1. Propósito:

Identificar y gestionar los riesgos a los cuáles están expuestos los procesos de **COVITEC LTDA**., para preservar su confidencialidad y disponibilidad, utilizando para ello, un proceso sistemático que garantice un adecuado tratamiento de los riesgos e implementación futura de controles efectivos.

2. Alcance:

Inicia con la identificación de los procesos de Direccionamiento estratégico, cadena de valor y termina con el diseño de las estrategias para el tratamiento de los riesgos de cada uno de los procesos de la Organización.

3. METODOLOGÍA PARA GESTIÓN DE RIESGOS

DEFINICIONES

Actividad: Acción derivada de un proceso y un subproceso para generar un resultado

Amenaza: Es la causa potencial de un incidente, que puede producir daño a un sistema u organización. Cualquier circunstancia o evento con el potencial de afectar adversamente un activo.

Análisis del Riesgo: proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Compartir el Riesgo: forma del tratamiento del riesgo que implica la distribución pactada del riesgo con las otras partes.

Control: medida que modifica el riesgo.

Consecuencia: Resultado de un evento que afecta a los objetivos.

Descripción del Riesgo: Declaración estructurada del riesgo que usualmente contiene cuatro elementos: Fuentes, eventos, causas y consecuencias.

Evento: Ocurrencia o cambio de un conjunto particular de circunstancias.

Evitar el Riesgo: decisión informada de no involucrarse de una actividad o retirase de ella con el fin de no quedar expuesto a un riesgo particular.

Evaluación de los Riesgo: proceso de comparación con los resultados del análisis de riesgos, con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambas son aceptables o tolerantes.

Establecimiento del contexto: Definición de os parámetros internos y externos que se han de tomar en consideración cuando se gestiona el riesgo, y establecimiento del alcance y los criterios del riesgo para la política para la gestion del riesgo.

Contexto Externo o Interno: Ambiente en el cual la organización busca alcanzar sus objetivos.

Exposición: extensión hasta la cual una organización, una parte involucrada o ambas están sujetas a un evento.

Financiación del Riesgo: forma del tratamiento del riesgo que implica acuerdos contingentes para la provisión de fondos, para satisfacer o modificar las consecuencias financieras si se presentan.

Frecuencia: Numero de eventos o efectos por unidad de tiempo definida.

Gestion del Riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Nivel de Riesgo: magnitud de un riesgo o de una combinación de riesgo, expresada en términos de la combinación de las consecuencias y su posibilidad.

Monitoreo: verificación, supervisión, observación crítica o determinación continúa del estado del riesgo con el fin de identificar cambios del nivel de desempeño requerido o esperado.

Peligro: Una fuente de daño potencial

Pérdida: Cualquier consecuencia negativa o efecto adverso, financiero u otro..

Posibilidad: Oportunidad de que algo suceda

Prevención: acciones emprendidas para disminuir la posibilidad de ocurrencia de un evento.

Probabilidad: Medida de la oportunidad de ocurrencia expresada en número entre 0 y 1, en donde 0 es la imposibilidad y 1 es la certeza absoluta..

Proceso: Conjunto de actividades interrelacionadas o que interactúan, las cuales transforman elementos de entrada en resultados.

Programa: plan que especifica las actividades, responsabilidades y recursos necesarios para alcanzar un objetivo.

Protocolo: conjunto de documentos adscritos al desarrollo de un programa.

Retención del Riesgo: Aceptación del beneficio potencial de ganar, o de la carga de perder, provenientes de un riesgo particular

Reporte del Riesgo: Forma de comunicación destinada a informar a las partes involucradas internas y externas, proporcionando información relacionada con el estado del riesgo y su gestion.

Registro del Riesgo: Registro de la información acerca de los riesgos identificados.

Riesgo: Efecto de la incertidumbre sobre los objetivos.

Riesgo de Seguridad de la Información: Potencial de que una amenaza determinada aproveche las vulnerabilidades de un activo o grupo de activos y produzca daño a la organización.

Riesgo Residual: Riesgo remanente despues del tratamiento del riesgos.

Severidad: Es la interpretación del parámetro de peligrosidad y su nivel de aceptación.

Subproceso: es el nivel de proceso que agrupa un conjunto de actividades.

Tratamiento del Riesgo: proceso para modificar el riesgo.

Vulnerabilidad: propiedades intrínsecas de algo que resulta en la susceptibilidad a una fuente de riesgo que puede ocasionar un evento con una consecuencia.

DESCRIPCION:

1. Planificación de la seguridad.

La previsión es la primera acción a desarrollar y esta se desarrolla en una etapa de Planificación de la Gestión, que nos permite establecer la información necesaria a través de datos relevantes del pasado y del presente de las Organizaciones y de su forma de operación; de tal forma que se puedan identificar contextos sociales, políticos y tecnológicos, en los que se ha desenvuelto la seguridad, tanto en el mediano como en el largo plazo.

La planificación se desarrolla en cinco (5) etapas secuenciales para que se realicen con el mayor rigor. Las etapas son sucesivas y deben realizarse en un tiempo prudente para que la información de la etapa inicial si agregue valor a la siguiente.

Las etapas de la planificación son 1) análisis de riesgos, 2) evaluación de riesgos, 3) tratamiento de riesgos, 4) definición de la política de seguridad y 5) planteamiento de objetivos.

1.1 Análisis de Riesgos.

Es un proceso sistemático para entender la naturaleza del riesgo y establecer el nivel de riesgo. Este proceso comienza con la determinación del perfil de la Organización, es decir la identificación de la actividad económica principal y secundaria y el contexto en la que se desarrolla. En cada Organización se evidencian multiplicidad de riesgos, unos relacionados con el contexto, otros con la operación misma (responsabilidades), los hay asociados al medio ambiente, las personas y los bienes o propiedades, entre otros.

Para hacer un análisis de contexto de la Organización es preciso tener en cuenta dos variables principales: ***una externa***, que puede incluir desde las tendencias macroeconómicas, las decisiones políticas que afecten el negocio, etc y ***una interna*** que incluye el Plan estratégico. El análisis interno se hace teniendo en cuenta cinco (5) factores a saber:

- **Organización y plan Estratégico.** Estructura de funcionamiento existente para la generación de valor y la entrega del producto de la empresa. En este aparte es

importante entender la composición del organigrama formal e informal de la empresa, así como la cadena de valor y/o mapa de procesos existentes. Incluye Misión, visión, valores, políticas, objetivos y estrategias.

• **Infraestructura.** Distribución espacial, equipamiento, capacidad, estado y disponibilidad de las instalaciones propias o subcontratadas de la Organización.
• **Capitación.** Capacidad de aforo de las instalaciones, población permanente y flotante, tipología de personas –clientes, proveedores, empleados, visitantes, etc.

• **Entorno.** Ubicación geográfica, vecindad, bienes y servicios próximos a las instalaciones y/u operaciones de la Organización.

• **Historial de Incidentes.** Entendiéndose como la sumatoria de los eventos de seguridad que hayan sucedido en un periodo determinado de tiempo, habiéndose manifestado directamente en la empresa o que hayan afectado a las personas, instalaciones y/o procesos de la Cadena de suministro de la Organización.

Con estos 5 factores debidamente documentados, el analista está en capacidad de entender la Organización y su funcionamiento, así como de identificar los posibles ***escenarios de riesgo*** y estará listo para comenzar a hacer una interrelación con las ***amenazas*** a las que está asociada la operación de la empresa y podrá definir cuales se constituyen en riesgos estratégicos, cuáles operativos y cuales residuales.

Es ideal que el análisis se realice sobre ***todos los procesos*** de la Organización (incluyendo los que al parecer no tuvieran relación con la seguridad), pues hacer esta tarea en forma segmentada parcializa los datos obtenidos y el análisis resultará incompleto. No obstante, algunas organizaciones tienen avances en esta materia, obtenidos a través de su corredor de seguros, la auditoría interna o la contraloría (si la hubiere) y deben retomarse las conclusiones de estos informes como un insumo para comprender el trabajo previo y lograr la construcción de un mapa de riesgo que en efecto si corresponda a la realidad y que agregue verdadero valor.

Una vez realizadas las inspecciones, es posible observar el tiempo, modo y lugar de las instalaciones obteniendo así un listado preciso de las áreas que conforman la estructura de las instalaciones propiedad del Cliente, identificando las instalaciones físicas y su destinación, qué actividades se desarrollan allí y a qué línea de trabajo y procesos de la Organización están vinculados. Con esto se logra obtener la información necesaria que se consolida en un registro. (1er. Documento)

Acto seguido y habiendo obtenido la información básica de los escenarios, estos se asocian con riesgos de la actividad específica que desarrolla la Organización, los asociados con la concentración de personas y otros asociados al comportamiento de las

personas relacionados con los procesos de la Organización. Con este análisis de vulnerabilidad aplicado a cada uno de los grupos de instalaciones (sedes) permiten con facilidad el manejo de la clasificación y categorización por grupos de riesgo, se consolida en un registro. (2º Documento).

Una vez hecha la selección de escenarios y amenazas con el fin de identificar los ***controles*** existentes, así como determinar las posibles consecuencias y la posibilidad de ocurrencia- , el analista debe construir ***las escalas de valoración*** apropiadas para medir el nivel de ocurrencia convirtiendo una observación puramente cualitativa en unos parámetros que permitan una medición semicuantitativa y/o cuantitativa de esas percepciones.

Como punto de partida para el Análisis de vulnerabilidad se identifican las amenazas (especialmente las Naturales, Tecnológicas y Sociales) que sean inherentes al desarrollo de las actividades de Seguridad en las Organización y/o Cliente y que puedan afectar los recursos, desde el punto de vista de "frecuencia y severidad" para cada uno de los recursos (Físicos, operativos, humanos, ambientales, financiero y de imagen corporativa) de la Organización.

Para evaluar la probabilidad de que se materialice una amenaza y la gravedad de sus consecuencias, se deben definir ***Escalas de valoración relativas***, para cada uno de los recursos y / o procesos, con el fin de valorar hasta donde la Empresa está en capacidad de resistir o afrontar las consecuencias de la ocurrencia de un evento. (3er Documento).

Ante la dificultad de evaluar en forma exacta la frecuencia y severidad de las consecuencias de cada uno de los riesgos, en organizaciones que no poseen historial de incidentes, la metodología posibilita la definición de escalas de valoración relativas que se establecen acorde con el conocimiento que se tenga del proceso y del riesgo que se está evaluando. También se puede recurrir a las estadísticas o tablas de valoración, establecidas por normas e instituciones especializadas en cada uno de los riesgos.

Finalmente, se llega a la fase de ponderación y se presenta en una ***Matriz de vulnerabilidad,*** denominada ***Boston Box**** (4º. Documento) donde se califican la gravedad de la consecuencia de los siniestros; (desde Insignificante hasta Catastrófico). De igual forma se procede con las frecuencias de ocurrencia de los siniestros (desde Improbable hasta Constante).

1.2 Evaluación de Riesgos

El propósito de la evaluación del riesgo es tomar decisiones, basadas en los resultados del análisis del riesgo. Así la Organización establece sus escalas para valorar tanto las amenazas como los escenarios y la posible afectación que se derive de la manifestación

de una amenaza. Para esto el análisis previo (del contexto) fija una idea del estado (Tiempo, modo y lugar) en que se encuentra la Organización con respecto a sus amenazas y de cómo las contramedidas –en este caso de seguridad- se constituyen en una garantía o son parte de la intervención.

Los riesgos se clasifican en **especulativos y puros:**

Riesgos Especulativos: Son aquellos que permiten ganar o perder y están relacionados con la parte lucrativa u objeto del negocio.

Riesgos Puros: son aquellos en los cuales es posible únicamente perder, en esta clase de riesgos, a los que están más expuestos y se identifican en muchas oportunidades con los riesgos antisociales, como el hurto, el secuestro, la extorsión, la piratería terrestre y aérea, el narcotráfico, el terrorismo, el lavado de activos, los Actos Malintencionados de Terceros – AMIT, la asonada, la conmoción civil, entre otras.

Así el Riesgo (R) es la resultante de la combinación de dos medidas previas: Una de frecuencia (F) que es la medición del número de ocurrencia de eventos por unidad de tiempo que suceden en un escenario y otra que es la severidad (S) , generalmente conocida como impacto, que corresponde a la valoración del nivel de pérdida o de las consecuencias de un evento. Así la valoración de la Frecuencia (F) por la Severidad se traduce en un indicador de riesgo (R). = a:

FRECUENCIA X SEVERIDAD = GRADO DEL RIESGO

La Frecuencia se mide por el número de eventos que suceden en un sistema o una Organización en un periodo de tiempo, midiéndose de 1 a 6, con una escala de número de repeticiones en un período determinado de tiempo (Improbable, Remoto, Ocasional, Moderado, Frecuente y Constante)

La severidad se estima de diferentes formas: En el campo de las decisiones financieras, tales niveles, las escalas se dan en función de las pérdidas máximas probables en términos de dinero; en lo tocante a la operación en función de los días de suspensión de la producción o la prestación del servicio, en cuanto a seguridad física se toma como referente la afectación del evento a la estructura física de la Organización; en cuanto al medio ambiente en lo que se refiere al impacto que pudiere sufrir el ecosistema de la empresa por la manifestación del riesgo, en lo humano el referente básico es el número máximo de personas afectadas por la ocurrencia de un evento y en la información la pérdida de información sensible o estratégica.

Una vez obtenido el indicador de severidad en una escala de valoración de 1 a 4, la Organización define la aceptabilidad, la tolerancia y la intolerancia con respecto al riesgo

según su nivel (Insignificante, Marginal, Crítico y Catastrófico) y con esto se definen los métodos de tratamiento a que haya lugar y que estén determinados por la política de gestión definida por la Alta Dirección de la Organización.

1.3 Tratamiento de riesgos.

Si recurrimos a la NTC 31.000 las opciones de tratamiento para los riesgos que tienen resultados negativos (que son de los que nos ocupamos en Seguridad) son:

1) Evitar el riesgo, decidiendo no empezar, ni continuar con la actividad que origina el riesgo.
2) Reducir la posibilidad de la ocurrencia o repetición de resultados negativos, que se conocen comúnmente como **Prevenir**.
3) Cambiar las consecuencias para reducir la extensión de las pérdidas, mitigar el impacto que comúnmente se conoce como **Proteger.**
4) Cuando la Organización decide contratar, esto implica que otra parte o partes soporten o compartan parte del riesgo, preferiblemente con consentimiento mutuo, se conoce como **Compartir** y finalmente después de cambiar o compartir los riesgos, puede haber riesgos residuales que se asumen, lo cual sucede también cuando no se identifican adecuadamente, a esto se le conoce como **Retener.**

Una vez seleccionado el método de gestión apropiado para cada escenario de riesgo (escenario amenazado), es importante considerar los costos directos e indirectos así como los beneficios de su aplicación, para poder medir la efectividad de la decisión en términos de la rentabilidad del negocio.

La selección del tratamiento es el punto de partida para la construcción de un Plan de Seguridad que no es otra cosa, dentro de un Sistema de Gestión, que el plan de implantación de los controles (m x) aplicables a la seguridad de la Organización; que destaca y prioriza los controles más "importantes" y su forma de operarlos, articulados en formato de "programas".

El tratamiento de los riesgos requiere entonces que la Organización tenga claro el nivel de concienciación que debe lograr, a través de la capacitación, formación y entrenamiento de su gente, para que los programas y protocolos de seguridad se apliquen de forma sistemática y permanente, y así garantizar la ¨vida¨ del Plan en cada momento y con cada persona.

1.4 Definición de la Política de seguridad.

Una política de seguridad es la expresión de la Gerencia de una Organización de la decisión de adoptar un plan de acción para afrontar los riesgos de seguridad, que

enmarcan un conjunto de reglas para el mantenimiento de ese cierto nivel de seguridad necesario para la productividad. Pueden cubrir desde las buenas prácticas de seguridad en un solo proceso, hasta las directrices de seguridad de un país entero.

La política de seguridad es un documento de alto nivel que denota el compromiso de la gerencia con la seguridad de la Organización. Contiene la definición de la seguridad de física, industrial y de la información, sin embargo debe ser compatible con otras políticas y objetivos de seguridad, así como estar fácilmente accesible de forma que los empleados estén al tanto de su existencia y entiendan su contenido. Puede ser también un documento único o inserto en un manual de seguridad. Se debe designar un propietario que será el responsable de su mantenimiento y su actualización a cualquier cambio que se requiera.

1.5 Definición de objetivos

Los objetivos constituyen un elemento esencial en el éxito de un Plan, especialmente de seguridad. En muchas ocasiones la falta de definición de los objetivos hace fracasar un Plan, o simplemente porque las actividades planteadas no obedecen a un objetivo concreto. Los objetivos son el punto de partida para seleccionar, organizar y conducir los programas de seguridad y sus respectivos protocolos, además de que son la guía para determinar qué alcance tendrán los métodos de gestión de riesgo. En los objetivos se determinan los alcances de una actividad de prevención, protección y control y de paso permiten determinar (medir) cuál ha sido el progreso de Plan de Seguridad, facilitando a los agentes intervinientes la labor de determinar cuáles aspectos deben ser reforzados, evitando así inversiones en seguridad injustificadas y costosas, que se convierten en gastos para la Organización.

1.5.1 Tipos de objetivos. De acuerdo a los fines que se desean lograr, los objetivos pueden ser de mayor o menor amplitud y en cada caso existen procedimientos y recursos específicos para alcanzarlos.

La clasificación que se hace entre objetivos generales y específicos es relativa, ya que cada uno de ellos puede ser considerado como general o especifico según la forma como sean interpretados y de la relación que tengan con otros objetivos.

No debe confundirse a los objetivos con los resultados, puesto que un resultado puede ser un dato, pero un objetivo siempre significa un logro. Cuando los objetivos están bien formulados, ellos consiguen expresar el porqué, el para qué y el cómo del proyecto de investigación o desarrollo que estamos proponiendo.

Para lograr que los objetivos sinteticen tanta información y realmente consigan representar y organizar el trabajo en seguridad, hace falta tomar algunas precauciones:

• Verificar la relación con el escenario y la amenaza (el problema focal).

• Constatar la articulación entre los objetivos específicos y la meta a alcanzar.

Los objetivos expresan acciones que serán desarrolladas y por ello siempre se comienza su enunciado con un verbo en infinitivo. La elección del verbo adecuado es fundamental.

1.5.1.1 Nivel Estratégico. La planificación para la gestión del riesgo se da en una escala natural iniciando en el Nivel estratégico donde se plantea la Política de seguridad, que debe estar acorde con el plan estratégico y articulado con los objetivos de la Organización. Esa Política de seguridad se materializa en unos objetivos y estos a su vez derivan en el planteamiento de las estrategias (que son las formas de hacer operativos los objetivos)

Ejemplos:

POLITICA: Preservar a la Organización de la manifestación de riesgos sociales.

OBJETIVO: Prevenir delitos y contravenciones en las instalaciones de la Organización.

ESTRATEGIA: Implementar un programa de control de accesos.

1.5.1.2 Nivel Táctico. Véase numeral 1.3 de este procedimiento.

1.5.1.3 Nivel Operativo. El responsable de planificar las acciones operativas debe adoptar los programas que considere pertinentes, a saber:

Seguridad Pública: Coordinación y mantenimiento con las autoridades entre los Organismos de Seguridad del Estado (Fuerzas Militares, Policía, DAS, CTI) Organismos de Control (Inspección de Policía, Autoridades de Transito, Fiscalía, procuraduría, Contraloría, Personera) y los Organismos de Socorro y Asistencia Social (Comité Local de Atención de Desastres- CLOPAD, Bomberos, Defensa Civil Colombiana- DCC, Cruz Roja, Centro Regulador de Urgencias, Emergencias y Desastres- CRUE), a través de canales formales que se deben mantener de forma permanente.

Seguridad Perimetral: Actividad relacionada con la gestión de la seguridad del entorno de las instalaciones físicas de una organización, mediante la creación, liderazgo o vinculación a Frentes de Seguridad y Planes de Ayuda Mutua, además del monitoreo permanente del estado de sus barreras que definen el perímetro de las instalaciones.

Control de Accesos: Actividad que comprende el control de cualquier acceso a las instalaciones de la organización mediante la utilización de recursos humanos o tecnológicos. Su estructura de funcionamiento se representa para porterías y la operación se divide en control de accesos de personas (Operarios, Empleados, Usuarios, Funcionarios, Ejecutivo, Directivo, Visitante, Cliente, Invitado, Contratista, Proveedor), control de accesos de vehículos y control de accesos de mercancías (propietario, proveedor y cliente) las diferentes instalaciones de la empresa, exista o no servicio de vigilancia.

Vigilancia Humana: Servicio de seguridad humana prestado a una organización donde se debe definir con el cliente el esquema de funcionamiento, de la vigilancia fija y móvil (portero y rondero), además se deben elaborar protocolos de operación específicos para cada instalación acompañado de la definición de los responsables, los recursos asignados, documentos que aplican y modo de supervisión y auditoria. Este programa agrega valor en el control de accesos, ronda perimetral y oras actividades relacionadas con su servicio como la custodia de elementos, observación y contravigilancia, diligenciamiento de formatos, orientación de usuarios y verificación de información.

Medios Tecnológicos: Consiste en la utilización de todos los medios tecnológicos empleados para la seguridad de las personas e instalaciones, dependiendo de la política de seguridad que tenga la organización. Es el cliente quien debe definir el apalancamiento tecnológico aplicado a la seguridad asistido por sistemas de monitoreo de alarmas, y/o control de accesos y/o CCTV y/o nuevas tecnologías cuando apliquen. Deben elaborarse protocolos de operación y atención para estos sistemas, definir los responsables, recursos y documentos que aplican para el sistema. Entre estas encontramos las Radiotelecomunicaciones, Alarmas, Control de accesos, CCTV, Biometría y radiofrecuencia.

***Seguridad de las Personas*:** Consiste en suministrar un programa de sensibilización y orientación para el logro de conductas y hábitos seguros mediante la implementación de campañas y manuales de Autoprotección personal y familiar, seguridad del entorno y su lugar de trabajo (Charlas, capacitaciones, cultura de auto-cuidado, acompañamiento incidentes, acompañamiento clientes VIP, llamadas límite, escritorios limpios, etc.).

Atención de Incidentes Asociados al Servicio: Consiste en informar (contar) todo incidente (cualquier acción u omisión por actividad o comportamiento de personas, situaciones presentadas o por efectos de la naturaleza que ponga en peligro la seguridad de las personas, bienes o instalaciones de la organización, estas pueden ser también Intrusión, hurto simple, hurto calificado, hurto agravado, agresión física o verbal, coacción, retención de personas, conato de incendio, inundaciones, contaminación o actividades de descuido o similar) que sucede en los diferentes puntos de trabajo sin excepción, con el fin de que se asista, atienda, intervenga, estabilice e investigue en un

tiempo determinado y donde se debe contemplar un análisis de lecciones aprendidas. La intervención de estos incidentes es responsabilidad exclusiva del prestador del servicio, los cuales se les debe hacer seguimiento y tratamiento.

Aseguramiento de Procesos: Con este programa se debe estar en capacidad de generar aportes a la seguridad corporativa mediante la identificación, el análisis, evaluación, diseño, implantación y acompañamiento de procedimientos de seguridad para uno o varios procesos de la organización diferente al proceso de Seguridad Física, cuando se requiera.

Gestión de Eventos Críticos: Son aquellos dados como valor agregado al servicio y asociados con la integridad de las personas de la alta dirección (nivel de Directores) y la estabilidad operativa de las unidades de negocios, tales como, Secuestros, extorsiones a personas, accidentes de tránsito ,desaparición, homicidios retenciones ilegales, Incendio, catástrofes naturales cortes de suministros AMIT, Extorsión a la organización y amenazas terrorista.

Se debe desarrollar y operar un protocolo que contenga los procedimientos y niveles de asistencia, control, seguimiento y monitoreo de eventos críticos, donde se debe hacer acompañamiento, manejar la información y hacer seguimiento.

***Gestión de Emergencias*:** Este programa debe tener un protocolo que defina el alcance y la participación del componente humano de la seguridad física en la gestión de emergencia, evacuación, manejo, y recuperación de crisis en su etapa asistencial. Su objetivo es desarrollar estrategias para garantizar una gestión adecuada en el manejo de emergencias y la rehabilitación después de una crisis.

Continuidad del Negocio: En este programa, el servicio de Vigilancia Humana, debe contar con un protocolo de seguridad que contenga la lista de tareas acciones y responsabilidades de respuesta ante una crisis para asegurar las instalaciones, es decir el grado de participación que tiene el personal de seguridad física en caso de una catástrofe.

Cada programa puede contener una serie de protocolos individuales (por sede o instalación) y estos a sus vez se desagregan en actividades de seguridad, que se describen en forma secuencial, determinando los responsables, los recursos necesarios, los tiempos o momentos en que debe aplicarse o ejecutarse y de cómo operarán los encargados de las diferentes estaciones, puestos o centros donde la Organización tenga ¨seguridad¨.

Es preciso llamar la atención sobre que en seguridad la redacción de ¨consignas¨ se ha confundido tradicionalmente con las actividades de seguridad y en realidad son solo las

actividades que debe desarrollar el personal de vigilancia privada, lo que en resumen no constituye sino una parte de la seguridad de una Organización.

CONSIGNA: Controlar el ingreso, realizando la labor de identificación de personas, bienes y vehículos que soliciten permiso para el acceso al interior de las instalaciones de la Empresa, identificando a cada una de las personas que solicitan ingreso al área de parqueaderos

Vs.

ACTIVIDAD:

El guarda de seguridad debe identificar a cada persona que solicite el ingreso a las instalaciones de la empresa, solicitándole un documento de identificación que contenga los datos de nombre, número de identificación y preferiblemente que contenga una fotografía personal del solicitante.

Gestion de riesgos a procesos internos de la organización

La organización definió como herramienta para el análisis de riesgos de los procesos, una matriz de riesgos que contiene la siguiente informacion:

- Proceso
- Subproceso
- Actividad
- Objetivo estratégico
- Amenaza
- Fuente generadora de la amenaza
- Histórico de eventos sucedidos
- Definición de la probalidad de ocurrencia de la amenaza
- Descripción de la consecuencia, que define el nivel del riesgo.

Cada líder de proceso es responsable de actualizar permanentemente los riesgos de su proceso, darle tratamiento a los riesgos y medir la eficacia de esos controles. Ver matriz de riesgos por proceso (ISO 9001, planeación, gestion del riesgo).

Los procesos deben autoevaluarse frente a los riesgos identificados en su proceso y a la eficacia de los controles implementados.