**ARTÍCULO 6: DOMINIO ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN.**

**6.1 ORGANIZACIÓN INTERNA.**

**6.1.1 COMPROMISO DE LA DIRECCIÓN CON LA SEGURIDAD DE LA INFORMACIÓN.**

* La alta gerencia tiene la responsabilidad de respaldar activamente las iniciativas de seguridad brindando su claro apoyo y compromiso, asignando y aprobando explícitamente las responsabilidades del representante del SGSI

**6.1.2 COORDINACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.**

* Las actividades del SGSI deberían ser coordinadas por el Jefe de Sistemas (Ingeniero en Sistema o a fines) encargado del SGSI.

**6.1.3 ASIGNACIÓN DE RESPONSABILIDADES RELATIVAS A LA SEGURIDAD DE LA INFORMACIÓN.**

* La asignación de las responsabilidades se deben basar el organigrama estructural de la Empresa y deben se seleccionadas de acuerdo;
* A la relevancia en su puesto y funciones y de los distintos sectores que forman el Departamento de Sistemas. El representante del SGSI y dos Analistas de Sistemas son los encargados de las comunicaciones, desarrollo, administración y mantenimiento de los Sistemas Informáticos según la coordinación del Jefe Departamental.

**6.1.4 PROCESO DE AUTORIZACIÓN DE RECURSOS PARA EL TRATAMIENTO DE LA INFORMACIÓN.**

* Se debe definir y establecer un proceso de gestión de autorizaciones para los nuevos recursos de tratamiento de la información.
* La autorización de los recursos es tarea designada al jefe de Sistema, previo un aval técnico.

**6.1.5 ACUERDOS DE CONFIDENCIALIDAD.**

* El proceso de acuerdos de confidencialidad es llevado a cabo por el representante del Sistema de Gestión Integrado; el cual es responsable de elaborar, mantener y actualizar los instructivos correspondientes, que serán el modelo base para la aplicación del talento humano con resolución de la alta gerencia como política integrada en cada una de sus versiones.
* Los convenios de confidencialidad son aplicables a todo el personal que conformen el sistema de información, que tenga acceso a esta y es de propiedad de la empresa.

**6.1.6 CONTACTO DE AUTORIDADES.**

* En caso de incidentes al SGSI relacionado con los medios de telecomunicaciones, al violarse control establecido para la mitigación del suceso; es labor del Departamento de Sistemas mediante comunicado informar la Super Intendencia de Telecomunicaciones el acontecimiento como único organismo en el Ecuador encargado de garantizar la Seguridad en las Telecomunicaciones (SUPERTEL).

**6.1.7 CONTACTO CON GRUPOS DE ESPECIAL INTERÉS.**

* Se debe crear y mantener un listado de relaciones externas: autoridades regulatorias, organismos de comunicación y denuncia de incidentes de seguridad en Ecuador.

**6.1.8 REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN.**

* Se deben revisar el cumplimiento del SGSI, objetivos de control, políticas, procesos y procedimientos de seguridad de forma independiente y a intervalos planificados o cuando se produzcan cambios significativos para la seguridad de la información en la Empresa.

**6.2 TERCEROS.**

**6.2.1 IDENTIFICACIÓN DE LOS RIESGOS DERIVADOS DEL ACCESO DE TERCEROS.**

* En caso de acceso por Terceros a los Sistemas de Información, se deben identificar los riesgos y a las instalaciones del procesamiento de información de los procesos de negocio que impliquen y se deben implementar controles apropiados antes de conceder el permiso.

**6.2.2 TRATAMIENTO DE LA SEGURIDAD EN LA RELACIÓN CON LOS CLIENTES.**

* Se deben mantener anexados todos los requisitos reconocidos de seguridad antes de dar a los clientes acceso a los activos de la Información.

**6.2.3 TRATAMIENTO DE LA SEGURIDAD EN CONTRATOS CON TERCEROS.**

* Para acuerdos con terceras partes que implican el acceso, proceso, comunicación o gestión de la información de la organización o de las instalaciones de procesamiento de información o la adición de productos o servicios a las instalaciones, deberían cubrir todos los requisitos de seguridad relevante.