	PROCEDIMIENTO SOBRE LA SEGURIDAD DEL SISTEMA DE INFORMACION	Código: P.SI.001
		Fecha de actualización: 13-03-2012
		Versión: 01
		Página 1 de 7

1. OBJETIVO

Resguardar la información que es el objeto de mayor valor para una organización, independientemente del lugar en donde se encuentre registrada, en algún medio electrónico o físico

2. ALCANCE

Este procedimiento aplica a los funcionarios que pertenecen al proceso Sistemas de Información y las personas que prestan los servicios.

3. DEFINICIONES

3.1. SEGURIDAD INFORMÁTICA: Es un estado de cualquier tipo de información que nos indica que ese sistema está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo.

La seguridad informática se resume, por lo general, en cinco objetivos principales:

- Integridad: garantizar que los datos sean los que se supone que son
- Confidencialidad: asegurar que sólo los individuos autorizados tengan acceso a los recursos
- Disponibilidad: garantizar el correcto funcionamiento de los sistemas de información
- Evitar el rechazo: garantizar de que no pueda negar una operación realizada.
- Autenticación: asegurar que sólo los individuos autorizados tengan acceso a los recursos


3.2. MANIFIESTO: Es un documento legal, en el cual se visualiza la lista de la mercancía que constituye el cargamento del vehículo de transporte, por ese motivo es delicado la manipulación y se requiere de cierta autorización.

4. RESPONSABLES


Coordinador de Sistemas y Coordinador Aplicativo.

5. PROCEDIMIENTO


ACTIVIDAD	RESPONSABLE	DESCRIPCIÓN
RETIRO DE USUARIOS	Auxiliar de Gestión Humana	<ul style="list-style-type: none"> Enviar correo con la información del empleado que se retira de la compañía: número cédula, nombre completo y cargo desempeñado.
	Coordinador de Sistemas y/o Aplicativo	<ul style="list-style-type: none"> Realizar la cancelación de las cuentas de usuario, como correo, y el acceso a la red de la compañía. Realizar un cambio de estado Activo a Inactivo ya que los empleados no son eliminados de la Base

	PROCEDIMIENTO SOBRE LA SEGURIDAD DEL SISTEMA DE INFORMACION	Código: P.SI.001
		Fecha de actualización: 13-03-2012
		Versión: 01
		Página 2 de 7


ACTIVIDAD	RESPONSABLE	DESCRIPCIÓN
		<p>de Datos.</p> <ul style="list-style-type: none"> Solicitar al usuario el diligenciamiento del <i>formato "Acta de devolución de equipos de computo"</i> donde realiza la entrega del equipo, dispositivos y claves de acceso. Realizar un Backup y guardarlo en CD para entregar la información al jefe inmediato. Enviar correo a Gestión Humana informando el Paz y Salvo del usuario para que procedan con la liquidación de prestaciones sociales
MANIPULACIÓN DE MANIFIESTOS	Auxiliar de despachos	<ul style="list-style-type: none"> Al realizar el proceso de generación de manifiesto e impresión del mismo, el manifiesto es bloqueado automáticamente por el sistema, cualquier solicitud de modificación y/o activación debe ser informada a la Gerencia Operativa, Contabilidad y al departamento de Sistemas de Información vía correo electrónico. Tener en cuenta la clase de solicitud ya que si la modificación del manifiesto es por cambio de valores, anulación, cambio de origen o destino que implica alterar el valor ya generado, o el manifiesto ya ha sido contabilizado esta modificación también debe ser autorizada por el Departamento de contabilidad. Si el cambio es para reimpresión, modificación de orígenes que no altera valores generados y no se haya contabilizado el manifiesto esta debe realizarla con aprobación de la Gerencia Operativa. Notificar el cambio por correo, cuando se haya realizado
	Gerencia Operativa o Contadora	<ul style="list-style-type: none"> Autorizar dicha modificación vía correo electrónico.
	Sistemas de Información	<ul style="list-style-type: none"> Realizar la habilitación para la modificación del registro en la Base de Datos del Sistema, y es notificado vía correo electrónico para que el solicitante realice dicha modificación. Almacenar los cambios realizados a manifiestos los cuales son almacenados en una carpeta por Sistemas de Información
ACCESO A INTERNET	Sistemas de Información	<ul style="list-style-type: none"> Proporcionar el acceso a internet ya sea controlado o ilimitado a los usuarios de la compañía, solo bajo autorización de la Gerencia Administrativa. Este acceso controlado es requerido, para evitar que los empleados desvíen el objetivo de sus labores

	PROCEDIMIENTO SOBRE LA SEGURIDAD DEL SISTEMA DE INFORMACION	Código: P.SI.001
		Fecha de actualización: 13-03-2012
		Versión: 01
		Página 3 de 7


ACTIVIDAD	RESPONSABLE	DESCRIPCIÓN
		<p>diarias dentro de la compañía</p> <ul style="list-style-type: none"> Realizar el acceso cuando tenga la solicitud vía correo electrónico del usuario, la cual debe estar copiada a la Gerencia General, Nacional o Regional, enumerando las paginas, anexando los links y el motivo por el cual requiere este acceso. Todo Movimiento en la Red es monitoreado por una herramienta del Isa Server, el filtro para la salida a Internet.
CUENTAS DE USUARIO CREACIÓN	Sistemas de Información / Gestión Humana	<ul style="list-style-type: none"> Las cuentas de usuario se utilizan para autenticar, autorizar o denegar el acceso a recursos a usuarios individuales de una red y para auditar su actividad en la red. La solicitud de creación de cuentas de Usuario en el Sistema de información debe realizar el departamento de Gestión Humana. Después de recibir el correo de Gestión Humana, informando el nuevo empleado, el rol y la descripción del Cargo, se procede a crear el usuario en la Base de Datos de nuestro sistema de información y en el dominio de la compañía (acceso a Windows, Sistema de Trazabilidad, y Servidor de Correo), con sus respectivas claves de acceso y su login. Por correo se envía a Gestión Humana, la clave temporal y el usuario. la clave debe ser cambiada cuando ingrese al sistema, ya que la enviada es asignada temporalmente. A veces los usuarios olvidan sus contraseñas de acceso a sus cuentas de usuario local. La contraseña de un usuario se puede restablecer manualmente, ingresando al servidor de Dominio y a la Base de Datos del Sistema de Información contactando a <i>Sistemas de Información</i>. Cuando se asigna un equipo a un funcionario se debe documentar en el formato "<i>Asignación de equipos de computo</i>"
RESPALDO DE INFORMACION	Sistemas de Información	<ul style="list-style-type: none"> Realiza una copia de respaldo de toda la información es importante para la compañía, para así evitar perdida de información en caso de suceder algún percance o siniestro. Realizar una copia de seguridad para la información de los servidores de Base de Datos de nuestro sistema de tracking, el Sistema Operativo y Correos Electrónicos. Este respaldo es realizado todos los días en horas de la madrugada por una tarea programada, y es guardado en una partición de un servidor, que está

	PROCEDIMIENTO SOBRE LA SEGURIDAD DEL SISTEMA DE INFORMACION	Código: P.SI.001
		Fecha de actualización: 13-03-2012
		Versión: 01
		Página 4 de 7

ACTIVIDAD	RESPONSABLE	DESCRIPCIÓN
		<p>alojado en un Datacenter externo en la ciudad de Bogotá, de ahí es guardado en cintas mediante una tarea programada y almacenado en un lugar seguro tanto desde el punto de vista de sus requerimientos técnicos como humedad, temperatura, campos magnéticos, como de su seguridad física y lógica.</p> <p>No es de gran utilidad respaldar la información y dejar el respaldo conectado a la computadora donde potencialmente puede haber un ataque de cualquier índole que lo afecte.</p> <p>Es necesario probar la confiabilidad del sistema de respaldo no sólo para respaldar sino que también para recuperar. Hay sistemas de respaldo que aparentemente no tienen ninguna falla al generar el respaldo de la información pero que fallan completamente al recuperar estos datos al sistema informático. Esto depende de la efectividad y calidad del sistema que realiza el respaldo y la recuperación. Este proceso de recuperación se realiza cada determinado tiempo.</p> <p>Realiza copia de respaldo al servidor de Correo, pero solo a la Base de Datos, estructura y buzón de los gerentes de la compañía. los buzones de los usuarios son descargados directamente y guardados en el computador local.</p>
CAMBIO DE CONTRASEÑAS	Sistemas de Información	<ul style="list-style-type: none"> Para la seguridad de la compañía y de los usuarios, es necesario que los empleados con acceso a la red, realicen periódicamente el cambio de dichas claves, voluntario o exigido por el Departamento de Sistemas de Información. El proceso de <i>Sistemas de Información</i> enviara un mensaje y/o requerimiento global solicitando el cambio de estas; y cada usuario la realizara de acuerdo a unas políticas de Grupo de Seguridad expuestas en el <i>Procedimiento de "Uso Adecuado de los Sistemas de Información"</i>. Este control se lleva de acuerdo a políticas de Grupo creadas en Servidor del Dominio.
LICENCIAS	Sistemas de Información	<ul style="list-style-type: none"> Una licencia de software es un contrato entre el licenciante (distribuidor) y el licenciataria del programa informático (usuario consumidor /usuario profesional o empresa), para utilizar el software cumpliendo una serie de términos y condiciones establecidas dentro de sus cláusulas. <p>Las licencias de software pueden establecer entre otras cosas: la cesión de determinados derechos</p>

	PROCEDIMIENTO SOBRE LA SEGURIDAD DEL SISTEMA DE INFORMACION	Código: P.SI.001
		Fecha de actualización: 13-03-2012
		Versión: 01
		Página 5 de 7

ACTIVIDAD	RESPONSABLE	DESCRIPCIÓN
		<p>del propietario al usuario final sobre una o varias copias del programa informático, los límites en la responsabilidad por fallos, el plazo de cesión de los derechos, el ámbito geográfico de validez del contrato e incluso pueden establecer determinados compromisos del usuario final hacia el propietario, tales como la no cesión del programa a terceros o la no reinstalación del programa en equipos distintos al que se instaló originalmente.</p> <ul style="list-style-type: none"> • El Proceso de <i>Sistemas de Información</i> se encarga que todo software instalado de la compañía debe ser legal y además cumpliendo con los roles predeterminados. • Estas Licencias no son Impresas, se puede visualizar en la página de Microsoft https://www.microsoft.com/licensing/servicecenter/. Solo está permitido el uso de personal autorizado por la Gerencia Nacional del Departamento de Sistemas. • En la hoja de vida del equipo se colocara el numero de la licencia Windows
AUDITORIA EN LA RED		<ul style="list-style-type: none"> • La primera razón es para saber qué hardware tenemos instalado. Cuando compramos un equipo sabemos perfectamente lo que tiene, pero en las empresas es habitual que con el uso diario falle algo y se cambie un componente. Los cambios hacen que con el tiempo, el ordenador inicial que compramos no se parezca en mucho al que actualmente tenemos. Con un programa de auditoría se puede conocer el hardware que hay instalado lo que nos facilita la tarea a la hora de planear futuras ampliaciones o mejoras. <p>La seguridad no solo consiste en ver los programas que hay instalados. Un buen programa de auditoría permitirá monitorizar una red de ordenadores, de tal forma que podamos averiguar qué equipos forma parte de la red, qué usuarios tienen privilegios de acceso y ciertos parámetros de la configuración de la red. El conjunto de esta información es vital a la hora de proteger nuestros equipos de ataques informáticos y facilita la labor, ya que no hay que ir equipo a equipo mirando estos datos. La mayoría de los programas de auditoría permitirán conocer esta información desde un servidor centralizado.</p> <p>A través de este tipo programas se pueden</p>

	PROCEDIMIENTO SOBRE LA SEGURIDAD DEL SISTEMA DE INFORMACION	Código: P.SI.001
		Fecha de actualización: 13-03-2012
		Versión: 01
		Página 6 de 7


ACTIVIDAD	RESPONSABLE	DESCRIPCIÓN
		<p>encontrar procesos desconocidos, spyware, elementos malignos y peligros de todo tipo, que de otro modo seguramente pasaran desapercibidos en tu PC.</p> <p>Adicional se realizan escaneos programados con el Antivirus, para la detección de amenazas informáticas que puedan afectar un ordenador o la red de la compañía. Este realiza una tarea de actualización diaria.</p> <ul style="list-style-type: none"> • Todo cambio realizado en las operaciones del sistema son registrados en una bitácora y/o Logs de las operaciones; ya que debemos de tener trazabilidad en los movimientos • El infractor del Sistema de Información se enviado a descargos a Gestión Humana, quienes tomaran las sanciones respectivas de acuerdo a al Reglamento Interno de Trabajo.
MANTENIMIENTO DE EQUIPOS	Coordinador de Sistemas	<ul style="list-style-type: none"> • Cualquier salida de equipos deberá ser registrada en el <i>formato "Orden de salida"</i>. • Cada equipo debe tener su hoja de vida y en el <i>formato "Hoja de vida equipos"</i> se documenta el historial de modificaciones, actualizados o mantenimiento que se le realice a cada equipo. • Anualmente se debe realizar el Cronograma de mantenimiento de equipos adscritos o a cargo de Sistemas de Información y se documenta en el <i>formato "Cronograma de mantenimiento de equipos"</i>, con el fin de controlar su ejecución.

6. MEDIDAS EN SSOA

Todo tipo de autorizaciones y modificaciones son almacenadas en unidades de red, para evitar el uso del papel.

7. DOCUMENTOS DE REFERENCIA

No. aplica

	PROCEDIMIENTO SOBRE LA SEGURIDAD DEL SISTEMA DE INFORMACION	Código: P.SI.001
		Fecha de actualización: 13-03-2012
		Versión: 01
		Página 7 de 7

8. REGISTROS

- Acta de devolución de equipos de cómputo.
- Asignación de equipos de cómputo.
- Orden de salida
- Hoja de vida equipos
- Cronograma de mantenimiento de equipos

9. ANEXOS

No aplica

ELABORADO POR: _____ Firma: Coordinador de Sistemas	REVISADO POR: _____ Firma: Coordinador de Sistemas	APROBADO POR: _____ Firma: Gerente Nacional de Sistemas
---	--	---