SOMOS moviendo futuro

SISTEMA OPERATIVO DE MOVILIDAD ORIENTE SOSTENIBLE

PLAN ESTRATEGICO DE TECNOLOGIAS Y SEGURIDAD DE LA INFORMACIÓN

Aprobó:

MARIA ALEJANDRA PEÑUELA RUBIO
GERENTE

2026

CONTROL CAMBIOS

Día	Mes	Año	Versión	Contenido	Elaboró	Revisó	Aprobó
22	6	2022	1	Creación documento	JCGP - PAG	DAGT	ORRS
23	01	2026	2	Actualización	SVM - TIC	DAGT	MAPR

1. OBJETIVO

Proteger, preservar y administrar objetivamente la información de LA ENTIDAD junto con las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de las características de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información.

1.1. OBJETIVOS ESPECIFICOS

- Mantener la Política de Seguridad de la Información actualizada, vigente, operativa y auditada dentro del marco determinado por los riesgos globales y específicos de SOMOS Rionegro S.A.S para asegurar su permanencia y nivel de eficacia.

- Definir las directrices de SOMOS Rionegro S.A.S para la correcta valoración, análisis y evaluación de los riesgos de seguridad asociados a la información y su impacto, identificando y evaluando diferentes opciones para su tratamiento con el fin de garantizar la continuidad e integridad de los sistemas de información.

2. ALCANCE

Esta política es de aplicación para SOMOS Rionegro S.A.S en el conjunto de dependencias que la componen, a sus recursos, a la totalidad de los procesos internos o externos vinculados a SOMOS Rionegro S.A.S a través de contratos o acuerdos con terceros y a todo el personal, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe.

3. DEFINICIONES

Activo de Información: Datos o información propiedad de SOMOS Rionegro S.A.S que se almacena en cualquier tipo de medio y que es considerada por la misma como sensitiva o crítica para el cumplimiento de los objetivos misionales.

Administración de Riesgos: Proceso de identificación, control y reducción o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

Autenticidad: Los activos de información los crean, editan y custodian usuarios reconocidos quienes validan su contenido.

Cadena de custodia: En el ámbito de la seguridad de la información, la cadena de custodia es la aplicación de una serie de normas y procedimientos tendientes a asegurar, depositar y proteger cada activo de información para evitar la pérdida de integridad, disponibilidad o confidencialidad.

Comité de Seguridad de la Información (Informática y Telecomunicaciones): El Comité de Seguridad de la Información, es un cuerpo integrado por diferentes representantes de SOMOS destinado a garantizar el apoyo manifiesto de las directivas a las iniciativas de seguridad. Su función principal es definir, estructurar, recomendar, hacer seguimiento y mejorar el Sistema de Gestión de Seguridad de la Información (SGSI) SOMOS. Depende directamente de la Gerencia, sirviendo como consultor técnico en temas relacionados con la seguridad de la información.

Confiabilidad de la Información: Es fiable el contenido de los activos de información que conserven la confidencialidad, integridad, disponibilidad, autenticidad y legalidad.

Confidencialidad: los activos de información solo pueden ser accedidos y custodiados por usuarios que tengan permisos para ello.

Disponibilidad: Los activos de información sólo pueden ser obtenidos a corto plazo por los usuarios que tengan los permisos adecuados.

Evaluación de Riesgos: Evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto.

Gestión pública: Es el conjunto de acciones mediante las cuales las entidades tienden al logro de sus fines, objetivos y metas, los que están enmarcados por las políticas gubernamentales establecidas por el Poder Ejecutivo.

Grupo responsable de Seguridad Informática: Grupos de apoyo creados para que manejan información sensible o crítica y que se encargan de velar por la operación del SGSI. Están conformados por funcionarios o contratistas de LA ENTIDAD que tengan formación en temas de seguridad de la información.

Imagen corporativa: Es el elemento por medio del cual se define la identidad de la empresa, es la percepción del público interno y externo.

Incidente de Seguridad Informática: Un incidente de seguridad informática es un evento adverso en un sistema de computadoras, o red de computadoras, que compromete la confidencialidad, integridad, disponibilidad, legalidad o confiabilidad de la información.

Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

Información: Toda forma de conocimiento objetivo con representación física o lógica explícita.

Integridad: El contenido de los activos de información debe permanecer inalterado y completo. Las modificaciones realizadas deben ser registradas asegurando su confiabilidad.

Legalidad: Los activos de información cumplen los parámetros legales, normativos y estatutarios de la institución.

Medios de comunicación interna: Se trata de los canales internos de comunicación, cuya creación debe responder a un diagnóstico del estado de la comunicación interna de la organización. Pueden ser: carteleras, boletines, correo institucional, intranet, material POP, suvenires, reuniones institucionales, comités primarios, entre otros.

No repudio: Los autores, propietarios y custodios de los activos de información se pueden identificar plenamente.

Posibilidad de Auditoría: Se mantienen evidencias de todas las actividades y acciones que afectan a los activos de información.

Propietario de Activos de Información: En el contexto de la norma NTC 27001, un propietario de activos de información es cualquier persona o entidad a la cual se le asigna la responsabilidad formal de custodiar y asegurar un activo de información o un conjunto de ellos.

Protección a la duplicación: Los activos de información son objeto de clasificación, y se llevan registros de las copias generadas de aquellos catalogados como confidenciales.

Responsable de Seguridad Informática: Coordinador general del Comité de Seguridad de la Información. Su función principal es supervisar el cumplimiento de la presente Política y los lineamientos del SGSI.

Sistema de Información: Conjunto ordenado de elementos cuyas propiedades se relacionan e interaccionan permitiendo la recopilación, procesamiento, mantenimiento, transmisión y difusión de información utilizando diferentes medios y mecanismos tanto automatizados como manuales.

Tecnología de la Información: Conjunto de hardware y software operados por la entidad - o por un tercero en su nombre, que componen la plataforma necesaria para procesar y administrar la información que requiere la entidad para llevar a cabo sus funciones.

4. CONDICIONES GENERALES

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal de SOMOS Rionegro S.A.S cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe.

El Comité de Seguridad de la Información es responsable de revisar y proponer el texto de la Política de Seguridad de las tecnologías de la Información, las funciones generales en materia de seguridad de la información y la estructuración, recomendación, seguimiento y mejora del Sistema de Gestión de Seguridad Información. Es responsabilidad de dicho comité definir las estrategias de capacitación en materia de seguridad de la información al interior de la entidad. Asimismo, cumplir lo siguiente:

- El Coordinador del Comité de Seguridad de la Información será el responsable de coordinar las acciones del Comité y de impulsar la implementación y cumplimiento de la presente Política.

- El grupo responsable de Seguridad Informática será responsable de cumplir funciones relativas a la seguridad de los sistemas de información de la entidad, lo cual incluye la operación del SGSI y supervisión del cumplimiento, dentro de la dependencia, de aspectos inherentes a los temas tratados en la presente Política.

- El nivel de supervisión que pueda realizar cada grupo responsable de seguridad, está relacionado con el talento humano que lo conforma y en todo caso deberá ser aprobado por el Comité de Seguridad de la Información.

- Los propietarios de activos de información (ver su definición en el glosario) son responsables de la clasificación, mantenimiento y actualización de la misma; así como de documentar y mantener actualizada la clasificación efectuada, definiendo qué usuarios deben tener permisos de acceso a la información de acuerdo a sus funciones y competencia. En general, tienen la responsabilidad de mantener íntegro, confidencial y disponible el activo de información mientras que es desarrollado, producido, mantenido y utilizado.

- El área de Recursos Humanos y/o la secretaria general cumplirá la función de notificar a todo el personal que se vincula contractualmente con SOMOS, de las obligaciones respecto del cumplimiento de la Política de Seguridad de la Información

y de todos los estándares, procesos, procedimientos, prácticas y guías que surjan del Sistema de Gestión de la Seguridad de la Información. De igual forma, será responsable de la notificación de la presente Política y de los cambios que en ella se produzcan a todo el personal, a través de la suscripción de los Compromisos de Confidencialidad y de tareas de capacitación continua en materia de seguridad según lineamientos dictados por el Comité de Seguridad de la Información.

- El coordinador del área de Sistemas debe seguir los lineamientos de la presente política y cumplir los requerimientos que en materia de seguridad informática se establezcan para la operación, administración, comunicación y mantenimiento de los sistemas de información y los recursos de tecnología de SOMOS.

- Corresponde a dicha área determinar el inventario de activos de información y recursos tecnológicos de los cuales es propietario o custodio, el cual será revisado y avalado por él.

- El área Jurídica de SOMOS, verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación con empleados y con terceros. Asimismo, asesorará en materia legal en lo que se refiere a la seguridad de la información.

- Los usuarios de la información y de los sistemas utilizados para su procesamiento son responsables de conocer y cumplir la Política de Seguridad de la Información vigente.

- La Oficina de Control Interno es responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la gestión de activos de información y la tecnología de información. Es su responsabilidad informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta Política y por las normas, procedimientos y prácticas que de ella surjan.

5. DESCRIPCIÓN DEL PROCEDIMIENTO

DESCRIPCIÓN DE LA ETAPA	RESPONSABLE
IDENTIFICACIÓN, CLASIFICACIÓN Y VALORACIÓN DE ACTIVOS DE INFORMACIÓN. Cada dependencia, bajo supervisión del Comité de Seguridad de la Información, debe elaborar y mantener un inventario de los activos de información que poseen (procesada y producida). Las características del	Gerencia General TIC´S

inventario, donde se incorpore la clasificación, valoración, ubicación y acceso de la información, las especifica el Comité de Seguridad de la Información, correspondiendo al área de Sistemas brindar herramientas que permitan la administración del inventario por cada dependencia, garantizando la disponibilidad, integridad y confidencialidad de los datos que lo componen. El área de sistemas de SOMOS tiene la responsabilidad de mantener el inventario completo y actualizado de los recursos de hardware y software.	
SEGURIDAD DE LA INFORMACIÓN EN EL RECURSO HUMANO Todo el personal de SOMOS, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe debe tener asociado un perfil de uso de los recursos de información, incluyendo el hardware y software asociado. El área de Sistemas debe mantener un directorio completo y actualizado de tales perfiles. El Comité de Seguridad de la Información determina cuales son los atributos que deben definirse para los diferentes perfiles. El Comité de Seguridad de la Información debe elaborar, mantener, actualizar, mejorar y difundir el manual de “Responsabilidades Personales para la Seguridad de la Información en LA ENTIDAD”. La responsabilidad de custodia de cualquier archivo mantenido, usado o producido por el personal que se retira, o cambia de cargo, recae en el supervisor del contrato; en todo caso el proceso de cambio en la cadena de custodia de la información debe hacer parte integral del procedimiento de terminación de la relación contractual o de cambio de cargo.	TIC´S
RESPONSABILIDADES DEL PERSONAL DE LA ENTIDAD Todo el personal de SOMOS, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y las tareas que desempeñe, debe firmar un acuerdo que contenga los términos y condiciones que regulan el uso de recursos de TI y las reglas y perfiles que autorizan el uso de la información SOMOS.	

Los procedimientos para obtener tales perfiles y las características de cada uno de ellos deben ser mantenidos y actualizados por cada dependencia, de acuerdo a los lineamientos dados por el área de Sistemas, en cuanto a la información y en a los dispositivos hardware y los elementos software. El manual de funciones de SOMOS debe contemplar procesos y sanciones disciplinarias para los casos en que se presente usos de información y TI que violen los términos y condiciones. El área de Recursos Humanos y/o la secretaria general, junto con el área de Sistemas, se encargarán de crear, actualizar, mantener y ejecutar un plan de capacitación en seguridad de la información que propenda por el crecimiento continuo de la conciencia individual y colectiva en temas de seguridad de la información. El área de Sistemas se encargará de crear y mantener un centro documental de acceso general con información relacionada con temas de seguridad de la información tales como responsabilidad en la administración de archivos, buenas prácticas, amenazas de seguridad, entre otros.	Talento Humano
RESPONSABILIDADES DE LOS USUARIOS INTERNOS Para poder usar los recursos de TI de SOMOS, los usuarios internos deben leer y aceptar un acuerdo con los términos y condiciones. El área de Sistemas debe asegurar los mecanismos para la difusión y aceptación de dichas condiciones. SOMOS debe contemplar procesos y sanciones disciplinarias para los casos en que se presente usos de información y TI que violen los términos y condiciones.	TIC´S
RESPONSABILIDADES DE USUARIOS EXTERNOS Todos los usuarios externos y personal de empresas externas deben estar autorizados por un miembro del personal de SOMOS quien será responsable del control y vigilancia del uso adecuado de la información y los recursos de TI institucionales. Los procedimientos para el registro de tales usuarios deben ser creados y mantenidos por el área de Sistemas y la Oficina de Recursos Humanos y/o la secretaria general. Los usuarios externos deben aceptar por escrito los términos y condiciones de uso de la información y recursos de TI institucionales. Las cuentas de	TIC´S Comunicaciones

usuarios externos deben ser de perfiles específicos y tener caducidad no superior a tres (3) meses, renovables de acuerdo a la naturaleza del usuario.	
USUARIOS INVITADOS Y SERVICIOS DE ACCESO PÚBLICO El acceso de usuarios no registrados solo debe ser permitido al sitio web de información de LA ENTIDAD. El acceso y uso a cualquier otro tipo de recurso de información y TI no es permitido a usuarios invitados no autorizados o no registrados.	TIC´S Comunicaciones
SEGURIDAD FÍSICA Y DEL ENTORNO **ACCESO** Se debe tener acceso controlado y restringido a los cuartos de servidores principales, subsidiarios y a los cuartos de comunicaciones. El área de Sistemas elaborará y mantendrán las normas, controles y registros de acceso a dichas áreas. **SEGURIDAD EN LOS EQUIPOS** Los servidores que contengan información y servicios de SOMOS deben ser mantenidos en un ambiente seguro y protegido por los menos con: • Controles de acceso y seguridad física. • Detección de incendio y sistemas de extinción de conflagraciones. • Controles de humedad y temperatura. • Bajo riesgo de inundación. • Sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS). Toda información DE LA ENTIDAD en formato digital debe ser mantenida en servidores aprobados por el área de Sistemas. El Comité de Seguridad de la Información define el límite de responsabilidades de las dependencias. No se permite el alojamiento de información de LA ENTIDAD en servidores externos sin que medie una aprobación por escrito del Comité de Seguridad de la Información. Equipos y claves de comunicaciones deben se alimentados por sistemas de potencia eléctrica regulados y estar protegidos por UPS. El área de Sistemas debe asegurar que la infraestructura de servicios de TI está cubierta por mantenimiento y soporte adecuados de hardware y software. Las estaciones de trabajo deben estar correctamente aseguradas y operadas por personal de SOMOS, el cual debe estar capacitado acerca del contenido de esta	TIC´S Talento Humano Secretaría General

política y de las responsabilidades personales en el uso y administración de la información institucional. Los medios que alojan copias de seguridad deben ser conservados de forma correcta de acuerdo a las políticas y estándares que para tal efecto elabore y mantenga el Comité de Seguridad en la Información. Las dependencias tienen la responsabilidad de adoptar y cumplir las normas definidas para la creación y el manejo de copias de seguridad.	
ADMINISTRACIÓN DE LAS COMUNICACIONES Y OPERACIONES **REPORTE E INVESTIGACIÓN DE INCIDENTES DE SEGURIDAD** El personal de SOMOS debe reportar con diligencia, prontitud y responsabilidad presuntas violaciones de seguridad a través de su jefe inmediato o supervisor contractual al área de Sistemas. En casos especiales dichos reportes podrán realizarse directamente al área de Sistemas, la cual debe garantizar las herramientas informáticas para que formalmente se realicen tales denuncias. El Comité de Seguridad de la Información debe preparar, mantener y difundir las normas, procesos y guías para el reporte e investigación de incidentes de seguridad. De conformidad con la ley, SOMOS podrá interceptar o realizar seguimiento a las comunicaciones por diferentes mecanismos, previa autorización del Comité de Seguridad de la Información (Informática y Telecomunicaciones), y en todo caso notificando previamente a los afectados por esta decisión. El área de Sistemas mantendrá procedimientos escritos para la operación de sistemas cuya no disponibilidad suponga un impacto alto en el desarrollo normal de actividades. A dichos sistemas se debe realizar seguimiento continuo del desempeño para asegurar la confiabilidad del servicio que prestan.	TIC´S Talento Humano Secretaría General
PROTECCIÓN CONTRA SOFTWARE MALICIOSO Y HACKING Todos los sistemas informáticos deben ser protegidos teniendo en cuenta un enfoque multinivel que involucre controles humanos, físicos técnicos y administrativos. El Comité de Seguridad de la Información elaborará y	

mantendrá un conjunto de políticas, normas, estándares, procedimientos y guías que garanticen la mitigación de riesgos asociados a amenazas de software malicioso y técnicas de hacking. En todo caso y como control mínimo, las estaciones de trabajo de SOMOS deben estar protegidas por software antivirus con capacidad de actualización automática en cuanto a firmas de virus. Los usuarios de las estaciones no están autorizados a deshabilitar este control. SOMOS a través del área de Sistemas podrá hacer seguimiento al tráfico de la red cuando se tenga evidencias de actividad inusual o detrimentos en el desempeño. La dependencia que realice dicho seguimiento deberá informar a SOMOS, a través de correo electrónico o noticias en el portal institucional, de la ejecución de esta tarea. El área de Sistemas debe mantener actualizada una base de datos con alertas de seguridad reportadas por organismos competentes y actuar en conformidad cuando una alerta pueda tener un impacto considerable en el desempeño de los sistemas informáticos.	TIC´S Talento Humano Secretaría General
COPIAS DE SEGURIDAD Toda información que pertenezca a la matriz de activos de información de LA ENTIDAD o que sea de interés para un proceso operativo o de misión crítica debe ser respaldada por copias de seguridad tomadas de acuerdo a los procedimientos documentados por el Comité de Seguridad de la Información. Dicho procedimiento debe incluir las actividades de almacenamiento de las copias en sitios seguros. Las dependencias de SOMOS deben realizar pruebas controladas para asegurar que las copias de seguridad pueden ser correctamente leídas y restauradas. Los registros de copias de seguridad deben ser guardados en una base de datos creada para tal fin. El área de Sistemas debe proveer las herramientas para que las dependencias puedan administrar la información y los registros de copias de seguridad. La Oficina de Control Interno debe efectuar auditorías aleatorias que permitan determinar el correcto funcionamiento de los procesos de copia de seguridad. Las copias de seguridad de información crítica deben ser mantenidas de acuerdo a cronogramas definidos y publicados por el área de Sistemas. La creación de copias de seguridad de archivos usados, custodiados o producidos por usuarios individuales es responsabilidad exclusiva de dichos	TIC´S Subgerente Técnico

usuarios. Los usuarios deben entregar al respectivo jefe, supervisor o coordinador de dependencia, las copias de seguridad para su registro y custodia.	
ADMINISTRACIÓN DE CONFIGURACIONES DE RED La configuración de enrutadores, switches, firewall, sistemas de detección de intrusos y otros dispositivos de seguridad de red; deben ser documentadas, respaldada por copia de seguridad y mantenida por el área de Sistemas. Todo equipo de TI debe ser revisado, registrado y aprobado por el área de Sistemas antes de conectarse a cualquier nodo de la Red de comunicaciones y datos de SOMOS. Dicha dependencia debe desconectar aquellos dispositivos que no estén aprobados y reportar tal conexión como un incidente de seguridad a ser investigado.	TIC´S Subgerente Técnico
INTERCAMBIO DE INFORMACIÓN CON ORGANIZACIONES EXTERNAS. Las peticiones de información por parte de entes externos de control deben ser aprobadas por LA ENTIDAD, y dirigida por dichos entes a los responsables de su custodia. Toda la información institucional debe ser manejada de acuerdo a la legislación. **INTERNET Y CORREO ELECTRÓNICO** Las normas de uso de Internet y de los servicios de correo electrónico serán elaboradas, mantenidas y actualizadas por el Comité de Seguridad de la Información y en todo caso este comité debe velar por el cumplimiento del código de ética institucional y el manejo responsable de los recursos de tecnologías de la información. **INSTALACIÓN DE SOFTWARE** Todas las instalaciones de software que se realicen sobre sistemas de SOMOS deben ser aprobadas por el área de Sistemas, de acuerdo a los procedimientos elaborados para tal fin por dichas dependencias. El Comité de Seguridad de la Información (Informática y Telecomunicaciones) definirá el ámbito en el cual actuará cada dependencia. No se permite la instalación de software que viole las leyes de propiedad intelectual y derechos de autor en especial la ley 23 de 1982 y relacionadas. El área de sistemas debe desinstalar cualquier software ilegal y registrar este hecho como un incidente de seguridad que debe ser investigado.	TIC´S Subgerente Técnico

Corresponde al área de Sistemas mantener una base de datos actualizada que contenga un inventario del software autorizado para su uso e instalación en los sistemas informáticos institucionales.	
CONTROL DE ACCESO **CATEGORÍAS DE ACCESO** El acceso a los recursos de tecnologías de información institucionales debe estar restringidos según los perfiles de usuario definidos por el Comité de Seguridad de la Información. **CONTROL DE CLAVES Y NOMBRES DE USUARIO** El acceso a información restringida debe estar controlado. Se recomienda el uso de sistemas automatizados de autenticación que manejen credenciales o firmas digitales. Corresponde al área de Sistemas elaborar, mantener y publicar los documentos de servicios de red que ofrece la institución a su personal, usuarios, y terceros. El área de Sistemas debe elaborar, mantener y publicar procedimientos de administración de cuentas de usuario para el uso de servicios de red. El acceso a sistemas de cómputo y los datos que contienen es responsabilidad exclusiva del personal encargado de tales sistemas. SOMOS debe propender por mantener al mínimo la cantidad de cuentas de usuario que el personal, los usuarios y los terceros deben poseer para acceder a los servicios de red. El control de las contraseñas de red y uso de equipos es responsabilidad del área de sistemas. Dichas contraseñas deben ser codificadas y almacenadas de forma segura. Las claves de administrador de los sistemas deben ser conservadas por el área de Sistemas y deben ser cambiadas en intervalos regulares de tiempo y en todo caso cuando el personal adscrito al cargo cambie. Se exceptúa de lo anterior las claves de administrador de servidores y equipos de escritorio adscritos al área de Sistemas o de SOMOS las cuales deben ser conservadas y deben ser cambiadas en intervalos regulares de tiempo y en todo caso cuando el personal adscrito al cargo cambie. El área de Sistemas debe elaborar, mantener y actualizar el procedimiento y las guías para la correcta definición, uso y complejidad de claves de usuario. Como requisito para la terminación de relación contractual - o laboral - del personal de SOMOS, el área de sistemas debe expedir un certificado de	TIC´S Subgerente Técnico

cancelación de las cuentas de usuario asignadas para el uso de recursos de tecnologías de la información de la institución. **COMPUTACIÓN MÓVIL** SOMOS reconoce el alto grado de exposición que presenta la información y los datos almacenados en dispositivos portátiles (computadores portátiles, notebooks, PDA, celulares, etc). Corresponde al área de Sistemas en conjunto con el área de Recursos Humanos y/o la secretaria general de SOMOS elaborar, mantener e implementar planes de capacitación que propendan por la formación y mantenimiento de la conciencia en cuestión de seguridad de la información. Las redes inalámbricas potencialmente introducen nuevos riesgos de seguridad que deben ser identificados, valorados y tratados de acuerdo a los lineamientos de la Política de Seguridad en redes inalámbricas que debe elaborar el Comité de Seguridad de la Información.	
AUDITORIA Y SEGUIMIENTO Todo uso que se haga de los recursos de tecnologías de la información en SOMOS debe ser seguidos y auditados de acuerdo con los lineamientos del Código de Ética y del Código de Uso de Recursos de Tecnologías de la Información, el cual debe ser elaborado por el Comité de Seguridad de la Información. **ACCESO REMOTO** El acceso remoto a servicios de red ofrecidos por SOMOS debe estar sujeto a medidas de control definidas por el área de sistemas, las cuales deben incluir acuerdos escritos de seguridad de la información. **ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS SOFTWARE** Para apoyar los procesos operativos y estratégicos, SOMOS debe hacer uso intensivo de las Tecnologías de la Información y las Comunicaciones. Los sistemas de software utilizados pueden ser adquiridos a través de terceras partes o desarrollados por personal propio. El área de Sistemas debe elegir, elaborar, mantener y difundir el “Método de Desarrollo de Sistemas Software en SOMOS que incluya lineamientos, procesos, buenas prácticas, plantillas y demás artefactos que sirvan para	TIC´S Subgerente Técnico

regular los desarrollos de software internos en un ambiente de mitigación del riesgo y aseguramiento de la calidad.

Todo proyecto de desarrollo de software interno debe contar con un documento de Identificación y Valoración de Riesgos del proyecto. SOMOS no debe emprender procesos de desarrollo o mantenimiento de sistemas software que tengan asociados riesgos altos no mitigados. Los sistemas software adquiridos a través de terceras partes deben certificar el cumplimiento de estándares de calidad en el proceso de desarrollo.

ADMINISTRACIÓN DE CONTINUIDAD DEL NEGOCIO

La Administración de Continuidad del Negocio debe ser parte integral del Plan de Administración de Riesgo de SOMOS.