

1. INTRODUCCION

La seguridad es un proceso y como tal se ve sujeto a constantes cambios por su permanente dinamismo, debido a factores externos producto de la globalización, las leyes y exigencias aplicadas por las diferentes naciones en torno al comercio internacional y el creciente desarrollo tecnológico. Siempre se resuelven situaciones que aparentemente son sencillas, pero podrían presentar un riesgo de proporciones inimaginables o de alto impacto para la compañía. Para promover el desarrollo, la empresa se debe mover en un campo donde se requieren nuevos medios, nuevos métodos, nuevas técnicas y nuevas tecnologías.

El sistema de seguridad informática nace el 1 de Abril del año 2014, siendo gerente y actual director Juan Carlos Cardona, con la compra de tres nuevos equipos, uno como principal o gerencia, servicio de contabilidad y otro en ventas, son reutilizados dos computadores que venían inicialmente con la compañía, uno para administración y otro para el personal asesor, adicionalmente se crean dos puntos adicionales, pensando a futuro, Inicialmente fue de mayor interés el servicio prestado en la plataforma Windows 8.1 x64, de la empresa Microsoft el cableado estructurado completamente nuevo cumple con la norma internacional que rige para nuestro país Colombia, la EIA/TIA-568B (T568B), se autoriza el levantamiento inicial de los planos esquemático, físico, y geográfico, para regulaciones laborales y en cumplimiento de la ley 603 de 2000 la cual estipula que todas las empresas deben reportar en sus Informes Anuales de Gestión el cumplimiento de las normas de propiedad intelectual y derechos de autor, ubicación de los equipos, y la cantidad de medios informáticos facultando a la DIAN para supervisar el cumplimiento de estas leyes y a las Superintendencias para vigilar a las sociedades que sean sujetos de control.

Posteriormente se llamará “red los Califas” en conmemoración a su fundador.

2. OBJETIVOS

Objetivo General

El Plan de Seguridad Física y de la Información tiene como objetivo fundamental garantizar que se cumpla con los mínimos elementos y estándares de seguridad en la actividad de transportes especiales y sus procesos administrativos que requieren gran atención puesto que es el centro estratégico del proceso productivo de la empresa. De esta forma, se contribuye a la protección de la cadena de suministro y se hace prevención y administración de los riesgos durante las diferentes etapas de la prestación del servicio de transporte especial.

Específicos

- Implementar los protocolos y procedimientos de seguridad establecidos por la Gerencia.
- Mantener un ambiente de trabajo seguro.
- Incrementar la productividad.
- Prevenir actos delictivos.
- Disminuir el trámite administrativo ocasionado por reclamos (control de pérdidas y daños).

3. ALCANCE

El plan de seguridad física y de la información aplica para todos los procesos y servicios de la empresa.

4. GESTIÓN DE RIESGOS

a. Tratamiento del riesgo

El riesgo definido como la situación o evento que pueda afectar el desarrollo normal de las funciones de la entidad y el logro de sus objetivos¹, está asociado a medidas de control como: Prevención, protección, transferencia del riesgo y asumir el riesgo. Para la óptima gestión de riesgos, fundamentalmente debe hacerse una mezcla de los aspectos antes anotados.

Lo anterior, además de ser una buena práctica de seguridad que le ayudará a la protección y desarrollo del objeto social de la compañía permitirá tener elementos suficientes para negociar con las compañías aseguradoras, ya que en el cálculo de la prima de riesgo de un seguro influye el grado de implementación de las estrategias de mitigación o prevención.

Evitar la exposición a los riesgos es eliminar la posibilidad para que un riesgo ocurra, es tomar la decisión de eliminar una actividad, operación, implementar un control u acción.

En algunos casos es necesario cambiar completamente la forma o el procedimiento en que se viene desarrollando una actividad. Las medidas preventivas de seguridad son la estrategia que se debe seguir dentro de las operaciones de administración del riesgo.

b. Seguridad Física – Instalaciones

La protección física de instalaciones consiste en la aplicación de diversas medidas que se diseñan y se adoptan para preservar la instalación, incluyendo los bienes, materiales, documentos y personas que en ella se encuentran. Esta preservación está orientada con el propósito de evitar la destrucción total o parcial de la instalación, la intromisión de personas no autorizadas, la fuga de informaciones o documentos de vital interés, pérdida de objetos o materiales por efectos de robos y hurtos, acciones de sabotaje, etc.

Todas las medidas que se adopten deben ir unidas, enlazadas y coordinadas entre sí, quiere decir, que la seguridad física, debe ser un sistema integrado de protección.

Dependiendo del entorno, de los recursos y de los sistemas a proteger, se aplicarán y utilizarán en mayor o menor grado las medidas y mecanismos de prevención, detección y restricción.

¹ Norma Técnica de Calidad en la Gestión Pública NTC GP 1000:2009, Términos y Definiciones, pág. 14.

A continuación, se mencionan aspectos básicos de seguridad que permiten revisar las acciones de seguridad que debe tener implementadas la compañía y las medidas que se pueden tomar para hacer una excelente administración de los riesgos.

- **Perímetro:** Por ser la línea fronteriza que señala claramente el límite de la propiedad privada, goza de sistemas especiales de construcción que impide el paso de personas y/o vehículos desde y hacia el exterior de la compañía. Cuenta con un perímetro global de 1.200 m.
- **Muros:** Están contruidos en materiales compactos y resistentes, con el fin de prevenir o retardar el rompimiento ante una posible intrusión, su altura es de 3 metros
- **CCTV:** La empresa actualmente cuenta con un sistema CCTV, el cual permite el monitoreo permanente de las instalaciones el cual es revisado desde dispositivos móviles.
- **GPS:** se cuenta con sistema de GPS de última tecnología en cada vehículo lo cual garantiza la recuperación o alarma ante cualquier situación de riesgo.
- **Comunicaciones:** La empresa cuenta con líneas internas fijas y celulares que permiten la comunicación interna de manera permanente, además cada motorista cuenta con un plan corporativo lo cual le facilita estar en comunicación continua con lass dependencia administrativas.
- **Parqueadero:** Se cuenta con parqueaderos para visitantes y vehículos propios
- **Vehículos propios de la compañía:** Por ser parte de los activos de la compañía o por haber una responsabilidad frente a éstos, tienen la prioridad de asignación de espacios en zonas próximas a los edificios administrativos y los espacios están debidamente demarcados, señalizados y asignados.
- **Vehículos de Visitantes:** Los visitantes son por lo general proveedores y contratistas.

c. Instalaciones Administrativas

Son espacios de ingreso restringido, solo pueden acceder previa autorización del Gerente, Coordinador Comercial y de Mercadeo o personal administrativo, ya que en estas dependencias se encuentra información (física y sistematizada) que se considera un activo importante para la empresa.

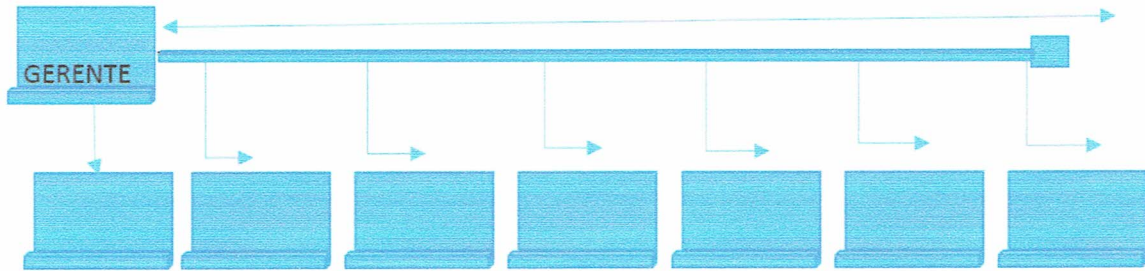
Frente a situaciones de emergencia la empresa cuenta con un Plan de Emergencia y Evacuación, indicando las responsabilidades y forma de actuar frente a cualquier situación de este tipo.

d. Seguros y control de llaves

Solo el personal autorizado tiene acceso a las llaves de las instalaciones de la empresa.

e. Seguridad para la información magnética

La distribución informática de la red “Los Califas” consta de un computador principal y siete terminales más, todos con comunicación directa al gerente, respaldo de datos, almacén masivo claves independientes, comunicación web, envío y recepción de datos externo.



Impresora en línea las 24 horas del día con recepción de datos y cola de impresión externos a través de un servidor basado en un sistema virtual Windows 7.

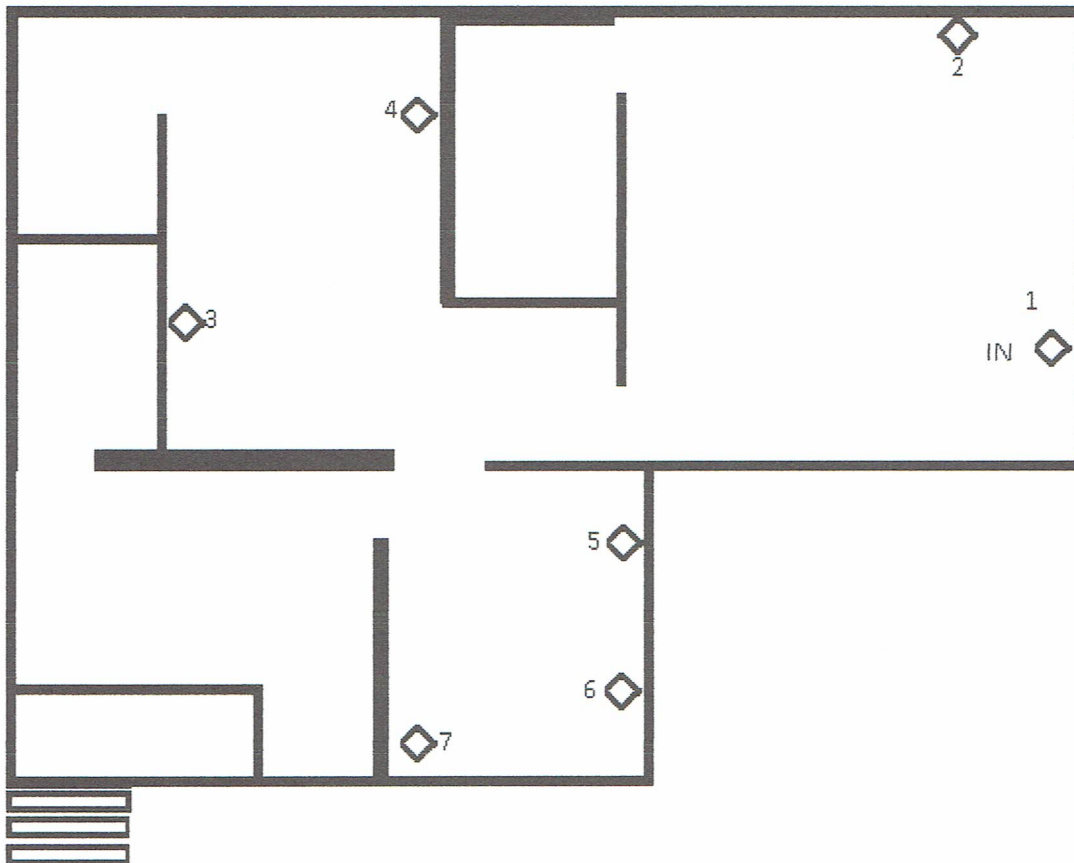
El detalle más importante es un banco de datos externo que también servirá de almacén masivo y respaldo de información crítica de la empresa.

Mantenimiento integral de la red y equipo mensualmente, aunque los equipos están expuestos a virus y contagios externos, el sistema se puede formatear independiente o totalmente.

Plano físico:

Para requerimientos laborales, contrato de terceros, o manejos externos se presentan físicamente los actuales puntos de conexión que posteriormente serán asignados a puestos de trabajo siendo el número uno (1) el computador de gerencia, dos (2) equipo audiovisual, tres (3) PC Ingeniería, cuatro (4) seguridad y Salud en el Trabajo, cinco (5) contabilidad, seis (6) Logística y Comercial, siete (7) personal Auxiliar Administrativo.

Las persona involucrada y reciban su asignación se les otorgara un nombre y una clave, personal e intransferible, y serán responsables de los datos y el cuidado de los mismos, teniendo especial cuidado en el manejo de medios extraíbles y su uso solo será autorizado por gerencia.



f. Sistemas de Control e identificación de empleados, visitantes y vehículos

La realización del control, entrega, devolución, cambio y pérdida de los dispositivos para el control de acceso para el personal vinculado visitantes se realiza de la siguiente manera:

El carnet de identificación se consolida como dispositivo de control de acceso para el personal vinculado a la compañía y para los visitantes a quienes se les deberá entregar un carnet de visitante al momento de ingresar a la empresa.

Entrega de Carnet a colaboradores

Cada que se contrata un nuevo funcionario a este se le entrega un carnet de identificación el cual deberá portar en un lugar visible con el fin de ser identificado con facilidad como funcionario de la compañía.

Entrega de Carnet a Visitantes

El personal de servicios varios entrega a los visitantes el carnet de identificación como visitante al momento del ingreso a las instalaciones, verificando previamente la autorización de acceso vía telefónica con el personal administrativo.

Perdida de Carnet

En caso de pérdida del carnet el funcionario deberá notificar por escrito a la compañía con el fin de tramitar un nuevo carnet de identificación y alertar a las partes interesadas sobre el caso de dicho documento perdido.

Devolución de Carnet

En caso de finalización de contrato el funcionario deberá entregar su carnet y dotación como requisito para la entrega de su paz y salvo para liquidación.

Cambio de carnet

En el caso de deterioro del carnet el funcionario deberá solicitar por escrito el cambio del mismo esta solicitud deberá estar acompañada de una fotografía vigente.

En caso de cambio de cargo la compañía deberá realizar el cambio de carnet del funcionario.


Los empleados deben conocer y transmitir a través de sus actuaciones al interior de la compañía las políticas en materia de seguridad adoptadas. Sin duda alguna las restricciones durante el control de acceso conllevarán a disminuir y eliminar riesgos de robo, tráfico ilícito, terrorismo y piratería entre otros.

El control se ejercerá por medio de carnet, y planillas de ingreso de visitantes, las cuales deberán ser verificadas por el personal de Servicios vario y/o auxiliares administrativos.

Seguridad con el personal

Cada dos años se realizan entrevistas y visitas domiciliarias al personal de la compañía, garantizando así la cercanía y el contacto permanente para poder evidenciar cualquier cambio en su comportamiento o estilo de vida, el personal encargado es el director de calidad y la Coordinadora Comercial y de mercadeo.

El personal es sometido a exámenes médicos ocupacionales anualmente.

	PROGRAMA DE SEGURIDAD FÍSICA Y DE LA INFORMACIÓN	Versión: 5 Fecha: 02 Ago 2017
---	---	----------------------------------

peatonal, zona de parqueo vehículos pesados y vehículos particulares, punto de encuentro en caso de emergencia teniendo en cuenta que fuera una zona abierta y segura.

También la señalización de los distintos lugares como zonas de mantenimiento que incluyen el taller, lámina y pintura, baños, oficinas y la implementación y reconocimiento de anuncios de la velocidad máxima permitida dentro de la instalación que es de 10 km.

Identificación y acciones frente personal no autorizado

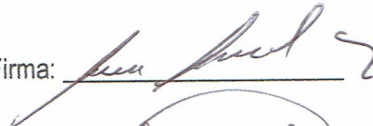
Cuando se realiza el proceso de identificación de personal y se detecta que no está autorizado para ingresar, el personal encargado debe:

- Restringir el ingreso del personal.
- Si se opone o muestran armas de fuego blancas o similares, no poner resistencia, permitir su ingreso y que los delincuentes se lleven lo que buscan.
- Tratar de recordar visualmente su rostro, placas del vehículo en el que se transportan y demás detalles que permitan su identificación (tatuajes, ropa, accesorios, etc.)
- Acudir a las autoridades pertinentes para reportar lo sucedido.
- Inspeccionar el recinto que fue vulnerado e identificar cual fue el objetivo del delincuente.
- Revisar las cámaras de video, y buscar almacenarlo de manera segura, para tener evidencias de lo sucedido.
- Acudir a la póliza del establecimiento para buscar el reconocimiento económico de lo que fue hurtado.

Control de cambios:

Se modifica el documento en general debido a solicitudes de ente certificador con respecto a requerimientos de PVP por parte de la empresa AES, se incluyen las operaciones de manejo de dispositivos de control de acceso (carnet), e incluye el control de acceso a peatones y vehículos visitantes. Se incluye el manejo de intrusión de personal no autorizado.

Documento modificado por: director de calidad: Jaime Quintero: Firma:



Documento revisado por: Gerencia: Juan Carlos Cardona: Firma:

