	PROCEDIMIENTO	CÓDIGO: PRC-LOG-009
		VERSIÓN: 9
	IDENTIFICACION, CONTROL Y MANTENIMIENTO DE INSTALACIONES INFORMACION Y PERSONAS	FECHA: 21/DIC/2011

VERSIÓN NO.	FECHA	DESCRIPCIÓN BREVE
1	15/Ene/2004	Versión inicial.
2	20/Jun/2005	Inclusión de definiciones.
3	11/Jul/2007	Supresión de definiciones.
4	31/Ene/2008	Inclusión de formato de inspección de instalaciones y a procesos.
5	25/Nov/2008	Inclusión del control de cambios,
6	08/Jun/2010	Inclusión de flujograma.
7	14/Ene/2011	Inclusión de exigencia de identificación con foto para visitantes.
8	12/Dic/2011	Se modifica la periodicidad de los mantenimientos preventivos, se define responsable de eliminar huella digital en biométrico, se relaciona el listado de los dispositivos electrónicos, nuevos criterios para el resguardo y control del mapa de riesgos físicos “Sede Principal”.
9	21/Dic/2011	Se define responsable de “Control de Llaves”, y correspondencia recibida y entregada. Parámetros establecidos para garantizar la protección y resguardo de la información.

1. OBJETIVO:

Garantizar la seguridad física de las instalaciones por medio de la identificación, control y mantenimiento de las instalaciones, información , equipos electrónicos y correspondencia.

2. ALCANCE:

Aplica para todas las instalaciones en Sede Principal Bogotá.

RESPONSABLE: Jede de Tráfico y Seguridad.

3. DEFINICIONES:

4. CONDICIONES GENERALES:

Mecanismos de Control (Dispositivos electrónicos).

Transportes Vigia, cuenta con dispositivos electrónicos que permiten asegurar las instalaciones, procesos y personal.

Entre los dispositivos electrónicos se ubican los siguientes:

Listado de identificación y ubicación de los dispositivos electrónicos.

Nº DE ZONA	DISPOSITIVO ELECTRONICO	AREAS
1	Pánico fijo/inalámbrico.	Recepción.
2	Sabotaje.	N/A
3	Infrarrojo.	Tráfico y Seguridad.
4	Infrarrojo.	Tráfico y Seguridad/escaleras.
5	Infrarrojo/ magnético puerta cumplidos	Cumplidos.
6	Infrarrojo.	Cumplidos entrada.
7	Infrarrojo.	Cumplidos /entrada principal-escaleras
8	Magnético	Puerta entrada principal.
9	Infrarrojo.	parqueadero bodega 2
10	Infrarrojo.	parqueadero bodega 3
11	Magnético 2	Parqueadero puerta.
12	Infrarrojo.	Dirección carga seca.
13	Infrarrojo. 2	Tesorería - dirección proyectos.
14	Infrarrojo. 2	contabilidad gerencia piso 3
15	Infrarrojo. 2	Pasillo auditoria/hall entrada a gerencia.
16	Infrarrojo.	Oficina dirección HSEQ/hall gerencia 3 piso.
17	Infrarrojo.	hall recepción.
19	Infrarrojo.	operaciones niñeras
20	Infrarrojo. 2	Recursos humanos/facturación.
21	Infrarrojo. 2	Dirección técnica/subgerencia.
22	Infrarrojo.	Informática.
23	Infrarrojo.	Mantenimiento.
24 25	Infrarrojo. Cámara de Seguridad.	Hall de mantenimiento. Tráfico y Seguridad.

Control de acceso de visitantes /funcionarios.

ACTIVIDAD	DESCRIPCIÒN	RESPONSABLE	DOCUMENTO
	Cuando el personal visitantes/funcionario, se retire por finalización de labores o terminación de la visita realizada a cualquiera de las áreas debe: **1. VISITANTES** • Cada vez que un visitante ingrese a las instalaciones de la Empresa, la persona encargada de la recepción debe solicitarle un documento con foto		

Salida de Personal/ Visitantes y/o Elementos.	y entregarle un carné de identificación de visitante. Además debe anotar los datos del visitante tales como nombre, identificación, hora de llegada y salida y finalmente el nombre de la persona a quien visita (quien será el responsable del visitante durante su estancia en las instalaciones de la compañía), esta información se relaciona en un libro de control asignado para tal efecto. • Devolver ficha de ingreso para que le sea devuelto el documento de identificación • Registrar hora de salida. • Sin ninguna excepción el visitante debe ser acompañado por el funcionario hasta la recepción. • Para el ingreso los días en los que no hay atención al público debe ser con autorización directa del área a la cual se va a dirigir y teniendo en cuenta que se deben restringir al máximo cada una de las visitas. **2. FUNCIONARIOS.** • Cada vez que un funcionario salga de las instalaciones, debe realizar la marcación en el sensor biométrico cada ingreso y salida debe ser registrado. • Todo paquete que salga de las instalaciones debe ser inspeccionado en portería, si la persona (visitante y/o proveedor) retira elementos estos deben ir acompañados de la respectiva autorización de salida por una firma autorizada.	Guarda portería	Minuta de ingreso y salida de elementos
Asignación e ingreso al sistema biométrico de control de acceso	• Todo nuevo funcionario debe ser ingresado a la base de datos con la información completa verificando que esta concuerde con la que se encuentra en la hoja de vida, se deben hacer las pruebas correspondientes para verificar que la información se grabó adecuadamente y no se van a presentar inconvenientes en su utilización.	Recursos humanos, recepcionista	Software
Horarios de ingreso y salida	• Todo el personal de empleados sin excepción alguna deben ingresar por la puerta principal en un horario establecido de la 08:00 horas y la salida a las 18:00 horas siempre deben hacer el registro de ingreso este horario aplicara de lunes a viernes. • El día sábado el ingreso será por la puerta principal y todo el personal que labora deberá dejar registrado su ingreso y salida garantizando de esta manera el cumplimiento del horario.		

Acceso de puerta principal: El acceso del personal por esta puerta se controla mediante el citófono que es manejado por el colaborador que desempeña tareas en recepción, esta puerta además se encuentra dentro del área de supervisión de uno de los censores que es activado en horas de la noche. Las puertas restantes que son las de las bodegas únicamente se abren para el acceso de los vehículos de la empresa, es decir que no son usadas para que el personal ingrese a las instalaciones.

Acceso a las oficinas: Las puertas que permiten el ingreso a las oficinas en donde se desarrollan labores de gran riesgo permanentemente se encuentran cerradas a fin de evitar el ingreso de personal no autorizado o sospechoso.

FICHA DE IDENTIFICACION DE LOS VISITANTES.

Mientras los empleados de la Empresa permanezcan dentro de las instalaciones de las mismas, deben portar el correspondiente carné único de identificación visitantes, cuyo modelo es el siguiente:

FICHA DE IDENTIFICACION DE PERSONAL VIGIA. .

Mientras los empleados de la Empresa permanezcan dentro de las instalaciones de las mismas, deben portar el correspondiente carné único de identificación personal, cuyo modelo es el siguiente:

Sistemas de Seguridad en las instalaciones.

Control de los dispositivos de emergencia.

• **Extintores:** Transportes Vigía S.A.S tiene en sus instalaciones los extintores requeridos para un caso de emergencia disponibles para su uso ubicados en lugares estratégicos.

De tipo solkaflan actualmente están instalados dos uno de ello en el servidor y el otro en el área de mantenimiento. De acuerdo al programa de inspección de extintores se valida su vigencia y disponibilidad.

• **Sistema de alarma:** Transportes Vigía S.A.S tiene ubicado en sus instalaciones un sistema de alarma, que requiere un mantenimiento y control con el objetivo de asegurar su correcta funcionalidad en caso de emergencia.

Prueba de funcionalidad de la alarma: Los encargados de la manipulación del sistema de alarma quienes son las personas que conocen la clave y están previamente autorizados por la Dirección de la empresa deberán probar el sistema de alarma de manera periódica y aleatoria, para medición y trazabilidad estos resultados se registran en acta y si requiere plan de acción este se identifica en el formato creado para tal fin. El jefe de seguridad será el responsable de registrar, analizar y llevar la trazabilidad de medición para esta actividad.

Activación de la alarma: El personal de Tráfico y Seguridad deben activar el sistema de alarma diariamente, pero para ello es imprescindible revisar las áreas de protección de los censores a fin de que no hayan elementos que puedan activar involuntariamente el sistema, además de verificar que todas las zonas estén cerradas.

Desactivación de la alarma: Los encargados de Tráfico y Seguridad son igualmente los responsables de desactivar el sistema de alarma, deberán ingresar por la puerta principal al momento que el elemento emita los tonos indicadores de tiempo de entrada el personal ingresa la clave.

Entrenamiento de los empleados: Los empleados a los que se los asigna clave de manejo son entrenados previo al uso de los sistemas de alarma. Se les informa además de los cambios que se ejecutan a estas técnicas, por otro lado se realizan entrenamientos para la cancelación oportuna y adecuada de las activaciones accidentales.

Elicitadores: Las áreas protegidas son revisadas periódicamente para asegurar la inexistencia de artículos que posean movimiento que activen los detectores y causen falsas alarmas.

Usuarios con clave: Con el fin de mantener control sobre el manejo del sistema de alarma, las claves de activación y desactivación de este elemento la poseen de manera única el Gerente General de la empresa y el personal de seguridad, como se evidencia únicamente tres personas conocen la clave con el fin de no filtrar información y generar conductas delictivas con el manejo de esta misma.

Códigos: Las claves son usadas únicamente por el personas autorizado por Gerencia y estos no pueden ser cambiados si se carece de permisión de la dirección.Por seguridad periódicamente se le solicita al proveedor del sistema visita para efectuar cambios en las claves actuales.

Área del Servidor "Sistemas de Información": El servidor de sistemas está ubicado en el área de contabilidad, bajo llave, el acceso al manejo del equipo lo tiene exclusivamente la dirección general de la empresa y el proveedor de sistemas.

Programa de mantenimiento dispositivos electrónicos:

Si las revisiones periódicas que realizan los inspectores de seguridad o coordinador de tráfico o las pruebas de alarma evidencian que el sistema de alarma no trabaja apropiadamente se contacta de forma inmediata al proveedor del mantenimiento. De manera adicional el mantenimiento correctivos de los dispositivos electrónicos de seguridad se aplica cuando se requiera y el preventivo se realiza anualmente con proveedor certificado. El mantenimiento de central telefónica y comunicaciones internas es responsabilidad del proveedor seleccionado y calificado se encuentra contratada en la modalidad de outsourcing, por lo tanto, de existir algún problema con estos equipos, la reparación o reposición queda en manos de la empresa contratada para tal fin. El soporte técnico para el mantenimiento adecuado del servidor y los sistemas son realizado mínimo 1 vez cada 15 días por un proveedor de servicios del área, quien supervisa que el servidor no posea programas, elementos o documentos innecesarios que ocupen espacio o dificulte su fluidez, por otro lado el soporte técnico que brinda esta orientado a garantizar que los colaboradores cuenten con el equipo de Hardware y Software suficientes para la realización de la labor.

Control de Llaves:

Para asegurar el control de accesos a las diferentes áreas de la organización se define en el Listado de llaves en el cual se especifican los responsables de las llaves de cada área, el número de llaves existentes en las instalaciones físicas y la ubicación de la chapa correspondiente a cada una de las llaves. Para tal fin se ha dispuesto una caja control de llaves, solo tienen acceso la Subgerencia y Auditoria.

Condiciones generales del control de las llaves.

• La gerencia general aprueba quien debe tener llaves de las diferentes oficinas de la organización.

• El caja de las llaves reposará en el área responsable de supervisar su correspondiente control.

• El llavero maestro es responsabilidad del jefe del área de auditoría, y en el deben existir una copia de todas las llaves.

• Las llaves las deben mantener los responsables de las mismas y no deben ser prestadas.

• No se debe sacar duplicado de las llaves (original y/o copia) sin autorización previa del jefe del área de auditoría. Si se saca duplicado de una llave (original y/o copia), el jefe del área de auditoría debe hacer firmar el listado de Duplicados de llaves por la persona que recibe esta llave para su respectivo control.

• Todas las llaves de la organización, se identificarán por medio de un número impreso el cual se debe pegar en cada una de las llaves.

• La persona que pierda una llave, debe avisar al jefe del área de auditoría para gestionar el duplicado.

• Si por algún motivo se cambia una cerradura, se debe entregar una copia de esta al jefe del área de auditoría.

Control de huellas digitales.
El retiro de un funcionario de la organización se realiza asi:
El área de Recursos Humanos, es la responsable de eliminar la huella del personal retirado tan pronto le sea expedido el paz y salvo.

Revisión e inspección de instalaciones.

Revisión periódica de las instalaciones Físicas: el Inspector de Seguridad o coordinador de tráfico en conjunto con el área de hseq realizaran un recorrido de las instalaciones, revisando los puntos que se detallan en el formato FRM.LOG.10 “Inspección física de las instalaciones”, entre ellos encontramos funcionamiento de la central telefónica, estado de los extintores, seguridad y estado del tablero central de las llaves, sistema de alarma, etc., los responsables dejarán en el formato mencionado constancia escrita de las anomalías detectadas y/o elementos con el fin de realizar el ajuste, mantenimiento o reposición para conservar el correcto estado de las instalaciones y garantizar su integridad física e invulnerabilidad. Esta revisión se debe ejecutar de acuerdo a lo estipulado en el programa de inspecciones.

Inspecciones aleatorias a los procesos: Mensualmente junto a la realización de las inspecciones físicas a las se realizarán las inspecciones a aspectos o actividades de procesos, ya que los mismos se profundizan y verifican totalmente en los procesos de auditorías internas.

Seguridad de puertas y ventanas: Antes de programar la alarma el personal de Tráfico y Seguridad que son los últimos en salir deben asegurarse de que las puertas y ventanas estén cerradas perfectamente a fin de evitar el movimiento debido a diferentes causas y como consecuencia se active el sistema de alarma.

Protección y resguardo de la información.

El proveedor externo de sistemas de información realizará anualmente el mantenimiento

preventivo a los equipos de cómputo para asegurar su correcto estado a fin de minimizar la presencia de riesgos apoyándose en el registro FRM.LOG.12 Reporte de visita.
BACK UP.

Contabilidad: El back UP para el area contable se realiza diariamente desde el servidor destinado para esta area "UNO 50".

Es responsabilidad de cada funcionario realizar el back up de la información contenida de cada equipo asignado.
El back Up de cada equipo asignado se realizará de manera quincenal, la ubicación de esta información se realizará en la siguiente dirección:

"MI PC o en Equipo (si es windows 7) una carpeta del servidor llamada usuarios, alli debe crear una carpeta con el nombre de su cargo (ej B _AUXILIARCONTABLE) y utilizando los comandos copiar-pegar se realiza la copia de los archivos".

Es importante tener presente los siguientes parámetros:
•
No copiar ni fotos personales ni música (esto se borra).
Los archivos deben estar originalmente en el equipo y esta carpeta es solo para realizar copia.

• El nombre de los archivos no debe superar 20 caracteres que incluyen espacios, se sugiere no hacer uso de los siguientes caracteres para nombrar los archivos: @ ; ¨ Ç + , : " -.

El back Up de la información contenida en la red se realizara mensualmente, el control para registrar esta actividad se registrará en FRM.LOG.12 Reporte de visita.

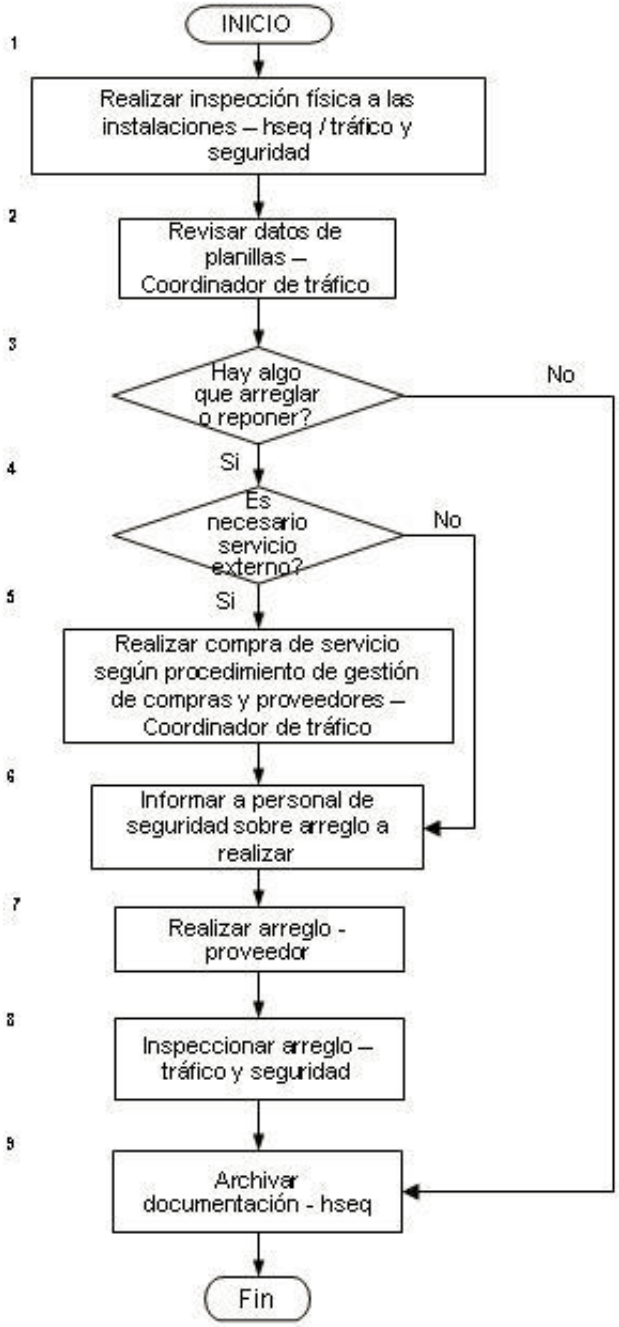
Planes de prevención: Es vital para la empresa conservar la estabilidad de sus instalaciones mediante la identificación de los elementos de control y su revisión periódica. El ingreso del personal debe ser controlado por recepción mediante el citófono y la solicitud de documentos para la ficha de ingreso. No permitir el ingreso de personal no autorizado a las oficinas de la empresa. No divulgue información confidencial de la empresa con personas no relacionadas con la compañía. Si no maneja la clave de activación y desactivación de la alarma no digite ningún numero en el teclado de esta, ya que podría ocasionar bloqueo del sistema. No mueva ni presione la llave de los extintores si no es necesario ya que podría generar una descomposición de este por golpes o fugas. No forcejee las chapas de puertas de acceso y caja de llaves.

Plan de contingencias: Es importante aclarar que los planes de contingencias se relacionan directamente con las actividades de reducción del riesgo. Para reaccionar ante los riesgos de la perdida e información se realizan diariamente las copias de seguridad. Frente a la activación de la alarma un colaborador de la empresa se comunica con las instalaciones para identificar las causas del evento. Ante el evento de intento o ejecución de robo, da aviso de inmediato a la policía de Mártires o a la CAI de policía de paloquemao, o se comunica con el frente de seguridad y defensa civil de paloquemao. Los números se encuentran constantemente actualizados en las carteleras y en recepción. Cuando se requiera evacuar rápidamente de las instalaciones la recepcionista inactiva el sistema electrónico de la puerta de ingreso y salida en las instalaciones como medida de seguridad con el propósito de que la evacuación se realice en un menor periodo de tiempo.

Señalizaciones, plano y mapa de riesgos: El plano que identifica las zonas sensibles o críticas de la

organización es controlado por el Jefe de Seguridad/Coordinador de SGI, este debe ser actualizado cuando las aéreas o dependencias de la organización se reubiquen en otras zonas diferentes. También tienen que estar debidamente señalizados los accesos restringidos y los elementos de seguridad como extintores y salidas rápidas.

DESCRIPCIÓN DE ACTIVIDADES



5. DOCUMENTOS DE REFERENCIA:

ELABORÓ		REVISÓ		APROBÓ	
Nombre:	Administrador del sistema	**Nombre:**	Mauricio Robayo Cardenas	**Nombre:**	Mauricio Robayo Cardenas
Cargo:	Coordinador Sistemas de información	**Cargo:**	DIRECTOR HSEQ	**Cargo:**	DIRECTOR HSEQ
Fecha:	21/Dic/2011	**Fecha:**	21/Dic/2011	**Fecha:**	21/Dic/2011