## 1. INTRODUCCION

Para la Compañía es estratégico, Asegurar el proceso de "Gestión De Informática Y Tecnología", con el objetivo de "Alcanzar excelencia operacional y optimizar los procesos y la productividad de la Organización.

Por lo anterior y como apoyo al logro de este objetivo, hemos adoptado las mejores prácticas contenidas en la Norma de Seguridad de la Información, creando nuestra propia Política de Seguridad de la información, en el presente documento.

La información es un recurso que, como el resto de los activos, tiene valor para la organización y por consiguiente debe ser debidamente protegida, garantizando la continuidad de los sistemas de información, minimizando los riesgos de daño y contribuyendo de esta manera, a una mejor gestión de la Compañía.
Para que los principios de la Política de Seguridad de la Información sean efectivos, se implementa La Política de Seguridad de la Información buscando que forme parte de la cultura organizacional de la Compañía, lo que implica que debe contarse con el manifiesto compromiso de todos(as) los(as) colaboradores(as) de una manera u otra vinculados a la gestión, para contribuir a la difusión, consolidación y cumplimiento.

## 2. DEFINICIONES

**2.1.** La seguridad de la información se entiende como la preservación de las siguientes características:

- **Confidencialidad**: Se garantiza que la información no esté disponible o se revele a personas no autorizadas.
- **Integridad**: Cuando la información es exacta y completa.
- **Disponibilidad:** Cuando la información es accesible y utilizable a los usuarios autorizados.

Adicional, se debe considerar los siguientes aspectos que la complementan:

- **Autenticidad**: Cuando se garantiza la identidad de quien solicita acceso a la información.
- **No repudio**: Es la forma de evitar que quien envió o recibió información alegue que no lo realizó ante terceros.
- **Legalidad**: Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta la Compañía.
- **Confiabilidad:** La información generada es la adecuada para la toma de decisiones.
- **Información**: se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, graficas, cartográficas, narrativas o audiovisuales y en cualquier medio, ya sea magnético, en papel, en computadoras, audiovisual u otro medio.
- **Sistema de Información**: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procesamientos, tanto automatizados como manuales.

**2.2.** **Activo:** Cualquier cosa que tenga valor para la compañía. (NTC 5411-1:2006)

**2.3.** **Control**: Medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la Compañía que pueden ser de naturaleza administrativa, técnica de gestión o legal. También se usa como sinónimo de salvaguarda o contramedida.

**2.4.** **Directriz:** Descripción que aclara lo que se debería hacer y cómo hacerlo, para alcanzar los objetivos establecidos en las políticas. (NTC 5411-1:2006)

**2.5.** **Servicios de procesamiento de Información**: Cualquier servicio, infraestructura o sistema de procesamiento de información o los sitios físicos que lo albergan.

**2.6.** **Evento de Seguridad de la Información**: Es la presencia identificada de un estado del sistema, del servicio o de la red que indica un posible incumplimiento de la política de seguridad de la información. Una falla de controles, o una situación previamente desconocida que puede ser pertinente para la seguridad. (ISO/IEC TR 18044:2000)

**2.7.** **Incidente de Seguridad de la información:** Está indicado por un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. (ISO/IEC TR 18044:2000)

**2.8.** **Política**: Toda intención y directriz expresada formalmente por la Compañía

**2.9.** **Riesgo**: Combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC Guía 73:2002)

**2.10.** **Amenaza:** Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema o a la Compañía. (NTC 5411-1:2006)

**2.11.** **Vulnerabilidad**: Debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas. (NTC 5411-1:2006)

## 3. MARCO REGULATORIO

Para los propósitos de este documento se considera la legislación vigente en informática y proyectos de ley en Colombia:

**LEY 603 DEL 2000**

Esta ley se refiere a la protección de los derechos de autor en Colombia. Recuerde que el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.

**LEY ESTATUTARIA 1266 DEL 31 DE DICIEMBRE DE 2008**

Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

**LEY 1273 DEL 5 DE ENERO DE 2009**

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

**LEY 1341 DEL 30 DE JULIO DE 2009**

Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

**LEY ESTATUTARIA 1581 DE 2012**

Entró en vigencia la Ley 1581 del 17 de octubre 2012 de **PROTECCIÓN DE DATOS PERSONALES**, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional.

Como resultado de la sanción de la anunciada ley, toda entidad pública o privada, cuenta con un plazo de seis meses para crear sus propias políticas internas de manejo de datos personales, establecer procedimientos adecuados para la atención de peticiones, quejas y reclamos, así como ajustar todos los procesos, contratos y autorizaciones a las disposiciones de la nueva norma.

**Aspectos claves de la normatividad**:
Cualquier ciudadano tendrá la posibilidad de acceder a su información personal y solicitar la supresión o corrección de la misma frente a toda base de datos en que se encuentre registrado.

Establece los principios que deben ser obligatoriamente observados por quienes hagan uso o de alguna manera realicen el tratamiento o mantengan una base de datos con información personal, cualquiera que sea su finalidad.

Aclara la diferencia entre clases de datos personales construyendo las bases para la instauración de los diversos grados de protección que deben presentar si son públicos o privados, así como las finalidades permitidas para su utilización.

Crea una especial protección a los datos de menores de edad.
Establece los lineamientos para la cesión de datos entre entidades y los procesos de importación y exportación de información personal que se realicen en adelante.

Define las obligaciones y responsabilidades que empresas de servicios tercerizados tales como Call y Contact Center, entidades de cobranza y, en general, todos aquellos que manejen datos personales por cuenta de un tercero, deben cumplir en adelante.

Asigna la vigilancia y control de las bases de datos personales a la ya creada Superintendencia Delegada para la Protección de Datos Personales, de la Superintendencia de Industria y Comercio.

Crea el Registro Nacional de Bases de Datos.

Establece una serie de sanciones de carácter personal e institucional dirigidas a entidades y funcionarios responsables del cumplimiento de sus lineamientos.

DECRETO 1377 DE 2013
Protección de Datos, decreto por el cual se reglamenta parcialmente la Ley 1581 de 2012.

## 4. LÍNEA BASE DE LA POLÍTICA GENERAL DE LA SEGURIDAD DE LA INFORMACIÓN

### 4.1. OBJETIVO

Proteger los recursos de información de la Organización y la tecnología, utilizada para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.
Asegurar la implementación de las medidas de seguridad comprendidas en esta Política, identificando los recursos y las partidas presupuestarias correspondientes, sin que ello implique necesariamente la asignación de partidas adicionales.
Mantener la Política de Seguridad de la Organización actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

## 4.2. ALCANCE

La presente Política de Seguridad de la Información se dicta en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico de la Organización.

La Política de Confidencialidad de la Información de la Compañía, establece los diferentes tipos de información que se maneja, el uso aceptable que debe hacerse de esta información, los principios de retención y divulgación de los datos confidenciales, los deberes de la Compañía y los derechos de los(as) colaboradores(as) y Contratistas y las medidas de seguridad adoptadas para garantizar la protección de esta información.

## 4.3. CUMPLIMIENTO

El cumplimiento de todas las leyes, regulaciones, estándares profesionales, políticas aplicables, la presente política y todos los contratos, es responsabilidad de los(as) colaboradores(as) de la Compañía, de los contratistas y de los Terceros.

## 4.4. EXCEPCIONES

En caso de existir situaciones en algún área de la Compañía que impidan cumplir con la política de forma parcial o total, debe el responsable del cumplimiento, exponerlo ante el Comité de Seguridad Informática, argumentando las razones; dicho Comité tiene la facultad de aprobar o no la solicitud y debe dejar la evidencia y documentarla para posterior revisión.

## 4.5. APLICABILIDAD

La Política de Seguridad de la Información de la Compañía, aplica a todo el personal vinculado laboralmente, contratistas y terceros que tengan acceso a los recursos de su información. Estas políticas deben ser compartidas, entendidas y acatadas por los anteriormente mencionados, siendo deber de éstos, expresar sus dudas oportunamente y de buena fe a los funcionarios administradores de la información.
Cabe anotar que su aplicación y cumplimiento es de carácter obligatorio para todo el personal de la Compañía, cualquiera que sea la situación que revista, el área a la cual se encuentre afectado y cualquiera sea el nivel de las tareas que desempeñe.

## 4.6. RESPONSABILIDAD

### 4.6.1. Directivos de la Compañía

- Implementar la Política de Seguridad de la Información dentro de sus áreas y velar por su cumplimiento por parte de su equipo de trabajo.

### 4.6.2. Comité de Seguridad de la Información

- El Comité representa el compromiso de la Gerencia General con la Seguridad de la Información y es el canal entre ésta y los(as) colaboradores(as).
- Revisar y proponer a la máxima autoridad de la Compañía para su aprobación, la Política de Seguridad de la Información y las funciones generales en materia de seguridad de la información.
- Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
- Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.
- Garantizar que la seguridad de la información sea parte del proceso de planificación de la Organización.
- Promover la difusión y apoyo a la seguridad de la información dentro de la Organización.

- Coordinar el proceso de administración de la continuidad de las actividades de la Organización.

#### 4.6.3. Coordinador del Comité de Seguridad de la Información

- Coordinar las acciones del Comité de Seguridad de la Información.
- Impulsar la implementación y cumplimiento de la presente Política.
- Mantener la Política de Seguridad actualizada, a efectos de asegurar su vigencia y nivel de eficacia.
- Coordinar la logística correspondiente a las sesiones del comité de seguridad de la información.
- Recepcionar, revisar, preparar y presentar ante el comité de seguridad de la información las propuestas que requieran ser aprobadas.

#### 4.6.4. Responsable de Seguridad Informática

- Cumplir funciones relativas a la seguridad de los sistemas de información de la Organización, lo cual incluye la supervisión de todos los aspectos inherentes a los temas tratados en la presente Política.

#### 4.6.5. Propietarios de la Información

- Clasificar la información de acuerdo con el grado de sensibilidad y criticidad de la misma.
- Documentar y mantener actualizada la clasificación efectuada
- Definir los criterios de acceso a la información de acuerdo a sus funciones y competencia para sus colaboradores(as).
- Asegurar que los controles de alto nivel para proteger la información sean implementados.
- Tomar las acciones definidas en las políticas, código de ética y cualquier otro reglamento o control, frente a violaciones de la seguridad.

#### 4.6.6. Responsable del Área de Talento Humano

- Notificar al personal que ingresa a la Compañía, sus obligaciones respecto al cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan.
- Socializar a toda la compañía los cambios que se realicen en la política de seguridad de la información, la implementación de la suscripción de los Compromisos de Confidencialidad (entre otros) y las tareas de capacitación permanente en materia de seguridad.
- incluir las funciones relativas a la seguridad de la información en la descripción de puestos de los(as) colaboradores(as).

#### 4.6.7. Responsable del Área Informática

- Cumplir la función de cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología de la Organización.
- Efectuar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida de sistemas apropiada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases.

#### 4.6.8. Usuarios de la información y los Sistemas utilizados para su procesamiento

Los usuarios incluyen a todo el personal vinculado laboralmente con la Organización, contratistas y terceros cuyas labores diarias comprenden el procesamiento, resguardo o transmisión de la información privada, confidencial, interna o pública de la Compañía.

- Conocer, dar a conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigente.
- Aceptar, comprender y aplicar las políticas, estándares y controles técnicos de seguridad de la información de la Organización.
- Usar la información y recursos de forma ética y responsable, para los propósitos autorizados únicamente.

#### 4.6.9. Unidad de Auditoría Interna

Quien sea propuesto por el Comité de Seguridad de la Información es responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la tecnología de información, debiendo 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.

#### 4.6.10. Custodios de la Información

- Implementar (a nivel técnico) los controles requeridos para proteger los activos de información, con base en el nivel de clasificación asignado por el administrador correspondiente.
- Proporcionar asistencia en la selección de soluciones técnicas apropiadas.
- Proveer operativamente el aseguramiento de la información.

#### 4.6.11. Asesor de Seguridad de la Información REDI

- Asesorar a la Compañía en Seguridad de la información:
    - Dar los lineamientos relacionados a la seguridad de la información sujetos a las mejores prácticas.
    - Diseñar y adaptar políticas enfocadas en las mejores prácticas de la seguridad de la información.
    - Asesorar en el diseño y preparación de los planes de trabajo como respuesta a las recomendaciones planteadas por las auditorías a la Compañía.
    - Realizar periódicamente monitoreos que permitan diagnosticar el estado de seguridad de la información.

## 5. POLITICA GENERAL DE LA SEGURIDAD DE LA INFORMACION

Surtigas consiente de la importancia que tiene la información para el desarrollo de sus procesos, los cuales son de obligatorio cumplimiento por colaboradores(as), proveedores, y contratistas que están encaminadas a proteger los recursos de información y tecnología utilizadas para su procesamiento, frente amenazas internas o externas implementa los mecanismos necesario para garantizar la confidencialidad, integridad y disponibilidad de la información

Para dar cumplimiento a esta política general, se establecen los siguientes objetivos de control:

- Los propietarios de la información, deben identificar y clasificar los Activos de información de la Compañía para establecer los mecanismos de protección necesarios.
- La Compañía define e implanta controles para proteger la información contra violaciones de autenticidad, accesos no autorizados, perdida de integridad y que garanticen la disponibilidad requerida por los clientes y usuarios de los servicios ofrecidos.
- Todos los(as) colaboradores(as) y contratistas, deben ser responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.
- Se deben realizar auditorías y controles periódicos sobre la gestión de Seguridad de la Información de la Compañía.

- La Compañía autoriza el uso de software adquirido legalmente.
- Es responsabilidad de todos(as) los(as) colaboradores(as) y contratistas de la Compañía, reportar los Incidentes de Seguridad, eventos sospechosos y el mal uso de los recursos que identifique.
- Las violaciones a las Políticas y Controles de Seguridad de la Información deben ser reportadas, registradas y monitoreadas.
- La Compañía debe contar con un Plan de Continuidad del Negocio que asegure la continuidad de las operaciones, ante la ocurrencia de eventos no previstos o desastres naturales.
- Adicionalmente la Compañía cuenta con políticas específicas y un conjunto de estándares y procedimientos que soportan la política corporativa.

### 5.1. Sistema de Gestión de la Seguridad de la Información

La Compañía, debe tener un modelo para administrar la Seguridad de la información, enfocado en las mejores prácticas y al cumplimiento a regulaciones internas y externas.

### 5.2. Capacitación y Concientización

La Compañía, debe llevar a cabo un programa anual de sensibilización y capacitación a los(as) colaboradores(as) sobre Seguridad de la Información, con el fin de que ésta sea parte integral de nuestra cultura Organizacional.

### 5.3. Organización de seguridad (D6-NORMA ISO 27002)

El Comité de Seguridad de la Información, debe diseñar e implementar las mejores prácticas y estándares de seguridad de la información, las cuales se deben socializar a través de procedimientos y campañas, asegurando el cumplimiento de su confidencialidad, integridad, disponibilidad y confiabilidad.

### 5.4. Seguridad de los Recursos Humanos (D7- NORMA ISO 27002)

La Compañía, debe establecer compromisos de confidencialidad con todos(as) los(as) colaboradores(as) y usuarios externos que tengan la posibilidad de acceder a nuestra información e infraestructura para su procesamiento, así como las herramientas y mecanismos para garantizar que los usuarios se encuentren capacitados para respaldar la Política de Seguridad de la Compañía, con el fin de reducir los riesgos de error humano, uso inadecuado de las instalaciones y recursos, y manejo no autorizado de la información.

### 5.5. Clasificación y control de activos-Gestión de Activos (D8- NORMA ISO 27002)

El área de informática, como custodio y responsable de la protección de los Activos de Información de la Compañía, debe diseñar y establecer los mecanismos que le permitan proteger su confidencialidad, integridad y disponibilidad, de tal manera que garantice que sus usuarios sean conscientes de su responsabilidad y protección.

### 5.6. Control de accesos (D9- NORMA ISO 27002)

Los responsables de la administración de la infraestructura tecnológica de nuestra Compañía, debe asignar los accesos a plataformas, usuarios y segmentos de red, de acuerdo a procesos formales de autorización, los cuales deben ser revisados de manera periódica, con el fin de evitar el acceso de usuarios no autorizados a los sistemas de información.

### 5.7. Criptografía (D10- NORMA ISO 27002)

El área de informática de Surtigas, debe implementar controles criptográficos que les permitan a los usuarios asegurar y proteger la confidencialidad, la autenticidad y la integridad de la información del negocio.

### 5.8. Seguridad física y del Entorno (D11- NORMA ISO 27002)

La Compañía debe contar con mecanismos y procedimientos de seguridad operacionales, para controlar el acceso a todas las áreas destinadas al procesamiento y/o almacenamiento de información sensible o crítica, así como aquellas en las que se encuentran los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, con el fin de proteger la información, el software y el hardware de daños intencionales o accidentales y evitar el acceso no autorizado. (Referencia: Manual de operaciones)

### 5.9. Seguridad de las Operaciones (D12- NORMA ISO 27002)

La Compañía, debe establecer los mecanismos que aseguren la operación correcta y segura del procesamiento de la información y comunicaciones, y la operación adecuada de su infraestructura tecnológica, a través de políticas, normas, procedimientos e instructivos de trabajo, debidamente actualizados y socializados.

### 5.10. Seguridad de las Comunicaciones (D13- NORMA ISO 27002)

La Compañía debe establecer los mecanismos que aseguren la protección y la confidencialidad e integridad de la información en las redes y los servicios relacionados contra acceso no autorizado, a través de procedimientos, documentos políticas y controles.

### 5.11. Adquisición, Desarrollo y Mantenimiento de Sistemas de información (D14- NORMA ISO 27002)

La Compañía debe contar con procedimientos que contengan los requisitos para los controles de seguridad en la adquisición de nuevos sistemas de información o en las mejoras a los existentes; proteger la confidencialidad, autenticidad o integridad de la información.

### 5.12. Relaciones con Proveedores (D15- NORMA ISO 27002)

La Compañía debe, implementar controles a los proveedores que gestionan información para asegurar la protección de los activos de la organización. Como también se debe establecer y acordar todos los requisitos, riesgos y niveles acordado de seguridad de la información pertinente, con cada proveedor.

### 5.13. Gestión de Incidentes de Seguridad de la información (D16- NORMA ISO 27002)

La Compañía debe establecer los mecanismos para que los(as) colaboradores(as), contratista y usuarios de terceras partes, tomen conciencia de su responsabilidad de reportar los eventos y debilidades de seguridad de la información, asociados con los sistemas de información, inmediatamente sucedan, con el fin de tomar las medidas necesarias para responder a tales incidentes y establecer las medidas necesarias para evitarlos en el futuro.

### 5.14. Plan de continuidad del negocio (D17- NORMA ISO 27002)

La Compañía, debe implementar un proceso de gestión para la continuidad del negocio, mediante controles preventivos y acciones de recuperación según la evaluación de riesgos, el cual contenga los requisitos de seguridad de la información necesarios, con el fin de atender la recuperación por la pérdida de los activos de información, causados por desastres naturales, accidentes, fallas o acciones deliberadas u otros hechos.

### 5.15. Cumplimiento de Políticas y normatividad legal (D18- NORMA ISO 27002)

La Compañía, debe implementar procedimientos y establecer controles para asegurar el cumplimiento de las normas y políticas de seguridad internas, requisitos estatutarios, reglamentarios y contractuales pertinentes para cada sistema de información. Todas las áreas que cumplan reglamentaciones, deben estar procedimentadas las leyes que se relacionan.

### 5.16. PROTECCION DE DATOS PERSONALES

Surtigas ha establecido procedimientos para el uso, protección y transferencia adecuado de los datos personales dando cumplimiento a la Ley 1581 de Protección de Datos Personales de Octubre del año 2012.

## 6. DOCUMENTOS DE REFERENCIA Y ANEXOS

Los siguientes documentos sirven de soporte para ampliar y completar la comprensión de esta política.

- Ley Habeas Data (1266)
- Ley 1581 de protección de datos personales
- NTC-ISO/IEC 27001
- N-929-8 Política de Tratamiento de Datos Personales



En la herramienta kawak aparecen los(as) colaboradores(as) que participaron en la revisión y aprobación del documento, los cuales hacen constar que recibieron documentación e información previa para tal efecto y que el documento está adecuado a las actividades y prácticas de la organización.

**Anexo A**

| REGISTRO DE CAMBIOS AL DOCUMENTO | | | | | |
|---|---|---|---|---|---|
| **FECHA** | **VERSION** | **PAGINA** | **SECCION** | **CAMBIOS EFECTUADOS** | **INCORPORO** |
| 27/oct/2015 | 1 | N.A. | N.A. | Se creó documento según solicitud con Id. 4082 | Cristian Salazar |
| 01/ago/2017 | 2 | Todas | Todas | Se revisa el documento y se agrega lenguaje de equidad de género. Se cambia versión y fecha de vigencia según solicitud con Id. 5903 | Cristian Salazar |