1. **OBJETIVO**  
      
   Establecer reglas y lineamientos técnicos para el uso controlado de la información que minimice el riesgo de pérdida de datos, accesos no autorizados, divulgación no controlada, duplicación e interrupción intencional de la información.  
      
   **2.     ALCANCE**  
      
   El procedimiento y Políticas de Seguridad Informática PINTURAS INDUSTRIALE S LTDA, integra a proveedores, clientes internos (departamentos y tiendas) que integra el grupo de trabajo y contratistas.

Incluye los lineamientos para proteger la información de la empresa y los recursos tecnológicos  con la que se procesa y se almacena, así como la recuperación de la información mantenida a nivel de medios (discos duros, memorias USB, entre otros).

**3.**     **OBLIGACIONES**  
   
Es un compromiso de todos los clientes de PINTURAS INDUSTRIALE S LTDA, conocer el Procedimiento y Políticas de Seguridad Informática y es su deber cumplirlas y respetarlas para el desarrollo de cualquier actividad TIC o consulta de sus productos.   
   
**4.**     **PROPÓSITO**  
   
El propósito que tiene PINTURAS INDUSTRIALE S LTDA al establecer el procedimiento y Políticas de Seguridad Informática es definir las normas y lineamientos a través de este documento para que la gestión de proyectos y recursos TIC se realice obedeciendo la directriz de seguridad y evitar que se creen vulnerabilidades que impacten la empresa.   
   
5.     **MARCO LEGAL**

* **Ley Estatutaria 15 81 de 2012 y Reglamentada Parcialmente por el Decreto Nacional 1377 de 2013:**Por la cual se dictan disposiciones generales para la protección de datos personales.

**Decreto 2693 de 2012:**Lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia que lidera el Ministerio de las Tecnologías de Información y las Comunicaciones, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.

**Decreto 2578 de 2012:**Por medio del cual se reglamenta el Sistema Nacional de Archivos. Incluye “El deber de entregar inventario de los documentos de archivo a cargo del servidor público, se circunscribe tanto a los documentos físicos en archivos tradicionales, como a los documentos electrónicos que se encuentren en equipos de cómputo, sistemas de información, medios portátiles” entre otras disposiciones.

* **Decreto 2609 de 2012:**Por medio del cual se reglamenta el Título V de la Ley General de Archivo del año 2000. Incluye aspectos que se deben considerar para la adecuada gestión de los documentos electrónicos.

* **Ley 1273 DE 2009:**Por medio de la cual se modifica el Código Penal, se crea un nuevo bien tutelado denominado “de la protección de la información y los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

* **Ley 1341 DE 2009:**Por medio de la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y comunicaciones - TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.

**Ley 1150 DE 2007:**Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos.

**Ley 962 DE 2005:**Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.

* **Ley 599 DE 2000:**Por la cual se expide el Código Penal. Se crea el bien jurídico de los derechos de autor e incorpora algunas conductas relacionadas indirectamente con los delitos informáticos como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas, y manifiesta que el acceso  abusivo a un sistema informático protegido con medida de seguridad o contra la voluntad de quien tiene derecho a excluirlo, incurre en multa.

6.     **ADVERTENCIA**  
   
Cualquier cliente de los recursos de TIC del PINTURAS INDUSTRIALE S LTDA que se encuentre realizando actividades que vayan en contra del Manual de Normas y Políticas de Seguridad Informática, da lugar a que la Entidad realice las investigaciones disciplinarias pertinentes y reportar a los entes de control del estado cuando haya lugar.  
   
7.     **DEFINICIONES**  
   
ACTIVO: Se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización.  
   
APLICACIONES CRITICAS: Son las aplicaciones o sistemas de información que reciben este término porque previamente se encuentran clasificados como vital o necesarias para el buen funcionamiento de los procesos y procedimientos misionales.  
   
BRECHA: Término que se utiliza para denominar la diferencia que se observa entre el mecanismo de seguridad que existe y la situación ideal para evitar que germinen vulnerabilidades que impacten el negocio de la Entidad.  
   
BUENAS PRACTICAS: Son lineamientos que contiene los principios básicos y generales para el desarrollo de los productos o servicios de la organización para la satisfacción al cliente.  
     
CICLO DE VIDA DE LA INFORMACIÓN DIGITAL: Se refiere a la clasificación y almacenamiento de la información; siendo necesario tener en cuenta los requisitos técnicos y legales; así como tener claro los conceptos de disponibilidad y velocidad que depende de la  misma clasificación que varía conforme su valor con el tiempo.  
   
CLASIFICACION DE LAS APLICACIONES: Las aplicaciones se clasifican conforme los procesos de la entidad y son: Misional, Estratégico y de Apoyo.  
    
CLASIFICACION DE LA INFORMACIÓN: Proceso formal que se utiliza para ubicar el nivel a la información  de la Entidad con el fin de protegerla; previa estructura de  valoración en atención al riesgo que se presume existe si hay una divulgación no autorizada. Generalmente la información debería clasificarse en relación a su valor, requisitos legales, sensibilidad y criticidad para la Organización.  
   
CLIENTES: Persona natural o usuario que recibe un producto Institucional. El cliente puede ser interno o externo a la organización.  
   
CONFIDENCIALIDAD: Acceso a la información por parte únicamente de quienes esté autorizado.

CORRIENTE ELECTRICA REGULADA: Se utiliza para regular o mantener el voltaje de la red eléctrica para que no afecte el funcionamiento de los recursos TIC de la Entidad.

DATO: Es una letra, número o símbolo que tiende a convertirse en información.  
   
DEPENDENCIAS: Son los grupos que conforman la estructura organizacional de la Entidad.

DOCUMENTO: Es el medio físico que contiene la información que se quiere transmitir.  
   
DUEÑO DE LA INFORMACIÓN: Es cualquier persona que es propietaria de la información y tiene la responsabilidad de custodiarla.  
   
INFORMACIÓN: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y que es guardada en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.  
   
INFORMACIÓN DIGITAL: Cuando la información está almacenada en un medio magnético porque cuando se imprime se convierte en documento físico y en este último caso existe en el SGC la dependencia que define los lineamientos, normas, guías y estándares.  
    
INTEGRIDAD: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

SERVICIO: Incluye los servicios profesionales para la instalación, mantenimiento, desarrollo, integración de software y adquisiciones, enajenaciones, arrendamientos y contratación de Hardware y soporte tanto de software como de hardware; así como de la Plataforma Tecnológica.

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 procedimientos, tanto automatizados como manuales.

 TIC: Conjunto de recursos, procedimientos y técnicas usadas en el procesamiento, almacenamiento y transmisión de información, en la actualidad no solo una computadora hace referencia al procesamiento de la información. Internet forma parte de ese procesamiento que, quizás, se realice de manera distribuida y remota.  
    
USUARIO: Persona que utiliza los recursos TIC y que interactúan de forma activa en un proceso, secuencia, código etc.

8.     **CONDICIONES GENERALES**

Los Directores Técnicos y Coordinadores de Grupos de Trabajo son los responsables de identificar y valorar su información; puesto que, son los propietarios de la información y el SGC es el responsable de protegerla.  Todos los servidores públicos deben seguir los lineamientos enmarcados en este documento.  
    
La seguridad de la información debe estar enmarcada con los siguientes principios:  
   
Confidencialidad, Integridad, Disponibilidad, Autenticidad, Legalidad, Confiabilidad De La Información.

**9.      POLÍTICAS**  
   
9.1 POLITICA DE SEGURIDAD

1. **PINTURAS INDUSTRIALE S LTDA** debe definir los mecanismos para proteger la información, su uso, procesamiento, almacenamiento, difusión; y, es su deber, mantener actualizada la presente política así como los demás componentes del Sistema de Gestión de la Seguridad de la Información que deben estar alineados con los demás sistemas de gestión de la Entidad.
2. El área de sistemas informáticos debe dar los lineamientos para clasificar, valorar y tratamiento de la información; así como, los recursos tecnológicos involucrados.
3. Todos los usuarios de los recursos TIC deben proteger, respaldar y evitar accesos de la información a personas no autorizadas; es decir son responsables de cuidar todos los activos digitales de información.
4. Todos los sistemas de información y recursos tecnológicos utilizados para el procesamiento deben contar con mecanismo de seguridad apropiados.
5. Todo usuario de TIC es responsable de la protección de la información a su cargo y no debe compartir, publicar o dejar a la vista, datos sensitivos como Usuario y Password, Direcciones IP entre otros.
6. Todo usuario de TIC debe bloquear la sesión de trabajo de su computador al alejarse aunque sea por poco tiempo.
7. Toda información que provenga de un archivo externo o que deba ser restaurado tiene que ser analizado con el antivirus.
8. Ningún usuario de los recursos TIC debe generar, compilar, copiar, almacenar, replicar o ejecutar código de computador malicioso con la intención de causar daño, afectar e interferir con los servicios.
9. Ningún funcionario debe brindar información no autorizada en ningún sitio ya sea interno o externo.
10. Se documentaran y divulgaran los controles que se deben aplicar para el uso adecuado de la información que se maneja en las oficinas desde el punto de vista laboral.
11. Los usuarios no deben descargar software de Internet bajo ninguna circunstancia y en caso de requerirlo debe informar al grupo de soporte de la Entidad.

**9.2 ORGANIZACIÓN**

1. **PINTURAS INDUSTRIALE S LTDA** debe tener el control de su información previa organización y administración conforme la definición de su marco gerencial (funciones y responsabilidades).
2. El área de sistemas informáticos debe elaborar los documentos que contenga los lineamientos, guías y procedimientos para organizar, clasificar y valorar la información.
3. Cada dependencia debe determinar cuál es su información sensible y su disponibilidad.
4. Todos los usuarios de los recursos TIC de la institución deben ubicar la información que necesita ser respaldada en los lugares previamente constituidos para ello; en caso contrario son responsables de sus actos y consecuencias.
5. La parte Jurídica debe verificar que en todos los contratos exista el compromiso de confidencialidad de la información.

**9.3CLASIFICACION** 

1. El área de sistemas informáticos debe documentar el procedimiento de Clasificación de la información, el cual debe prevalecer los principios de la información en las cuales se basa la seguridad como son confidencialidad, integridad y disponibilidad.
2. Todas las dependencias de **PINTURAS INDUSTRIALE S LTDA** deben clasificar la información y determinar su sensibilidad y criticidad.
3. Los propietarios de la información son los encargados de clasificar la información de acuerdo con su grado de sensibilidad y criticidad; así como de documentar y mantener actualizada la clasificación, los permisos de acceso a los sistemas de información.
4. Todos los propietarios de la información deben supervisar que en su dependencia se aplique el procedimiento previamente definido en la entidad para la clasificación de la información de su competencia.

**9.4 SEGURIDAD FISICA AMBIENTAL**

1. **PINTURAS INDUSTRIALE S LTDA** a través del Grupo de Servicios Administrativos debe garantizar la seguridad física en todas las sedes de la Entidad para prevenir e impedir accesos no autorizados, daños e interferencia a las sedes, instalaciones así como a la  información que recibe y genera.
2. Todos los recursos físicos inherentes a los sistemas de información del SGC como las instalaciones, equipos, cableado, expedientes, medios de almacenamiento, etc. deben estar protegidos.
3. Los recursos TIC utilizados para el procesamiento de la información deben ser ubicados en sitios estratégicos con  mecanismos de seguridad que permita controlar el acceso solo a las personas autorizadas e incluir en la protección de los mismos los traslados por motivos de mantenimiento u otros escenarios.
4. A través de las diferentes dependencias se debe identificar y garantizar el control de los aspectos ambientales que pueden llegar a interferir el correcto funcionamiento de los recursos tecnológicos inherentes en el procesamiento y almacenamiento de la información institucional.

**9.5 CONTINUIDAD DEL NEGOCIO**

1. La administración de Continuidad del Negocio debe ser parte integral del Plan de Administración de Riesgo del **PINTURAS INDUSTRIALE S LTDA**.
2. Los Directivos deben definir las pautas para el correcto análisis y evaluación de los riesgos de seguridad de la información así como identificar el nivel del impacto y gestionar las diferentes estrategias para el tratamiento de tal forma que garantice la continuidad e integridad de los sistemas de información del negocio de la Entidad.
3. Se debe documentar los procedimientos que contribuya a minimizar los efectos de las posibles interrupciones de las actividades normales de la Entidad (sean éstas resultado de desastres naturales, accidentales, fallas en el equipamiento, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.
4. Se debe analizar las consecuencias de la interrupción del servicio y tomar las medidas correspondientes para prevenir hechos similares en el futuro.
5. Se debe identificar las amenazas que puedan ocasionar interrupciones de los procesos y/o las actividades, así como evaluar los riesgos para determinar el impacto de dichas interrupciones e identificar los controles preventivos.
6. Se debe desarrollar un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de los sistemas y actividades del negocio.
7. Elaborar los planes de contingencia necesarios para garantizar la continuidad de las actividades del negocio.

 **10. ROLES Y RESPONSABILIDADES**

* 1. Direcciones o Áreas responsables de la Seguridad Informática

El área de sistemas informáticos, gestionado, conformado y respaldado por la Alta Dirección de la Empresa, es el responsable de establecer y mantener las Políticas de Seguridad Informática, las normas, directrices y procedimientos de la Organización.

Las siguientes son las principales responsabilidades a cargo del area de sistemas informáticos, dentro de la Entidad:

* Revisión y valoración de la Política de Seguridad Informática.
* Alineación e integración de la seguridad a los objetivos del negocio.
* Garantizar que la seguridad de la información forma parte integral del proceso de planeación estratégica de la organización.
* Establecer las funciones y responsabilidades específicas de seguridad de la información para la Empresa.
* Reportar, a través de reuniones semestrales a la Gerencia el estado de la seguridad y protección de la información en la Empresa y la necesidad de nuevos proyectos en temas de seguridad de la información
* Establecer y respaldar los programas de concientización de la Empresa en materia de seguridad y protección de la información
* Establecer, evaluar y aprobar el presupuesto designado para el tema de seguridad de la información
* Evaluar la adecuación, coordinación y la implementación de los controles de seguridad específicos para nuevos servicios o sistemas de información.
* Promover explícitamente el apoyo institucional a la seguridad de la información en toda la organización.
* Supervisar y controlar los cambios significativos en la exposición de los activos de información a las principales amenazas.
* Revisar y seguir los incidentes de seguridad de la información.

La investigación de incidentes de Seguridad Informática es responsabilidad del Jefe del Departamento de Sistemas.

Las medidas disciplinarias en respuesta a las violaciones de las normas de Seguridad Informática se adoptarán de acuerdo con los lineamientos establecidos en el Reglamento Interno de Trabajo de la Empresa.

**10.1.1. RESPONSABILIDADES DEL EMPLEADO**

Los empleados deben tomar conciencia de la importancia del establecimiento de la Política de Seguridad Informática, los procedimientos y la normatividad aplicable. Estas normas deben ser completamente entendidas y aplicadas en la cotidianidad de sus tareas.

Los empleados que sean responsables de la información deben establecer los medios que soporten la toma de decisiones con base en la información que se encuentre a su cargo.

Los empleados que sean responsables de la información deben establecer la clasificación que mejor refleje el carácter sensible, el valor crítico y la disponibilidad de cada tipo de información que se encuentre bajo su cuidado. Esta clasificación determinará el nivel de acceso a los empleados.

Los empleados, además de ser responsables de la información, serán también los encargados de administrarla. En consonancia con lo anterior serán responsables todos aquellos que manejen información en los computadores asignados para llevar a cabo sus actividades o que tengan acceso a cualquier aplicación o sistema que sirva de apoyo a sus tareas.

Son responsables por todas las actividades relacionadas con su identificación. La identificación no puede ser usada por otro individuo diferente a quien esta le fue otorgada. Los usuarios no deben permitir que otra persona realice labores bajo su identidad. De forma similar, los empleados y usuarios no deben realizar actividades bajo la identidad de alguien más. La utilización de los recursos informáticos por parte de terceras personas con conocimiento o consentimiento del usuario, o por su descuido o negligencia, lo hace responsable de los posibles daños que estas personas ocasionen a los equipos o a la propiedad de La Empresa. Los empleados responsables de la información deberán almacenarla, implementar los controles de acceso (para prevenir la divulgación no autorizada) y periódicamente hacer copias de respaldo y así evitar la pérdida de información crítica.

**10.2. MANEJO DE LA INFORMACION DE LA EMPRESA**

La Empresa usa controles de acceso y otras medidas de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información manejada por computadores y sistemas de información.

Para mantener estos objetivos La Empresa se reserva el derecho y la autoridad de:

1. Restringir o revocar los privilegios de cualquier usuario.

2. Inspeccionar, copiar, remover cualquier dato, programa u otro recurso que vaya en contra de los objetivos antes planteados.

3. Tomar cualquier medida necesaria para manejar y proteger los sistemas de información de La Empresa. Esta autoridad se puede ejercer con o sin conocimiento de los usuarios, bajo la responsabilidad del comité de seguridad siempre con el concurso de la Gerencia o de quién él delegue esta función.

4. La empresa controlara todo acceso a la información confidencial, con la empresa encargada de la seguridad informática, para que esta no sea copiada en discos extraíbles o memorias USB.

5. Los correos empresariales se verificaran constantemente, para comprobar que no se está filtrando información confidencial a otros usuarios que no pertenezcan a la empresa, o que sean detectados como sospechosos.

**10.3 SENSIBILIDAD Y CLASIFICACIÓN DE LA INFORMACIÓN**

La clasificación de la información constituye un elemento importante para la administración del riesgo, ya que determina la prioridad y el grado de protección requerido para cada tipo de información que repose en los sistemas informáticos.

La Compañía ha definido unos criterios para la clasificación de la información que reposa en la plataforma informática. Estos criterios establecen el nivel apropiado de protección para cada una de las categorías e informa a los empleados responsables de cualquier medida especial o tratamiento requerido. Toda la información del Sistema Informático debe estar clasificada dentro de los siguientes criterios:

**Confidencial:** Hace referencia a aquella información que solamente puede ser conocida y manejada por personal expresamente autorizado.

**De Uso Interno:** Información que puede ser de libre utilización por los empleados de la Empresa para llevar a cabo las actividades laborales.

**Pública:** Es aquella información que podrá ser utilizada o conocida por todos los empleados de la Empresa e, incluso, por terceros.