1. OBJETIVO.

Controlar y gestionar la seguridad de los sistemas de información de colviseg Ltda, garantizando la continuidad de los servicios, el respaldo de la información y la protección de la información.

2. CAMPO DE APLICACIÓN

Todos los sistemas de información de colviseg ltda.

3. RESPONSABLES.

Dirige : Jefe de Sistemas

Ejecuta : personal administrativo y operativo de colviseg ltda

Verifica : Jefe SIG, Auditores Internos.

4. POLÍTICA DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

POLÍTICA

La política de uso aceptable pretende facilitar y agilizar los procesos y mejorar la calidad en la prestación de servicios a los usuarios.

La mejora de los procesos en los Sistemas de Información supone regular el uso apropiado de sus componentes y equipos, así como implantación de aquellas medidas necesarias para garantizar la confidencialidad de la información.

Para conseguir estos objetivos resulta necesario establecer políticas que garanticen el uso efectivo y seguro de los Sistemas de Información y las herramientas asociadas a estos. Este documento tiene como objetivo fijar las normas fundamentales que deben regir el comportamiento de los empleados para garantizar el uso adecuado de estos recursos

Normas generales aplicables al uso de los Sistemas de Información

I. Los sistemas de información de COLVISEG LTDA, incluyendo los programas, aplicaciones y archivos electrónicos, pertenecen a COLVISEG LTDA, y sólo pueden utilizarse para fines relacionados con el desempeño de las tareas que los usuarios tengan encomendadas.

Esta misma consideración se aplica a la información almacenada en su ordenador o la emitida o comunicada a través de los Sistemas de Información de COLVISEG LTDA.

II. Los sistemas de información y las herramientas asociadas, como el correo electrónico y la conexión a Internet, sólo podrán ser utilizados por personal debidamente autorizado.

Será responsabilidad de cada área definir las tareas que conllevan acceso a tales herramientas. El uso de tales recursos deberá circunscribirse al ámbito profesional con el propósito de agilizar los trabajos de COLVISEG LTDA. No se autoriza su uso con fines personales.

La información desarrollada, transmitida o almacenada en los Sistemas de Información de COLVISEG LTDA pertenece a COLVISEG LTDA. Son de aplicación todas las disposiciones legales aplicables a los documentos privados. La divulgación de tal información sin autorización está estrictamente prohibida. La alteración, destrucción o distribución fraudulenta o malintencionada de cualquier documento en formato electrónico propiedad de COLVISEG LTDA puede perjudicar gravemente a la empresa y constituir una infracción grave; en tal caso se adoptarán las medidas disciplinarias previstas en el reglamento interno de trabajo, reservándose el derecho a interponer cuantas acciones legales sean necesarias.

III. No está permitido la creación de carpetas y/o archivos con datos personales sin la conformidad por escrito del Departamento de Sistemas, quien solicitará autorización a los dueños de procesos, con objeto de adoptar las medidas necesarias para asegurar la legalidad y seguridad del tratamiento de la información personal.

(*)Por datos personales se entiende toda información que identifique a personas físicas, por ejemplo: fotografías, nombre y apellidos, dirección, teléfono, correo electrónico, estado civil, sexo.

IV. Los usuarios de los sistemas de información deben respetar los derechos de propiedad intelectual de los autores de las obras, programas, aplicaciones u otros, manejadas o accedidas a través de dicho sistema.

V. Los programas y recursos utilizados en COLVISEG LTDA deben tener su correspondiente licencia en vigor o autorización de uso explícita para poder ser utilizados. Dichos programas sólo podrán ser instalados por personal autorizado a tales efectos. Además, no deberán instalarse programas sin la previa autorización del departamento de Sistemas, incluso cuando se trate de programas sin coste.

VI. Los programas y aplicaciones distribuidos por COLVISEG LTDA no podrán reproducirse sin autorización o ser utilizados para fines ajenos a las funciones y tareas encomendadas por COLVISEG LTDA.

VII. COLVISEG LTDA, será responsable de establecer las normas mediante las cuales se asignan las cuentas de acceso, incluyendo las medidas de seguridad aplicables tales como: claves secretas, contraseñas, controles de acceso a los servidores y sistemas para auditar su uso, la integridad y la seguridad de los datos y comunicaciones que se envían.

5. IDENTIFICACIÓN DE ABUSO DE LOS SISTEMAS INFORMÁTICOS.

CLASE	MÉTODO DE IDENTIFICACIÓN	MEDIDA DE CONTROL
Acceso no autorizado	Bloqueo de usuarios después de cierta cantidad de intentos de ingreso fallidos	Asignación de perfiles de usuario por equipo y por sistema de información
Manipulación indebida o alteración de la información	Auditorias de sistemas	Archivos estadísticos e informes a la dirección administrativa
Eliminación de información sin autorización	Registro de logs dentro de equipos	Realización de copias de seguridad y auditorias periódicas a los sistemas de información
Ataques por virus	Reportes del software de antivirus	Antivirus institucional administrado
Ataques externos a los sistemas de información y redes.	Reportes de firewall	Firewall institucional administrado
Suplantación	Auditorias de sistemas	Cambios recurrentes de claves
Sustracción de la información	Auditorias de sistemas	Registros de logs
Trafico de archivos pesados a través de la red y de correos electrónicos	Monitoreo de red	Restricción de ancho de banda de los usuarios
Mal uso de las herramientas tecnológicas	Mantenimientos preventivos	capacitaciones
Movilizaciones de equipos de computo sin autorización	Auditorias de sistemas	capacitación

Toda otra clase de ataque o daño a los sistemas de información se gestionaran directamente por el jefe de sistemas quien en la administración diaria de conexiones, servidores, sistemas de información, equipos de respaldo y auditorias periódicas identificara y mantendrá controlado y gestionara que el impacto de los ataques sea el mínimo y mantendrá disponible los servicios de TI.

6. Gestión de seguridad con los contratistas de Tecnologías de información.

- Todos los servicios que se realicen a través de contratistas deben estar debidamente autorizados por el jefe de sistemas a nivel nacional.
- Se restringirán y mantendrán controlados todos los permisos y autorizaciones de acceso mientras se ejecuten los servicios de los contratistas
- Antes de la realización de tareas de los contratistas se realizaran copias de seguridad y respaldo.
- Las actividades de mantenimiento con contratistas en los que se tenga que bajar los servicios preferiblemente se realizaran en horarios fuera de oficina que no afecte la operación normal.
- Para los servicios con contratistas preferiblemente se deben realizar pruebas antes de su implementación en un ambiente de pruebas para minimizar el impacto en la operación en el momento de la puesta en producción.
- Todas las relaciones contractuales con contratistas de servicios de tecnología de información debe ser bajo términos de confidencialidad.

7. HISTORIA DE LAS REVISIONES

HISTORIA DE LAS REVISIONES			
Versión	Descripción del cambio	Aprobado	Fecha

ELABORÓ	REVISÓ	APROBÓ
Jefe de Sistemas	Jefe de Sistemas Integrales de Gestión	Gerente General