**Grapas y Puntillas EL CABALLO S.A.**

La información contenida en este documento es propiedad Grapas y Puntillas EL CABALLO S.A., por lo tanto, no podrá ser reproducida, mostrada o divulgada fuera de Grapas y Puntillas EL CABALLO S.A., sin el correspondiente permiso escrito. Esta información es altamente sensible y de naturaleza competitiva.

Grapas y Puntillas EL CABALLO S.A., no asume ninguna responsabilidad financiera o de otro tipo que pueda ser el resultado del uso de la información contenida en este documento, incluyendo, pero no limitada a perjuicios directos, indirectos, especiales o consecuenciales.

Usted debe tener mucho cuidado de asegurar el uso de esta información conforme a las leyes, reglas, y regulaciones de la o las jurisdicciones con respecto a las cuales se utiliza. La información aquí contenida está sujeta a cambios sin previo aviso. Las revisiones se pueden publicar para notificar tales cambios y/o adiciones.

**Tabla de Contenido**

[INTRODUCCION](#_heading=h.30j0zll)

[OBJETIVO 5](#_heading=h.30j0zll)

[PRELIMINAR 7](#_heading=h.1fob9te)

[DEFINICIONES 8](#_heading=h.3znysh7)

[POLITICA 1: SEGURIDAD DE LA INFORMACIÓN 22](#_heading=h.2et92p0)

[POLITICA 2: ADMINISTRACIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFROMACIÓN 23](#_heading=h.2bn6wsx)

[POLITICA 3: DISPOTIVOS MOVILES 24](#_heading=h.3as4poj)

[POLITICA 4: ACCESO A LA INFORMACIÓN 25](#_heading=h.3as4poj)

[POLITICA 5: ADMINISTRACION DE CAMBIOS 26](#_heading=h.1pxezwc)

[POLITICA 6: SEGURIDAD PARA LOS SERVICIOS INFORMATICOS 27](#_heading=h.49x2ik5)

[POLITICA 7: SEGURIDAD EN RECURSOS INFORMATICOS 28](#_heading=h.2p2csry)

[POLITICA 8: SEGURIDAD EN COMUNICACIONES 30](#_heading=h.147n2zr)

[POLITICA 9: SEGURIDAD PARA LOS USUSARIOS TERCEROS 30](#_heading=h.3o7alnk)

[POLITICA 10: SOFTWARE UTILIZADO 31](#_heading=h.23ckvvd)

[POLITICA 11: ACCESO WEB 32](#_heading=h.ihv636)

[POLITICA 12: ACTUALIZACION DE HARDWARE 34](#_heading=h.32hioqz)

[POLITCA 13: ALMACENAMIENTO Y RESPALDO 35](#_heading=h.1hmsyys)

[POLITICA 14: CONTINGENCIA 35](#_heading=h.41mghml)

[POLITICA 15: AUDITORIA 35](#_heading=h.2grqrue)

[POLITICA 16: SEGURIDAD FISICA 36](#_heading=h.vx1227)

POLITICA 17: ESCRITORIOS LIMPIOS 38

POLITICA 18: ADMINISTRACION DE LA SEGURIDAD 38

POLITICA 19: MEDIOS EXTRAIBLES 39

[SANCIONES 40](#_heading=h.3fwokq0)

[NOTAS 41](#_heading=h.1v1yuxt)

**INTRODUCCION:**

La información para Grapas y Puntillas EL CABALLO S.A., es un recurso que, como el resto de los activos, tiene valor para la organización y por consiguiente debe ser debidamente protegida.

Las Políticas de Seguridad de la Información protegen a la compañía de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos.

Es importante que los principios de la Política de Seguridad sean parte de la cultura organizacional y para esto se asegura un compromiso manifiesto de la Dirección de Grapas y Puntillas EL CABALLO S.A., y de Direcciones Corporativas para la difusión, consolidación y cumplimiento de la presente política.

# OBJETIVO

1. Proteger los activos de información de la compañía y la infraestructura tecnológica 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, de la información y los procesos de negocio.
2. Mantener la clasificación de la información de acuerdo al nivel de confidencialidad que establezca cada una de las direcciones.
3. Mantener el manual de Seguridad de la información de la compañía actualizado, a efectos de asegurar su vigencia y nivel de eficacia.
4. Generar un ambiente de trabajo y cultura organizacional que refleje la importancia de la administración de la información.
5. Proteger la información contra cualquier acceso no autorizado, garantizando los requisitos legales y reglamentarios exigidos por la compañía en protección a la información.

# ALCANCE

Este Manual se aplica en todo el ámbito de la compañía, a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la organización a través de contratos o acuerdos con terceros.

El cumplimiento del Manual de Seguridad de la Información es obligatorio.

Todos los directores son directamente responsables de la aplicación del manual y asegurar el cumplimiento en sus respectivas áreas.

Además, se encuentra a disposición del público que lo solicite y es revisado cuando así se estime necesario.



**Cristian Garcia**  **Jose Bernardo Coronado**

**Director de Sistemas** **Gerente General**

Fecha: Julio 31 de 2024

# PRELIMINAR

La Dirección de Sistemas gestiona todo lo relacionado con la Informática, la Infraestructura y la Coordinación de mesa de ayuda en Grapas y Puntillas EL CABALLO S.A., basándose en el esquema ITIL (Information Technology Infrastructure Library) se encargan de brindar servicio directo al usuario, por el ámbito de competencia que tiene cada uno de las líneas en materia de informática, desde el suministro de equipos, instalación, alteración, cambio de lugar, programación.

Por lo que ha sido necesario emitir políticas particulares para la red de Grapas y Puntillas EL CABALLO S.A., que es el nombre oficial de un conjunto de recursos y facilidades informáticas, de la infraestructura de telecomunicaciones y servicios asociados a ellos, provistos por la Dirección de sistemas.

De esta manera, las políticas de seguridad en informática de Grapas y Puntillas EL CABALLO S.A., emergen como el instrumento para concientizar a sus miembros acerca de la importancia y sensibilidad de la información y servicios críticos, de la superación de las fallas y de las debilidades, de tal forma que permiten a la empresa cumplir con su misión.

El proponer esta política de seguridad requiere un alto compromiso con la empresa, agudeza técnica para establecer fallas y deficiencias, constancia para renovar y actualizar dicha política en función del ambiente dinámico que nos rodea.

# TERMINOS Y DEFINICIONES

## TERMINOS

Entiéndase para el presente documento los siguientes términos:

**Política**: Son instrucciones mandatarias que indican la intención de la alta gerencia respecto a la operación de la organización.

**Recurso Informático**: Elementos informáticos (base de datos, sistemas operacionales, redes, sistemas de información y comunicaciones) que facilitan servicios informáticos.

**Información**: Puede existir en muchas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, presentada en imágenes, o expuesta en una conversación. Cualquiera sea la forma que adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada.

**Usuarios Terceros**: Todas aquellas personas naturales o jurídicas, que no son empleados de Grapas y Puntillas EL CABALLO S.A., pero que por las actividades que realizan en la compañía, deban tener acceso a Recursos Informáticos.

**Criptografía de llave publica**: Es el arte o ciencia de cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos.

**Cifrar**: Quiere decir transformar un mensaje en un documento no legible, y el proceso contrario se llama `descodificar" o `descifrar". Los sistemas de cifrado se llaman `sistemas criptográficos".

**Certificado Digital**: Un bloque de caracteres que acompaña a un documento y que certifica quién es su autor (autenticación) y que no haya existido ninguna manipulación de los datos (integridad). Para firmar, el firmante emisor utiliza una clave secreta que le vincula al documento. La validez de la firma podrá ser comprobada por cualquier persona que disponga de la clave pública del autor.

**Departamento de Cómputo:** Es la entidad encargada del buen uso de las tecnologías de la computación, organización y optimización de los recursos computacionales de la institución.

**Bases de Datos:** Es un conjunto de datos interrelacionados y un conjunto de programas para accesarlos. Una recopilación de datos estructurados y organizados de una manera disciplinada para que el acceso a la información de interés sea rápido.

**WWW (World Wide Web):** Es una convergencia de conceptos computacionales para presentar y enlazar información que se encuentra dispersa a través de internet en una forma fácilmente accesible. Sistema avanzado para navegar a través de internet.

**Área Crítica:** Es el área física donde se encuentra instalado el equipo de cómputo y telecomunicaciones que requiere de cuidados especiales y son indispensables para el funcionamiento continuo de los sistemas de comunicación de la empresa.

**Equipo de Telecomunicaciones:** Todo dispositivo capaz de transmitir y/o recibir señales digitales o analógicas para comunicación de voz, datos y video, ya sea individualmente o de forma conjunta.

**Equipo de Cómputo:** Dispositivo con la capacidad de aceptar y procesar información en base a programas establecidos o instrucciones previas, teniendo la oportunidad de conectarse a una red de equipos o computadoras para compartir datos y recursos, entregando resultados mediante despliegues visuales, impresos o audibles.

**IP -** Internet Protocol: Parte de la familia de protocolos TCP/IP, que describe el software que supervisa las direcciones de nodo internet, encamina mensajes salientes y reconoce los mensajes entrantes.

**Dirección de INTERNET:** Identificador único de 32 bits para una computadora principal TCP/IP en una RED. También llamada un Protocolo Internet o dirección IP. Las direcciones IP están normalmente impresas en una forma decimal de puntos, tal como 190.123.50.334.

**Auditoría:** Llevar a cabo una inspección y examen independiente de los registros del sistema y actividades para probar la eficiencia de la seguridad de datos y procedimientos de integridad de datos, para asegurar el cumplimiento con la política establecida y procedimientos operativos, y para recomendar cualquier cambio que se estime necesario.

**Control de Acceso:** Técnica usada para definir el uso de programas o limitar la obtención y almacenamiento de datos a una memoria. Una característica o técnica en un sistema de comunicaciones para permitir o negar el uso de algunos componentes o algunas de sus funciones.

## DEFINICIONES

**Riesgo en la seguridad de la información**

En Base a la norma técnica ISO 31000, se define el riesgo como “el efecto de la incertidumbre sobre los objetivos” (ISO 31000 Icontec, 2011, Pág.4).

De igual manera el objetivo general de dicha norma es gestionar el riesgo para identificar y establecer controles efectivos que garanticen la confidencialidad, integridad y disponibilidad de la información de Grapas y Puntillas EL CABALLO S.A.

**Factor del riesgo**

Se entiende por factores de riesgo dentro del Sistema de Seguridad de la Información, aquellos que pueden afectar la confidencialidad, integridad y disponibilidad de la información de Grapas y Puntillas EL CABALLO S.A. Entre los factores de riesgos que se encuentran identificados dentro de la organización están los siguientes:

| **Factor de Riesgo** | **Descripción** |
| --- | --- |
| Personas | Personal de la organización que se encuentra relacionado con la ejecución del proceso de forma directa o indirecta. |
|
| Procesos | Conjunto interrelacionado entre sí de actividades y tareas necesarias para llevar a cabo el proceso. |
| Tecnología | Conjunto de herramientas tecnológicas que intervienen de manera directa o indirecta en la ejecución del proceso. |
|
| Infraestructura | Conjunto de recursos físicos que apoyan el funcionamiento de la organización y de manera específica el proceso. |
|
| Factores Externos | Condiciones generadas por agentes externos, las cuales no son controlables por la empresa y que afectan de manera directa o indirecta el proceso. |
|

Fuente: ISO 31000 Icontec

**Eventos**

En la NTC ISO 27001, se define un evento de seguridad de la Información como “la presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.” (ISO 27001), por lo tanto, dentro de los eventos de seguridad de la información que se pueden llegar a presentar en Grapas y Puntillas EL CABALLO S.A., se encuentran los siguientes:

| **Evento** | **Descripción** |
| --- | --- |
| Fraude Interno | Está asociado a la intención por parte de un funcionario de Grapas y Puntillas EL CABALLO S.A., de obtener información con fines ajenos a su labor, incumpliendo normas y políticas de la Entidad. |
|
|
| Fraude Externo | Son actos realizados por personal externo de Grapas y Puntillas EL CABALLO S.A., que busca apropiarse indebidamente de la información, por medio de acceso no autorizado, alterando o vulnerando el procesamiento de la información en la compañía. |
|
|
| Acceso a Usuarios | Según el Anexo A.9.2.2., de la norma ISO 27001:2013 “Se debe implementar el suministro de acceso formal de usuarios para asignar o revocar los accesos para todo tipo de usuario”. |
|
|
| Fallas Tecnológicas | Pérdida de información asociada a fallas tecnológicas debido a errores en el procesamiento de la información que vulneran la confidencialidad, integridad y disponibilidad de la misma. |
|
|
| Ejecución y administración de procesos | Pérdida de información asociada a errores de administración y ejecución de procesos en Grapas y Puntillas EL CABALLO S.A. |
|

**Incidentes de seguridad**

Según la norma ISO 27001 un incidente de seguridad de la información está definido como “un evento o una serie de eventos de seguridad de la información no deseados o inesperados, que tienen la probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información” (ISO 27001 Icontec), por lo cual se establecen los siguientes incidentes que pueden llegar a suceder dentro de Grapas y Puntillas EL CABALLO S.A.:

* Acceso no autorizado a la información.
* Divulgación de información sensible.
* Denegación del servicio.
* Daño de la información.
* Ataques externos o internos.
* Pérdida o robo de la información.
* Modificación no autorizada.
* Información no actualizada.
* Mala gestión del conocimiento.
* Diligenciamiento errado de formatos.
* Perdida o daño de la documentación.

Así pues, este apartado contiene una clasificación de estas políticas, y son:

# MARCO LEGAL

El Sistema de Gestión de Seguridad de la Información (SGSI) de Grapas y Puntillas EL CABALLO S.A., se encuentra alineado con el cumplimiento de la Normatividad Legal Vigente Colombiana.

# ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) Grapas y Puntillas EL CABALLO S.A.

Dentro del alcance en la planeación e implementación del Sistema de Gestión de Seguridad de la Información – SGSI para Grapas y Puntillas EL CABALLO S.A., se incluyen los procesos de gestión Seguridad, salud En el trabajo y Ambiente, Gestión de Compras y Almacén, Gestión de Mejora, Gestión de Talento Humano, Gestión de Capacitación, Gestión Logística, Gestión Administrativa Y financiera, Gestión Comercial, Gestión de Seguridad, Gestión Tecnológica, Gestión gerencial, Gestión del riesgo, Gestión Tecnología de La Información.

Los sistemas de información que dan soporte al SGSI se encuentran identificados en el inventario de activos de información administrado en el área de Tecnologia de la información.

La operación de los procesos mencionados se encuentra centralizada en la sede principal en la dirección Calle 95 # 15 - 47 Of. 505 Bogotá.

El SGSI está enfocado en el cumplimento de requerimientos normativos, reglamentarios y legales que son aplicables a la compañía, teniendo en cuenta las necesidades y expectativas de las partes interesadas que son pertinentes al SGSI.

## LIDERAZGO Y COMPROMISO

La Alta Dirección de Grapas y Puntillas EL CABALLO S.A., se encuentra comprometida con el funcionamiento de un Sistema de Gestión de Seguridad de la Información eficiente y eficaz.

Dentro de las actividades que se realizan para apoyar al SGSI se encuentran:

* Mediante Acta de fecha dd/mm/aaaa, se definió el equipo técnico de seguridad de la información constituido por: la gerencia General (como invitado permanente), el Director Administrativo, el oficial de Seguridad de la Información, Jefe de Gestión del Riesgo y el Jefe de los sistemas integrados de gestión. Este grupo propenderá por el éxito de la gestión del SGSI y su mejora continua.
  + - * Aprobación de la Política General de Seguridad de la Información y socialización con los colaboradores de la compañía, así como con las partes interesadas que interactúan con Grapas y Puntillas EL CABALLO S.A.
      * Definición de objetivos de seguridad de la información alineados con los objetivos estratégicos de Grapas y Puntillas EL CABALLO S.A., y que aportan valor al negocio.
      * Definición y establecimiento de los roles y responsabilidades relacionados con la seguridad de la información en todos los niveles de la organización, los cuales se encontrarán en las descripciones de cargo existentes en el área de Talento Humano.
      * Ejecución de revisiones periódicas en las cuales se llevará a cabo seguimiento y monitoreo del SGSI.

## SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN DEL SGSI

Grapas y Puntillas EL CABALLO S.A., evalúa el desempeño de la seguridad de la información y la eficiencia del SGSI”, a través de:

### Auditorías internas

Grapas y Puntillas EL CABALLO S.A., programa y ejecuta auditorías internas con fechas planificadas, tal como lo establece la norma ISO 27001 y en concordancia con el programa de auditoría establecido para el Sistema de Gestión de Calidad.

### Revisión por parte de la Alta Dirección

Según la norma ISO 27001 y lo establecido en el Sistema de Gestión de Calidad, la Alta Dirección debe efectuar revisiones y su respectivo seguimiento al SGSI en las fechas planificadas.

### Mejoramiento continuo del SGSI

El sistema de Gestión de la Seguridad de la Información tiene como finalidad la generación de acciones que permitan a Grapas y Puntillas EL CABALLO S.A., tener un proceso de mejoramiento continuo del SGSI, por lo que basados en la norma ISO 27001, se establece que:

1. Cuando existan no conformidades, Grapas y Puntillas EL CABALLO S.A., debe tomar acciones para controlarlas y prevenirlas. Adicionalmente establece y hace frente a las consecuencias propias de la no conformidad que llegó a materializarse.
2. Se definen las acciones para disminuir las causas de las no conformidades así:

* Revisión y evaluación de la no conformidad encontrada.
* Establecimiento de las posibles causas y consecuencias que se generaron de la no conformidad.
* Determinar si existen otras no conformidades similares para establecer acciones preventivas evitando así que éstas lleguen a materializarse.
* Emprender acciones preventivas que permitan gestionar el riesgo a tiempo, disminuyendo el impacto y la probabilidad de ocurrencia del riesgo detectado, así como la aparición de no conformidades dentro del SGSI.

1. Adicionalmente se lleva un registro documentado del tratamiento realizado a la no conformidad, así como las acciones realizadas para controlar el impacto de esta y su resultado, en futuras no conformidades.

# ROLES Y RESPONSABILIDADES PARA LA SEGURIDAD DE LA INFORMACIÓN

La Alta Dirección de Grapas y Puntillas EL CABALLO S.A., está comprometida con el Sistema de Gestión de Seguridad de la Información, por lo cual tiene como funciones las siguientes:

1. El establecimiento de objetivos dentro del Sistema de Gestión de Seguridad de la Información, que sean coherentes con el objetivo general de la organización.
2. El control por parte de la dirección del Sistema de Gestión de Seguridad de la Información se realizará a través de revisiones periódicas, las cuales serán planificadas, cumpliendo con los requerimientos del SGSI y de Grapas y Puntillas EL CABALLO S.A.
3. La Alta Dirección establece y aprueba una Política de Seguridad de la Información que debe ser publicada y divulgada a toda la Entidad.
4. Propender por la implementación de acciones tanto preventivas como correctivas que permitan a Grapas y Puntillas EL CABALLO S.A., la mitigación de los riesgos potenciales.
5. Este Manual será revisado al menos una vez al año y se realizarán las actualizaciones que sean necesarias para mantenerlo alineado con las necesidades de la Entidad.

## GESTIÓN DE TECNOLOGÍA

Es responsabilidad del Proceso de Gestión de tecnología de la Información de Grapas y Puntillas EL CABALLO S.A.:

1. Promover el cumplimiento por parte del personal bajo su responsabilidad de las políticas de seguridad de información.
2. Implementar y administrar las herramientas tecnológicas para el cumplimiento de las políticas de seguridad de información.
3. Registrar y mantener la información requerida para auditar y evaluar la ejecución de los controles específicos de seguridad de la información.
4. Diseñar, desarrollar, instalar y mantener las aplicaciones bajo su responsabilidad de acuerdo con la metodología establecida e incluyendo los controles de seguridad de información.
5. Establecer, documentar y dar mantenimiento a los procedimientos de seguridad que apliquen para la plataforma de tecnologías de información administrada por esta oficina.
6. Definir y aplicar los procedimientos para garantizar la disponibilidad y capacidad de los recursos tecnológicos a su cargo.
7. Establecer y dar mantenimiento a los procedimientos de continuidad y de contingencias para cada una de las plataformas tecnológicas críticas bajo su responsabilidad.
8. Evaluar los procesos o actividades sobre las plataformas tecnológicas, delegados en terceros.
9. Implementar y administrar los controles de seguridad sobre los datos y conexiones de la red bajo su administración.
10. Definir y gestionar programas de capacitación y entrenamiento que incluyan temas relevantes y pertinentes sobre seguridad de información.
11. Custodiar la información y los medios de almacenamiento bajo su responsabilidad.
12. Operar y administrar los recursos de cómputo, de red y de software bajo su responsabilidad.

## GESTIÓN DE RIESGOS

1. El objetivo de la Gestión de riesgos es identificar y evaluar los riesgos de seguridad de la información a los cuales están expuestos los activos de la Entidad, para identificar y aplicar el plan de tratamiento más adecuado.
2. La evaluación de riesgos está basada en el impacto y probabilidad de ocurrencia de éstos para la Entidad y los requerimientos de los niveles de seguridad, tomando en cuenta los controles existentes.
3. El análisis y evaluación de riesgos deberá hacerse al menos una vez al año.

El detalle de la metodología de riesgos se encuentra en el documento Metodología de Análisis de Riesgos de Seguridad de la Información. (F01-GR-MR-21 V2 MATRIZ DE RIESGOS OPERATIVOS)

## DUEÑOS DE LOS PROCESOS

Los dueños de los procesos tienen como funciones las siguientes: Definir, documentar, mantener, actualizar y mejorar permanentemente los procedimientos relacionados a su proceso, incluyendo aquellas actividades que sean consideradas como controles de seguridad de la información dentro de dichos procedimientos.

## PROPIETARIOS DE LOS RIESGOS (LÍDERES DE LOS PROCESOS)

Es responsabilidad de los propietarios del riesgo:

1. Clasificar sus activos de información de acuerdo con los requerimientos de confidencialidad, integridad y disponibilidad.
2. Participar en la definición de los requerimientos de continuidad y de recuperación en caso de desastre.
3. Realizar, en conjunto con el director de riesgos, un análisis anual de riesgos, para determinar el grado de exposición a las amenazas existentes y verificar los controles relacionados con la protección de la confidencialidad, integridad y disponibilidad de los activos de Información de su proceso.
4. Definir, con el acompañamiento del director de riesgos, los requerimientos de seguridad para los activos de información que hacen parte de su proceso, para que se les proporcione el nivel adecuado de protección de conformidad con los estándares, políticas y procedimientos de seguridad de información.
5. Determinar y autorizar todos los privilegios de acceso a sus activos de información.
6. Comunicar y gestionar con el Área de Seguridad de la Información sus requerimientos en capacitación sobre seguridad de información.
7. Reportar cualquier situación que involucre un incumplimiento o violación a la seguridad de Información, de acuerdo con el procedimiento de Gestión de Incidentes de Seguridad.
8. Participar en la resolución de los incidentes relacionados con el acceso no autorizado o mala utilización de los activos de información bajo su responsabilidad.

## FUNCIONARIOS, CONTRATISTAS Y TERCEROS

Es responsabilidad de los funcionarios Contratistas y terceros, salvaguardar la información institucional de Grapas y Puntillas EL CABALLO S.A., garantizando así la confidencialidad, integridad y disponibilidad de la información teniendo como funciones:

1. Cumplir fielmente las políticas de seguridad de la información, contempladas en el presente manual.
2. Reportar, a la mayor brevedad posible y a través de los canales establecidos, la sospecha u ocurrencia de eventos considerados incidentes de seguridad de información.
3. Realizar sugerencias a la Alta dirección para mejorar los procesos relacionados con los activos de información de Grapas y Puntillas EL CABALLO S.A., y optimizar así el sistema de seguridad de la información.
4. Utilizar los sistemas de información y el acceso a la red únicamente para los propósitos indicados en las políticas de seguridad de la información.
5. Incorporar la seguridad de información como parte de las actividades y tareas bajo su responsabilidad.
6. Conocer las directrices de protección de los activos de información que utilicen.
7. Utilizar únicamente software y demás recursos tecnológicos autorizados.

## EQUIPO TÉCNICO DE SEGURIDAD DE LA INFORMACIÓN

Este equipo asegura que exista una dirección y apoyo gerencial para soportar la administración y desarrollo de iniciativas sobre seguridad de la información, a través de compromisos apropiados y uso de recursos adecuados en la compañía, así como la formulación y mantenimiento de una política de seguridad de la información para Grapas y Puntillas EL CABALLO S.A.

Su función principal es definir, estructurar, recomendar, hacer seguimiento y mejoras al Sistema de Gestión de Seguridad de la Información (SGSI) de Grapas y Puntillas EL CABALLO S.A.

El equipo técnico de Seguridad de la Información de Grapas y Puntillas EL CABALLO S.A., está conformado así:

1. Oficial de Seguridad de la Información, Líder del equipo.
2. Líder del proceso Gestión de Riesgos, quien ejercerá la secretaría técnica del equipo.
3. Gerente General como invitado permanente.
4. Director Administrativo y Financiero como invitado permanente.
5. Líder del proceso Sistema Integrado de Gestión

## OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

Será el responsable por la implementación, operación, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información en Grapas y Puntillas EL CABALLO S.A. Entre sus principales funciones estarán:

1. Ejecutar las tareas de seguridad de la información asignadas por la compañía.
2. Monitorear las violaciones de seguridad y aplicar acciones correctivas para asegurar que se provea la seguridad adecuada
3. Revisar y evaluar periódicamente la política de seguridad y sugerir a la alta dirección los cambios necesarios.
4. Preparar y monitorear el programa de sensibilización en seguridad para todos los empleados y terceros.
5. Probar la arquitectura de seguridad para evaluar la fortaleza de la seguridad y para detectar las posibles amenazas.
6. Trabajar con la Oficina Asesora de Gestión del Riesgo, el monitoreo de los riesgos para validar que el esquema de seguridad de la información esté diseñado de manera apropiada y actualizada sobre la base de retroalimentación de auditoría o de pruebas.
7. Mantener informado al proceso Gestión tecnología de la Información, sobre los eventos e incidentes de seguridad que se presenten al interior de la misma.
8. Gestionar la actualización del Sistema de Gestión de Seguridad de la Información.
9. Definir la estrategia de gestión de los riesgos de seguridad de la información, coordinar su implementación y centralizar el monitoreo sobre su ejecución.
10. Supervisar el cumplimiento de los procedimientos del Sistema de Gestión de Seguridad de la Información.
11. Promover la creación y actualización de las políticas y estándares de seguridad de la información y velar por el cumplimiento de las mismas.
12. Apoyar la consolidación de la cultura de seguridad de la información entre todo el personal.
13. Coordinar la difusión de cualquier comunicación relacionada con el proceso Gestión tecnología de la Información.
14. Participar activamente en las actividades convocadas por el proceso Gestión tecnología de la Información.
15. Coordinar la realización periódica de auditorías internas y pruebas de vulnerabilidad de acuerdo con las políticas establecidas.
16. Elaborar y proponer al proceso Gestión tecnología de la Información, planes, procedimientos y controles para el mejoramiento del Sistema de Gestión de Seguridad de la Información.
17. Proponer al proceso Gestión tecnología de la Información, planes de capacitación y entrenamiento para difundir las políticas, normas y estándares de seguridad de la información al personal.
18. Apoyar y coordinar el desarrollo de actividades de investigación y búsqueda de información referente a seguridad de la información.
19. Elaborar los informes que le sean requeridos por el proceso Gestión tecnología de la Información sobre el Sistema de Gestión de Seguridad de la Información.
20. Coordinar la implementación de acciones preventivas y correctivas del Sistema de Gestión de Seguridad de la Información con los respectivos responsables, de acuerdo con los resultados de las auditorías internas o externas.
21. Implementar y hacer seguimiento al plan de mejora continua del Sistema de Gestión de Seguridad de la Información.
22. Coadyuvar en los procesos de certificación y recertificación.
23. Proponer y apoyar proyectos de seguridad de la información.

# POLITICAS

# POLITICA 1: SEGURIDAD DE LA INFORMACION

Los empleados de Grapas y Puntillas EL CABALLO S.A., son responsables de la información que manejan y deberán cumplir los lineamientos generales y especiales dados por la compañía, para protegerla y evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma.

Los funcionarios y/o contratistas que laboren en Grapas y Puntillas EL CABALLO S.A., no deben suministrar información de la compañía a ningún ente externo sin las autorizaciones respectivas.

Todo empleado de Grapas y Puntillas EL CABALLO S.A., tiene la responsabilidad de velar por la integridad, confidencialidad y disponibilidad de la información que maneje, especialmente si dicha información está protegida por consideraciones legales o ha sido clasificada como confidencial con una clasificación de criticidad.

Los empleados y/o contratistas deben firmar un acuerdo de cumplimiento de la seguridad de la información, la confidencialidad y el buen manejo de la información. Después de que el trabajador o el contratista, deja de prestar sus servicios a la Empresa, se compromete entregar toda la información respectiva del trabajo realizado. Una vez retirado el empleado y/o contratistas debe comprometerse a no utilizar, comercializar o divulgar la información generada o conocida durante la gestión, directamente o través de terceros, así mismo, los empleados que detecten el mal uso de la información están en la obligación de reportar el hecho al proceso de Gestión Tecnología de la información.

Como regla general, la información de políticas, normas y procedimientos de seguridad se deben revelar únicamente a empleados y entes externos que lo requieran, de acuerdo con las actividades a desarrollar según sea el caso.

## POLÍTICA 2: ADMINISTRACIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN

Los dueños de cada proceso en Grapas y Puntillas EL CABALLO S.A., identifican, analizan y evalúan los riesgos asociados a sus activos de información, de acuerdo con la metodología establecida. Adicionalmente implementan las acciones tanto correctivas como preventivas establecidas en el plan de tratamiento definido para los riesgos analizados y que estén por encima del nivel de riesgo aceptable definido por la Entidad.

### Normas de uso

1. Los Líderes de Procesos de Grapas y Puntillas EL CABALLO S.A., tienen conocimiento de los posibles riesgos, causas y vulnerabilidades asociados a cada activo de información, con el fin de garantizar los principios de confidencialidad, integridad y disponibilidad de la información.
2. La Alta Dirección promueve el seguimiento de los eventos asociados con la prevención de los riesgos para la seguridad de la información.
3. Se revisarán las políticas para la seguridad de la información en periodos planificados establecidos por la Entidad.

## POLÍTICA 3: POLÍTICA PARA LOS DISPOSITIVOS MÓVILES

Para el uso de dispositivos de computación móvil como equipos portátiles, teléfonos móviles, tabletas, entre otros, se implementan controles de acceso, técnicas criptográficas para cifrar la información crítica almacenada en éstos, mecanismos de respaldo de la información que contienen y los demás que se consideren necesarios y pertinentes para garantizar la seguridad de la información.

### Normas dispositivos móviles

1. El proceso de Gestión Tecnología de la Información, definirá los mecanismos de autorización y conexión de dispositivos móviles que no son de su propiedad y que necesiten hacer uso de sus redes inalámbricas públicas.
2. Los dispositivos móviles que hagan uso de las redes inalámbricas institucionales deben contar con las herramientas de seguridad necesarias para mitigar el contagio de código malicioso y que garanticen la seguridad de la información que contienen.
3. La conexión de los dispositivos móviles a la infraestructura tecnológica institucional deberá ser autorizada por el proceso de Gestión tecnología de la información, previa verificación de que cuenten con las condiciones de seguridad necesarias para proteger los demás recursos e información de la red.

Adicionalmente se establece que:

1. Se identifican y autentican los dispositivos específicos antes de establecer cualquier tipo de conexión a recursos informáticos de Grapas y Puntillas EL CABALLO S.A.
2. Se establece un conjunto de derechos y privilegios restrictivo a los accesos mínimos necesarios por los usuarios para el desempeño de tareas específicas.

### Trabajo Remoto

Para la ejecución de actividades de trabajo remoto se deben tener en cuenta las siguientes consideraciones:

1. Acceder a la infraestructura tecnológica únicamente desde equipos autorizados por Grapas y Puntillas EL CABALLO S.A.
2. No está permitido conectarse a los sistemas de información de Grapas y Puntillas EL CABALLO S.A., a través de redes públicas.
3. Para acceder a los sistemas o aplicaciones de Grapas y Puntillas EL CABALLO S.A., se debe gestionar el acceso por VPN con el proceso de Gestión Tecnología de la información.

# POLITICA 4: ACCESO A LA INFORMACIÓN

Todos los funcionarios y/o, contratistas, que laboran para Grapas y Puntillas EL CABALLO S.A., deben tener acceso sólo a la información necesaria para el desarrollo de sus actividades.

El otorgamiento de acceso a la información está regulado mediante las normas y procedimientos definidos para tal fin.

Todos los privilegios para el uso de los sistemas de información de la organización deben terminar inmediatamente después de que el trabajador finaliza de prestar sus servicios a la compañía.

Proveedores o terceros solamente deben tener privilegios durante el periodo del tiempo requerido para llevar a cabo las funciones aprobadas.

Para dar acceso a la información se tendrá en cuenta la clasificación de la misma al interior de la compañía, la cual deberá realizarse de acuerdo con la importancia de la información.

Mediante el registro de eventos en los diversos recursos informáticos de la plataforma tecnológica se efectuará un seguimiento a los accesos realizados por los usuarios a la información de la Organización, con el objeto de minimizar el riesgo de pérdida de integridad de la información. Cuando se presenten eventos que pongan en riesgo la integridad, veracidad y consistencia de la información se deberán documentar y realizar las acciones tendientes a su solución.

# POLÍTICA 5: ADMINISTRACIÓN DE CAMBIOS

Todo cambio (creación y modificación de programas, pantallas y reportes) que afecte los recursos informáticos, debe ser requerido por los usuarios de la información y aprobado formalmente por el responsable de la administración del mismo

El responsable de la administración de los accesos tendrá la facultad de aceptar o rechazar la solicitud.

Para la administración de cambios se efectuará el procedimiento correspondiente definido por Grapas y Puntillas EL CABALLO S.A. de acuerdo con el tipo de cambio solicitado en la plataforma tecnológica.

Cualquier tipo de cambio en la plataforma tecnológica debe quedar formalmente documentado desde su solicitud hasta su implantación. Este mecanismo proveerá herramientas para efectuar seguimiento y garantizar el cumplimiento de los procedimientos definidos.

Todo cambio a un recurso informático de la plataforma tecnológica relacionado con modificación de accesos, mantenimiento de software o modificación de parámetros debe realizarse de tal forma que no disminuya la seguridad existente.

# POLITICA 6: SEGURIDAD PARA LOS SERVICIOS INFORMATICOS

El correo electrónico, herramientas de mensajería instantánea, listas de distribución y demás servicios asociados de la compañía debe ser usado únicamente para la ejecución de las funciones de competencia de cada empleado y de las actividades contratadas por un tercero.

La compañía se reserva el derecho de acceder y revelar todos los mensajes enviados por medio del sistema de correo electrónico para cualquier propósito.

La propiedad intelectual desarrollada o concebida mientras el trabajador se encuentre en sitios de trabajo alternos, es propiedad exclusiva de la compañía. Esta política incluye patentes, derechos de reproducción, marca registrada y otros derechos de propiedad intelectual según lo manifestado en memos, planes, estrategias, productos, programas de computación, códigos fuentes, documentación y otros materiales.

Los empleados y/o contratistas que hayan recibido aprobación para tener acceso a Internet deberán aceptar, respetar y aplicar las políticas y prácticas de uso de Internet.

En cualquier momento que un trabajador publique un mensaje en un grupo de discusión de Internet, en un boletín electrónico, o cualquier otro sistema de información público, este mensaje debe ir acompañado de palabras que indiquen claramente que su contenido no representa la posición de la empresa.

Si los usuarios sospechan que hay infección por un virus, deben inmediatamente llamar a la oficina de informática, no utilizar el computador y desconectarlo de la red.

# POLITICA 7: SEGURIDAD EN RECURSOS INFORMATICOS

Todos los recursos informáticos deben cumplir como mínimo con lo siguiente:

Administración de usuarios: Establece como deben ser utilizadas las claves de ingreso a los recursos informáticos. Establece parámetros sobre la longitud mínima de las contraseñas, la frecuencia con la que los usuarios deben cambiar su contraseña y los períodos de vigencia de las mismas, entre otras.

Rol de Usuario: Los sistemas operacionales, bases de datos y aplicativos deberán contar con roles predefinidos o con un módulo que permita definir roles, definiendo las acciones permitidas por cada uno de estos. Deberán permitir la asignación a cada usuario de posibles y diferentes roles. También deben permitir que un rol de usuario administre la Administración de usuarios.

Plan de auditoría: Hace referencia a las pistas o registros de los sucesos relativos a la operación.

El control de acceso a todos los sistemas de computación de la compañía debe realizarse por medio de códigos de identificación y palabras claves o contraseñas únicos para cada usuario.

Las palabras claves o contraseñas de acceso a los recursos informáticos, que designen los empleados y/o, contratistas son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgados a ninguna persona.

Los usuarios son responsables de todas las actividades llevadas a cabo con su carnet de identificación de usuario y sus claves personales.

Todo sistema debe tener definidos los perfiles de usuario de acuerdo con la función y cargo de los usuarios que acceden a él.

El nivel de superusuario de los sistemas críticos debe tener un control dual, de tal forma que exista una supervisión a las actividades realizadas por el administrador del sistema.

Toda la información de los servidores de base de datos que sea sensible, crítica o valiosa debe tener controles de acceso y sometida a procesos de cifrado para garantizar que no sea inapropiadamente descubierta, modificada, borrada o no recuperable.

Antes de que un nuevo sistema se desarrolle o se adquiera, los directores en conjunto con el asesor de seguridad informática, deberán definir las especificaciones y requerimientos de seguridad necesarios.

La seguridad debe ser implementada por diseñadores y desarrolladores del sistema desde el inicio del proceso de diseño de sistemas hasta la conversión a un sistema en producción.

Los ambientes de desarrollo de sistemas, pruebas y producción deben permanecer separados para su adecuada administración, operación, control y seguridad y en cada uno de ellos se instalarán las herramientas necesarias para su administración y operación.

# POLITICA 8: SEGURIDAD EN COMUNICACIONES

Las direcciones internas, topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la compañía, deberán ser consideradas y tratadas como información confidencial.

La red de amplia cobertura geográfica a nivel nacional estar dividida en forma lógica por diferentes segmentos de red, cada uno separado con controles de seguridad perimetral y mecanismos de control de acceso.

Los computadores de Grapas y Puntillas EL CABALLO S.A., se conectarán de manera directa con computadores de compañías externas y/o filiales debe ser mediante conexiones seguras, previa autorización del área de seguridad informática y/o la Jefatura de sistemas.

Toda información confidencial que se transmita por las redes de comunicación de la empresa e Internet deberá estar cifrada.

# POLITICA 9: SEGURIDAD PARA USUARIOS TERCEROS

Los dueños de los Recursos Informáticos que no sean propiedad de la compañía y deban ser ubicados y administrados por ésta, deben garantizar la legalidad del recurso para su funcionamiento. Se debe definir un documento de acuerdo oficial entre las partes.

Cuando se requiera utilizar recursos informáticos u otros elementos de propiedad de Grapas y Puntillas EL CABALLO S.A. Para el funcionamiento de recursos que no sean propios de la empresa que deban ubicarse en sus instalaciones, los recursos serán administrados por el Help Desk de Grapas y Puntillas EL CABALLO S.A.

Los usuarios terceros tendrán acceso a los Recursos Informáticos, que sean estrictamente necesarios para el cumplimiento de su labor, servicios que deben ser aprobados por quien será el Director de sistemas. En todo caso deberán firmar el acuerdo de confidencialidad.

La conexión entre sistemas internos de la empresa y otros de terceros debe ser aprobada y certificada por la Dirección de sistemas con el fin de no comprometer la seguridad de la información interna de la empresa.

Los equipos de usuarios terceros que deban estar conectados a la Red, deben cumplir con todas las normas de seguridad informática.

# POLITICA 10: SOFTWARE UTILIZADO

Todo software que utilice Grapas y Puntillas EL CABALLO S.A., será adquirido de acuerdo con las normas vigentes establecidos y reguladas por el gobierno colombiano y siguiendo los procedimientos específicos de la empresa para su utilización.

Todo el software de manejo de datos que utilice en Grapas y Puntillas EL CABALLO S.A., dentro de su infraestructura informática, deberá contar con las técnicas más avanzadas de la industria para garantizar la integridad de los datos.

Debe existir una cultura informática al interior de la empresa que garantice el conocimiento por parte de los empleados y/o terceros, de instalar software ilegal en los computadores de Grapas y Puntillas EL CABALLO S.A.

Existirá un inventario de las licencias de software de Grapas y Puntillas EL CABALLO S.A., que permita su adecuada administración y control evitando posibles sanciones por instalación de software no licenciado.

# POLITICA 11: ACCESO A WEB

En concordancia con la legislación actual y de común acuerdo con las políticas generales de informática, la dirección de sistemas a través de la coordinación de infraestructura, coordinación de seguridad de la información es el responsable de instalar y administrar el o los servidores WWW. Es decir, sólo se permiten servidores de páginas autorizados por la Dirección de sistemas.

La Dirección de sistemas en conjunto con la coordinación de infraestructura deberá emitir las normas y los requerimientos para la instalación de servidores de páginas locales, de bases de datos, del uso de la Intranet de la empresa, así como las especificaciones para que el acceso a estos sea seguro.

Los accesos a las páginas de web a través de los navegadores deben sujetarse a las normas que previamente se manifiestan en la estrategia de infraestructura y seguridad de la información con relación al acceso a la red de Grapas y Puntillas EL CABALLO S.A.

A la coordinación de Infraestructura y coordinación de seguridad de la información corresponden los servidores de Web, para su verificación de respaldo y protección adecuada.

Toda la programación involucrada en la tecnología Web deberá estar de acuerdo con las normas y procedimientos que la Dirección de sistemas emita.

El material que aparezca en la página de Internet de Grapas y Puntillas EL CABALLO S.A., deberá ser aprobado por la Gerencia General y la Dirección de Informática, respetando la ley de propiedad intelectual (derechos de autor, créditos, permisos y protección, como los que se aplican a cualquier material impreso).

En concordancia con la libertad de investigación, se acepta que en la red de Grapas y Puntillas EL CABALLO S.A., conectada a Internet pueda ponerse información individual sin autorización (siempre y cuando no contravenga las disposiciones que se aplican a las instituciones gubernamentales y estatales),

Con referencia a la seguridad y protección de las páginas, así como al diseño de las mismas deberá referirse a las consideraciones de diseño de páginas electrónicas establecidas por la Dirección de sistemas.

La Dirección de sistemas tiene la facultad de llevar a cabo la revisión periódica de los accesos a nuestros servicios de información, y conservar información del tráfico.

# POLITICA 12: ACTUALIZACION DE HARDWARE

Cualquier cambio que se requiera realizar en los equipos de cómputo de la empresa (cambios de procesador, adición de memoria o tarjetas) debe tener previamente una evaluación técnica y autorización del área responsable.

La reparación técnica de los equipos, que implique la apertura de los mismos, únicamente puede ser realizada por el personal autorizado.

Los equipos de microcomputadores (PC, servidores, LAN etc.) no deben moverse o reubicarse sin la aprobación previa del administrador, Dirección, coordinador del área involucrada.

# POLITICA 13: ALMACENAMIENTO Y RESPALDO

La información que es soportada por la infraestructura de tecnología informática de Grapas y Puntillas EL CABALLO S.A. Deberá ser almacenada y respaldada de acuerdo con las normas establecidas por la Dirección de sistemas de tal forma que se garantice su disponibilidad.

Debe existir una definición formal de la estrategia de generación, retención y rotación de las copias de respaldo.

La empresa definirá la custodia de los respaldos de la información que se realizará externamente con una compañía distinta, que asegure las condiciones de disponibilidad, integridad y confidencialidad.

El almacenamiento de la información deberá realizarse interna y/o externamente a la empresa, esto de acuerdo con la importancia de la información para la operación del Grapas y Puntillas EL CABALLO S.A.

La dirección dueña de la información en conjunto con la Dirección de sistemas definirá la estrategia a seguir para el respaldo de la información.

Los empleados son responsables de los respaldos de su información en los computadores y/o portátiles, siguiendo las indicaciones técnicas dictadas por la Dirección de sistemas. La Dirección de sistemas será la autorizada para realizar el seguimiento y control de esta política.

# POLITICA 14: CONTINGENCIA

La administración de la empresa debe preparar, actualizar periódicamente y probar en forma regular un plan de contingencia que permita a las aplicaciones críticas y sistemas de cómputo y comunicación estar disponibles en el evento de un desastre de grandes proporciones como terremoto, explosión, terrorismo, inundación etc. (DRP)

# POLITCA 15: AUDITORIA

Todos los sistemas automáticos que operen y administren información sensible, valiosa o crítica para la compañía, como son sistemas de información en producción, sistemas operativos, Bases de Datos y telecomunicaciones deben generar pistas (adición, modificación, borrado) de auditoría.

Todos los archivos de auditorías deben proporcionar suficiente información para apoyar el monitoreo, control y auditorias.

Todos los archivos de auditorías de los diferentes sistemas deben preservarse por periodos definidos según su criticidad y de acuerdo a las exigencias legales para cada caso.

Todos los archivos de auditorías deben ser custodiados en forma segura para que no puedan ser modificados y para que puedan ser leídos únicamente por personas autorizadas; los usuarios que no estén autorizados deben solicitarlos al área encargada de su administración y custodia.

Todos los computadores y/o portátiles de la empresa deben estar sincronizados y tener la fecha y hora exacta para que el registro en la auditoria sea correcto.

# POLITICA 16: SEGURIDAD FISICA

La compañía deberá contar con los mecanismos de control de acceso tales como puertas de seguridad, sistemas de control con tarjetas inteligentes, sistema de alarmas y circuitos cerrados de televisión en las áreas que la compañía considere críticas.

Los visitantes de las oficinas de la empresa deben ser escoltados durante todo el tiempo por un empleado autorizado y/o contratista. Esto significa que se requiere de un escolta tan pronto como un visitante entra a un área y hasta que este mismo visitante sale del área controlada. Todos los visitantes requieren una escolta incluyendo clientes, antiguos empleados, miembros de la familia del trabajador.

Siempre que un trabajador se dé cuenta que un visitante no escoltado se encuentra dentro de áreas restringidas de la compañía, el visitante debe ser inmediatamente cuestionado acerca de su propósito de encontrarse en área restringida e informar a las responsables de la seguridad de las instalaciones de la compañía.

Los centros de cómputo o áreas que la compañía considere críticas, deben ser lugares de acceso restringido y cualquier persona que ingrese a ellos deberá registrar el motivo del ingreso y estar acompañada permanentemente por el personal que labora en estos lugares.

Toda persona que se encuentre dentro de la compañía deberá portar su identificación en lugar visible.

En los centros de cómputo o áreas que la empresa considere criticas deberán existir elementos de control de incendio, inundación y alarmas.

Los centros de cómputo o áreas que la empresa considere criticas deberán estar demarcados con zonas de circulación y zonas restringidas.

Las centrales de conexión o centros de cableado deben ser catalogados como zonas de alto riesgo, con limitación y control de acceso.

Todos los computadores portátiles, módems y equipos de comunicación se deben registrar su ingreso y salida y no debe abandonar la compañía a menos que esté acompañado por la autorización respectiva y la validación de supervisión de la Dirección de sistemas.

Todos los visitantes deben mostrar identificación con fotografía y firmar antes de obtener el acceso a las áreas restringidas controladas por la empresa.

Los equipos (PCs, servidores, equipos de comunicaciones, entre otros) no deben moverse o reubicarse sin la aprobación previa.

Los empleados se comprometen a NO utilizar a la red regulada de energía para conectar equipos eléctricos diferentes a su equipo de cómputo, como impresoras, cargadores de celulares, grabadoras, electrodomésticos, fotocopiadoras y en general cualesquiera equipos que generen caídas de la energía.

Los particulares en general, entre ellos, los familiares de los empleados, no están autorizados para utilizar los recursos informáticos de la compañía.

# POLITICA 17: ESCRITORIOS LIMPIOS

Todos los escritorios o mesas de trabajo deben permanecer limpios para proteger documentos en papel y dispositivos de almacenamiento como CD, s, USB, entre otros dispositivos móviles de almacenamiento, con fin de reducir los riesgos de acceso no autorizado, perdida y daño de la información durante el horario normal de trabajo y fuera del mismo.

# POLITICA 18: ADMINISTRACION DE LA SEGURIDAD

Riesgos Por evaluar con la DS

Cualquier brecha de seguridad o sospecha en la mala utilización en el Internet, la red corporativa o Intranet, los recursos informáticos de cualquier nivel (local o corporativo) deberá ser comunicada por el empleado que la detecta, en forma inmediata y confidencial a la Jefatura de sistemas y/o Coordinación de seguridad Informática.

La coordinación de seguridad de la información divulgará, las políticas, estándares y procedimientos en materia de seguridad de la información efectuará el seguimiento al cumplimiento de las políticas de seguridad y reportará a la dirección General, los casos de incumplimiento con copia a la Direccion de sistemas.

# POLITICA 19: MEDIOS EXTRAIBLES

Grapas y Puntillas el caballo restringe el uso de dispositivos de almacenamiento extraíble para todos los usuarios y funcionarios de la compañía, sin embargo, el área de TI por directivas de seguridad tiene una unidad organizativa que permite usar estos dispositivos para el ingreso de información a los equipos de la compañía, para el caso de poder sacar información de los quipos de la compañía siempre será necesario solicitar el permiso al área de TI quienes realizaran la debida inspección de la información requerida.

El usuario o funcionario que posea de forma temporal o permanente un dispositivo de almacenamiento extraíble, incluyendo aquellos de propiedad de Grapas y Puntillas el Caballo y que le fueron asignados para custodia y uso, es el único responsable de uso y manejo del mismo, así como de la información contenida en dicho dispositivo, su correcto uso y resguardo.

• Los usuarios o funcionarios que posean de forma temporal o permanente un dispositivo de almacenamiento extraíble, están sujetos a las mismas normas y reglamentos que se aplican dentro de las dependencias de la compañía en cuanto al manejo, uso, resguardo y confidencialidad de la información; así como, a todas aquellas normas, reglamentos y disposiciones emitidas por la entidad o autoridad competente. Su incumplimiento será motivo de las acciones o sanciones que correspondan, según la gravedad de la falta.

• El Personal de TI únicamente brinda apoyo y asesoría a los funcionarios y usuarios, para el formateo y correcto uso de los dispositivos, mas no es responsable de la información contenida en los mismos, ni de su uso, transporte, manejo o manipulación.

El área de TI de grapas y puntillas el caballo no provee de dispositivos de almacenamiento extraíbles a ningún Usuario o funcionario. En caso de requerir algún dispositivo, este debe ser requerido al área administrativa o la que corresponda.

• Previo a usar un dispositivo de almacenamiento extraíble en los equipos corporativos, se recomienda a los Usuarios y funcionarios que lo posean, hagan una revisión de virus utilizando el antivirus instalado por el área de TI de grapas y puntillas el caballo confiable y actualizado.

• Se recomienda a usuarios y funcionarios que posean de forma temporal o permanente un dispositivo de almacenamiento extraíble, que el equipo personal que usan fuera de la compañía y que no pertenece a la misma, tenga un antivirus instalado y debidamente actualizado.

• Se sugiere a usuarios y funcionarios que el resguardo de los dispositivos de almacenamiento de información extraíble, debe hacerse en función de las recomendaciones de los fabricantes.

• Es altamente recomendable que en los medios o dispositivos extraíbles que permitan incluir claves de acceso, el propietario o custodio las incluya. Del mismo modo, en la información corporativa relevante y que sea trasladada empleando medio o dispositivos extraíbles, se asigne contraseña para garantizar la seguridad de la información.

# SANCIONES

Cualquier violación a las políticas y normas de seguridad deberá ser sancionada de acuerdo al reglamento emitido por la Dirección de sistemas y validada con la Gerencia General de la empresa.

Las sanciones pueden ser desde una llamada de atención o informar al usuario hasta la suspensión del servicio dependiendo de la gravedad de la falta y de la malicia o perversidad que ésta manifiesta.

Corresponderá al Comité Gerencial hacer las propuestas finales sobre las sanciones a quienes violen las disposiciones en materia de informática de la empresa.

Todas las acciones en las que se comprometa la seguridad de Grapas y Puntillas EL CABALLO S.A., y que no estén previstas en esta política, deberán ser revisadas por la Dirección General y la Dirección de sistemas para dictar una medida frente al incidente de seguridad presentado.

# NOTAS

Esta política de seguridad deberá seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: crecimiento de la planta de personal, cambio en la infraestructura computacional, desarrollo de nuevos servicios, entre otros.

El documento que contiene la política de seguridad deber ser difundido a todo el personal involucrado en la definición de estas políticas.