información</b>		
12.1.5	Política 1201-016	<p>Uso de fotocopiadoras con fines personales</p> <p>Las fotocopiadoras y/o duplicadoras, no deben usarse para uso personal. De manera excepcional, el supervisor inmediato puede dar permiso específico al empleado para su uso.</p>
12.1.5	Política 1201-017	<p>Uso del correo para fines personales</p> <p>El uso personal del correo electrónico (email) debe reducirse al mínimo. El correo postal sólo se debe utilizar para propósitos de la organización.</p>
12.1.5	Política 1201-018	<p>Uso del teléfono para fines personales</p> <p>Las llamadas telefónicas personales a través de sistemas telefónicos, incluidos los móviles, de la organización deben ser reducidas al mínimo.</p>
12.1.5	Política 1201-019	<p>Juegos en computadores</p> <p>El uso de computadoras de la organización para juegos está estrictamente prohibido.</p>
<b>12.1.7 Recopilación de pruebas</b>		
12.1.7	Política 1201-020	<p>Recolección de pruebas de delitos informáticos</p> <p>La organización denunciará, con todo el peso de la ley, a los autores de delitos informáticos. Se deben desarrollar procedimientos apropiados para asegurar la recolección y protección adecuada de evidencias.</p>
12.1.7	Política 1201-021	<p>Recopilación de evidencias de brechas de Seguridad de la Información</p> <p>Toda evidencia referente a brechas de seguridad de la información debe ser recopilada y remitida al OSI.</p>
<b>12.2 Revisiones de la Política de Seguridad y de la conformidad técnica</b>		
<b>12.2.1 Conformidad con la política de seguridad</b>		
12.2.1	Política 1202-001	<p>Cumplimiento de las Políticas de Seguridad de la Información</p> <p>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.</p>

<b>12.2.2 Comprobación de la conformidad técnica</b>		
	Política 1202-002	<p>Examen y pruebas de conformidad</p> <p>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, realizados por profesionales independientes especialistas en el tema.</p>
<b>12.3 Consideraciones sobre la auditoría de sistemas</b>		
<b>12.3.1 Controles de auditoría de sistemas</b>		
	Política 1202-003	<p>Planificación de las actividades de auditoría</p> <p>Para minimizar el riesgo de interrupción de los procesos de negocio, las actividades de auditoría se deberán planificar cuidadosamente, registrándose y supervisando todos los accesos. Asimismo, todos los procedimientos, requisitos y responsabilidades deberán estar documentados.</p> <p>Los registros de auditoría debieran incluir, cuando sea relevante:</p> <ul style="list-style-type: none"> <li>a) utilizar IDs;</li> <li>b) fechas, horas y detalles de eventos claves; por ejemplo, ingreso y salida;</li> <li>c) identidad o ubicación de la identidad, si es posible;</li> <li>d) registros de intentos de acceso fallidos y rechazados al sistema;</li> <li>e) registros de intentos de acceso fallidos y rechazados a la data y otros recursos;</li> <li>f) cambios en la configuración del sistema;</li> <li>g) uso de privilegios;</li> <li>h) uso de las utilidades y aplicaciones del sistema;</li> <li>i) archivos a los cuales se tuvo acceso y los tipos de acceso;</li> <li>j) alarmas activadas por el sistema de control de acceso;</li> <li>k) activación y desactivación de los sistemas de protección; como sistemas anti-virus y sistemas de protección perimetral.</li> </ul>

**HISTORIAL DE CAMBIOS DEL DOCUMENTO**

FECHA DE MODIFICACIÓN/ ACTUALIZACIÓN	VERSIÓN DEL DOCUMENTO	NATURALEZA DE LA MODIFICACIÓN
21/11/2023	1.0	Se realizan cambios en el diseño general del documento, disposición de párrafos, y estructura de las tablas.
11/12/2023	2.0	Se añade la política 0301-006 / Responsabilidad de Proveedor(es) de servicios para transacciones con tarjeta de crédito.