

	SECAP LTDA.	Página	Página 1 de 18
		Versión	7
		Fecha de Aprobación	10/07/2012
		Fecha Última Actualización	24/02/2017
CÓDIGO: PR-07-06	GESTIÓN INTEGRAL DEL RIESGO		

1. OBJETIVO
2. ALCANCE
3. RESPONSABLE
4. DESARROLLO
5. ANEXOS

ELABORO	REVISO	APROBO
		
LAURA LAMPREA MARTÍNEZ Oficial de Cumplimiento	ROBERTO MOLINA C. Director Nacional de Operaciones y Seguridad	MARCELA MARTINEZ C. Gerente General

	SECAP LTDA.	Página	Página 2 de 18
		Versión	7
		Fecha de Aprobación	10/07/2012
		Fecha Última Actualización	24/02/2017
CÓDIGO: PR-07-06	GESTIÓN INTEGRAL DEL RIESGO		

1. OBJETIVO

Realizar e implementar en **SECAP LTDA.**, las políticas de gestión del riesgo, con el fin de mejorar la eficiencia y eficacia de la compañía para lograr Ser el aliado estratégico de Asesoría & Consultoría e Investigación en Seguridad Privada para satisfacer la necesidad de las empresas en los procesos de Selección y Seguridad. Y detectar los riesgos existentes dentro de la compañía, identificar su nivel y establecer métodos para medir el riesgo y su tratamiento, controlando, eliminando o trasladando los riesgos que puedan afectar al objetivo de la organización.

Proteger la organización para desarrollar la misión de la organización identificando los riesgos existentes que afectan la operación de la compañía y las amenazas latentes en cada etapa de la cadena de suministros.

2. ALCANCE

Este procedimiento es aplicable para los procesos de SECAP LTDA, dentro de los cuales se encuentran:

- Gestión Gerencial
- Sistemas de Gestión
- Direccionamiento estratégico
- Asesoría, consultoría en seguridad privada.
- Investigación.
- Gestión administrativa y financiera
- Gestión de Talento Humano
- Desarrollo y tecnología.

3. RESPONSABLES

- Líderes de procesos

4. DESARROLLO

4.1. CONTEXTO INTERNO Y EXTERNO

Para establecer el contexto interno y externo se tiene en cuenta la misión de la compañía y los objetivos de la misma detectando que factores internos y externos pueden afectar los objetivos de la razón social.

	SECAP LTDA.	Página	Página 3 de 18
		Versión	7
		Fecha de Aprobación	10/07/2012
		Fecha Última Actualización	24/02/2017
CÓDIGO: PR-07-06	GESTIÓN INTEGRAL DEL RIESGO		

La mejor forma de evaluar el riesgo y su incidencia en el normal desarrollo de las operaciones es destacando uno a uno los ítems dentro de la cadena de operaciones, creando estrategias para administrar el riesgo de forma efectiva y eficiente y así garantizar el normal funcionamiento de la operación y que el cliente final no se vea afectado.

De acuerdo a lo anterior premisa se tendrá en cuenta dentro del presente análisis las instalaciones, las personas, información y la operación.

En el contexto externo es importante tener en cuenta el ambiente social y cultural, político, legal, reglamentario, financiero, tecnológico, económico, natural y competitivo, bien sea internacional, nacional, regional o local.

En el contexto interno es el ambiente en donde la organización busca alcanzar sus objetivos como la organización de la compañía, las responsabilidades y funciones en los cargos, capital, procesos, personas.

4.2. IDENTIFICACIÓN DEL RIESGO

Se realiza una lista exhaustiva de riesgos que podrían crear, aumentar, prevenir, degradar o retrasar el logro del objetivo de cada proceso dentro de la compañía.

Para identificar los riesgos se hace un análisis periódico a cada proceso y una vez identificados, se describe de donde proviene el riesgo (fuente) y qué consecuencias puede generar a la operación.

4.3. ANALIZAR EL RIESGO

El análisis del riesgo medirá la frecuencia en que este ocurre a lo largo de 12 meses, para esto se tendrán en cuenta los siguientes rangos:

PROBABILIDAD	Frecuencia de que el riesgo se materialice	
VALOR/ESCALA	FRECUENCIA	DESCRIPCION
1	BAJA	Un caso entre 6 y 12 meses
2	MEDIA	Entre 1 y 5 casos entre 1 y 6 meses
3	ALTA	Más de 5 casos en el mes

Con base a esto se definirá la forma de proceder para controlar cada riesgo, para esto se tendrá en cuenta la causa y consecuencia de cada uno.

4.4. SEVERIDAD E IMPACTO

	SECAP LTDA.	Página	Página 4 de 18
		Versión	7
		Fecha de Aprobación	10/07/2012
		Fecha Última Actualización	24/02/2017
CÓDIGO: PR-07-06	GESTIÓN INTEGRAL DEL RIESGO		

Analizando la frecuencia de cada riesgo y teniendo en cuenta el nivel de impacto que este generaría en la Organización se procederá a describir el impacto en términos económicos, operacionales, e imagen de SECAP LTDA.

SEVERIDAD E IMPACTO				
VALOR	IMPACTO	DESCRIPCIÓN EN TÉRMINOS ECONÓMICOS	DESCRIPCIÓN EN TÉRMINOS OPERACIONALES	DESCRIPCIÓN EN TÉRMINOS DE IMAGEN
5	Leve	Pedidas hasta de \$ 1.000.000	Se interrumpe la operación menos de 4 horas	De conocimiento a nivel interno
10	Moderado	Perdidas entre \$ 1.000.000 y \$ 10.000.000 millones.	Se interrumpe la operación Hasta 1 día.	De conocimiento de un Cliente.
20	Grave	Perdidas entre \$10.000.000 y \$ 30.000.000 millones de pesos	Se interrumpe la operación Más de 1 día.	De conocimiento a nivel Nacional
40	Catastrófico	Pérdidas de más de \$30.000.000 millones de pesos	Se interrumpe la operación más de 2 días.	De conocimiento a nivel nacional e internacional

4.5.EVALUACIÓN DEL RIESGO

La evaluación de riesgo se genera para facilitar la toma de decisiones, para realizarla se va a comparar la probabilidad que se tiene de que un riesgo ocurra, la vulnerabilidad e impacto.

A continuación se detallan las escalas para la evaluación del riesgo:

PROBABILIDAD	Frecuencia de que el riesgo se materialice	
VALOR/ESCALA	FRECUENCIA	DESCRIPCION
1	BAJA	Un caso entre 6 y 12 meses
2	MEDIA	Entre 1 y 5 casos entre 1 y 6 meses
3	ALTA	Más de 5 casos en el mes

	SECAP LTDA.	Página	Página 5 de 18
		Versión	7
		Fecha de Aprobación	10/07/2012
		Fecha Última Actualización	24/02/2017
CÓDIGO: PR-07-06	GESTIÓN INTEGRAL DEL RIESGO		

VULNERABILIDAD		Debilidades en procesos, procedimientos, personal, instalaciones, sistema de seguridad, etc, que nos vuelve propensos a la materialización del riesgo.
1	BAJA	Los controles de seguridad establecidos y aplicados en la empresa son totalmente eficaces para evitar la materialización del riesgo.
2	MEDIO BAJA	Los controles de seguridad establecidos y aplicados son satisfactorios para evitar la materialización del riesgo
3	MEDIA	Los controles de seguridad establecidos y aplicados son mínimos para evitar la materialización del riesgo
4	ALTA	No se han establecido y aplican controles de seguridad para evitar la materialización del riesgo. Existen controles de seguridad establecidos y aplicados pero son ineficaces.

CONSECUENCIA (IMPACTO / DAÑO)		El impacto que puede ocasionar a la organización la materialización del riesgo. Pueden ser sociales, legales, económicas, físicas, operativa, etc.
5	LEVE	Las consecuencias son mínimas o casi nulas. Las consecuencias pueden ser asumidas por la organización sin ningún problema.
10	MODERADO	Con consecuencias para los bienes, la infraestructura, los documentos, la información, etc. (Afecta solamente un área de la organización).
20	GRAVE	Con consecuencias para gran parte de la empresa. Impacto legal medio. (Afecta los procesos y las actividades)
40	CATASTRÓFICO	Con consecuencias para las personas, bienes e instalaciones la empresa. Afectación al negocio, gran pérdida de valores de difícil recuperación, daño a las instalaciones, afectación a la imagen y reputación organizacional)

4.6. NIVEL DE RIESGO

La determinación del nivel de riesgo se realizará mediante la siguiente fórmula:

	SECAP LTDA.	Página	Página 6 de 18
		Versión	7
		Fecha de Aprobación	10/07/2012
		Fecha Última Actualización	24/02/2017
CÓDIGO: PR-07-06	GESTIÓN INTEGRAL DEL RIESGO		

Nivel de Riesgo = Probabilidad*Vulnerabilidad*Impacto

Posterior a ello, el resultado de esta fórmula determinará la magnitud del riesgo evaluado y así poder tomar acciones que permitan realizar el respectivo tratamiento. A continuación se detallan las escalas para determinar el nivel de riesgo:

NIVEL DE RIESGO		Mide el grado de aceptabilidad de un riesgo. Este ítem alerta sobre los riesgos que se consideran más importantes y a los cuales se les debe prestar mayor atención.
0 - 96	ACEPTABLE	Mantener el monitoreo sobre los controles establecidos para evitar la materialización del riesgo. Tomar acciones correctivas para los riesgos materializados.
97 - 193	TOLERABLE	Tomar acciones e implementar medidas de control para reducir el riesgo residual.
194 - 290	MODERADO	Implementar programas y medidas de seguridad, protección de activos y prevención de pérdidas. Tomar acciones para reducir el riesgo residual. Requiere la atención por parte de los líderes de procesos.
291 - 387	IMPORTANTE	Requiere atención por parte de las directivas. Tomar las acciones requeridas para reducir el riesgo residual. De aplicar se recomienda compartir los riesgos con la adquisición de pólizas de seguros.
388 - 484	INACEPTABLE	Requiere implementar medidas urgentes. Diseñar e implementar un Plan de continuidad del negocio puntual reducir el riesgo residual. De aplicar, eliminar la fuente/actividad que genera el riesgo.

4.7. TRATAMIENTO DEL RIESGO

Para realizar un tratamiento adecuado al riesgo es necesario seleccionar una o más opciones para modificar el riesgo esta selección se hacen equilibrando los costos y esfuerzo de la implementación frente a los beneficios derivados.

El tipo de tratamiento que se le dará al riesgo se hará de acuerdo al resultado del “Nivel de Riesgo” que se presente dentro del proceso, así:

) Aceptable-Tolerable, el riesgo se CONTROLARÁ

	SECAP LTDA.	Página	Página 7 de 18
		Versión	7
		Fecha de Aprobación	10/07/2012
		Fecha Última Actualización	24/02/2017
CÓDIGO: PR-07-06	GESTIÓN INTEGRAL DEL RIESGO		

-) Moderado, el riesgo se EVITARÁ
-) Importante e Inaceptable, el riesgo se ELIMINARÁ.

4.8. PLANES DE CONTINGENCIA

El manejo de la materialización del riesgo se llevara a cabo a través de planes de contingencia por proceso que se evidencian en la matriz (MT-05-02). Estos planes de contingencia tendrán sus responsables, controles y tratamiento dependiendo de la escala evaluativa anteriormente mencionada.

4.9. MONITOREO Y REVISIÓN

El monitoreo y la revisión de los riesgos será responsabilidad del proceso de Sistemas de Gestión, quien con la ayuda de los líderes de los procesos restantes monitorearan que los controles plasmados en la matriz de riesgo se estén cumpliendo, a su vez se revisaran los riesgos en caso de cualquier cambio operativo

4.10. CARGOS CRÍTICOS DENTRO DE LA OPERACIÓN

Para determinar la criticidad de los cargos dentro de las operaciones es necesario fijar criterios de seguridad como lo son:

-) Contacto con la información de la operación.
-) Acceso a información confidencial o sensible.
-) Posible modificación de información confidencial o sensible
-) Impacto de decisiones tomadas.
-) Impacto de mal manejo de la información

Los anteriores criterios se determinaron teniendo en cuenta La información como activo importante para la organización y para los clientes. La metodología que se utilizó para determinar los cargos críticos se encuentra descrita y calculada en la matriz de cargos críticos (MT-01-03)

4.11. CARGOS CRÍTICOS

De acuerdo a los parámetros enunciados anteriormente se determina que los cargos críticos de la empresa y que tienen injerencia directa con la operación son:

-) Gerente general.

	SECAP LTDA.	Página	Página 8 de 18
		Versión	7
		Fecha de Aprobación	10/07/2012
		Fecha Última Actualización	24/02/2017
CÓDIGO: PR-07-06	GESTIÓN INTEGRAL DEL RIESGO		

-) Director nacional de operaciones y seguridad
-) Jefe de operaciones
-) Líder de operaciones.
-) Referenciador académico y laboral
-) Consolidadores
-) Ejecutivo(a) de cuenta.
-) Asistente de operaciones.
-) Coordinador de visitas
-) Auxiliar Gestión Documental
-) Analista de Riesgo.
-) Coordinadora financiera
-) Asistente administrativo
-) Auxiliar de cartera y facturación
-) Jefe nacional de direccionamiento estratégico
-) Consultor comercial
-) Analista de Licitación
-) Analista de investigación
-) Coordinador de visitas
-) Coordinador de Selección
-) Psicólogo Junior

5. ANEXOS

5.1. ESTABLECIMIENTO DEL CONTEXTO:

SECAP LTDA. Se encuentra ubicada en calle 25 bis #31ª- 16, Barrio gran américa, estrato tres (3) perteneciente a la localidad de Teusaquillo.

De acuerdo a lo anterior premisa se tendrá en cuenta dentro del presente análisis las instalaciones, las personas y las operación.

Es necesario establecer el contexto en el cual se evidencian los factores de riesgo asociados al objeto social de la empresa, con el fin de desarrollar una gestión de riesgos acorde a las necesidades.

En el contexto externo es importante tener en cuenta el ambiente social y cultural, político, legal, reglamentario, financiero, tecnológico, económico, natural y competitivo, bien sea internacional, nacional, regional o local.

	SECAP LTDA.	Página	Página 9 de 18
		Versión	7
		Fecha de Aprobación	10/07/2012
		Fecha Última Actualización	24/02/2017
CÓDIGO: PR-07-06	GESTIÓN INTEGRAL DEL RIESGO		

En el contexto interno es el ambiente en donde la organización busca alcanzar sus objetivos.

ESTABLECIMIENTO DEL CONTEXTO		
AGENTE	CONTEXTO EXTERNO	CONTEXTO INTERNO
INTRUSIÓN VIOLENTA	X	
BLOQUE PUERTAS DE ACCESO	X	
FALLA DE COMUNICACIONES	X	X
INUNDACIÓN	X	
ROBO	X	X
SECUESTRO	X	
ABUSO DE AUTORIDAD		X
INFILTRACIÓN		X
PENETRACIÓN DEL PERSONAL		X
CONSPIRACIÓN INTERNA		X
PERDIDA DE INFORMACIÓN		X
TERREMOTO	X	
ASONADA	X	
ESPIONAJE INDUSTRIAL	X	
COMPETENCIA DESLEAL	X	
EXPLOSIÓN	X	
INCENDIO	X	X
FALLA EN EL FLUIDO ELÉCTRICO	X	
ACCIDENTE DE TRABAJO		X
ROTACIÓN DE PERSONAL		X
LAVADO DE ACTIVOS	X	
CORTE DE ENERGIA	X	X
SABOTAJE ELECTRONICO	X	X
CIBERATAQUE	X	

5.2. IDENTIFICACIÓN DEL RIESGO

IDENTIFICACIÓN DEL RIESGO		
RIESGOS	FUENTES DE RIESGO	CONSECUENCIA
TRANSITO DE PERSONAL POR LA COMPAÑÍA EN ÁREAS NO AUTORIZADAS	Personas	Perdida de información, robo, atentados.



SECAP LTDA.

Página

Página **10** de **18**

Versión

7

Fecha de
Aprobación

10/07/2012

Fecha Última
Actualización

24/02/2017

CÓDIGO: PR-07-06

GESTIÓN INTEGRAL DEL RIESGO

INGRESO DE PAQUETES SOSPECHOSOS	Personal interno y externo	Perdidas de paquetes
FALLA DE COMUNICACIONES INTERNAS	Personas. Herramientas de comunicación.	
FALLAS EN EL CTV	CCTV	Impunidad, no tener registro fotográfico.
MANIPULACIÓN INDEBIDA DE LA INFORMACIÓN	Personas	Pérdida de imagen y problemas legales.
EVALUACIÓN ERRADA DE LOS RIESGOS	Persona	Generación del riesgo
OMITIR REQUISITOS LEGALES PARA CON EL TRABAJADOR	Persona	Demandan laborales, indemnizaciones.
NO CUMPLIMIENTO DE OBLIGACIONES FISCALES	Persona	Multas y pérdida de imagen
EXTRAVIÓ DE LA INFORMACIÓN SECUESTRO	Personas ,archivo Persona	Fraude ,extorción Falta de gestión gerencial ,pérdida de vidas
FRAUDE DOCUMENTAL	Omitir controles de verificación en los documentos	Pérdida de imagen
LAVADO DE ACTIVOS	Selección de asociado de negocios	Pérdida de imagen, sanciones y problemas legales.
HACKEO DE CUENTAS BANCARIAS	Control de las cuentas bancarias	Perdidas económicas del patrimonio de la compañía
ALTERACIÓN DE CORREOS ELECTRÓNICOS	Jefe De Operaciones	No realización del estudio de seguridad ,mala imagen de la compañía
MANIPULACIÓN INDEBIDA DE LA INFORMACIÓN DEL CANDIDATO	Toda persona que tiene contacto con la información del candidato	Fraude Documental, pérdida de imagen y credibilidad
PERDIDA INTERNA DE LA INFORMACIÓN	Toda persona que tiene contacto con la información del candidato	Fraude documenta

	SECAP LTDA.	Página	Página 11 de 18
		Versión	7
		Fecha de Aprobación	10/07/2012
		Fecha Última Actualización	24/02/2017
CÓDIGO: PR-07-06	GESTIÓN INTEGRAL DEL RIESGO		

ERROR EN LA VERIFICACION DE ANTECEDENTES	Gerente de seguridad y operaciones	Perdida de cliente ,imagen y credibilidad
SELECCIÓN ERRÓNEA DE CLIENTES	Jefe nacional de mercadeo y servicios	Lavado de activos ,competencia desleal
CIBERATAQUE	Personas que tienen acceso a la seguridad informática de la información	Perdida de información

5.3. RIESGO PARA LAS INSTALACIONES

Se determina que el riesgo para las instalaciones se encuentra enmarcado y clasificado de acuerdo a su grado de vulnerabilidad así:

SEGURIDAD DE LAS INSTALACIONES					
RIESGO	P	C	P XC	EVALUACIÓN	TRATAMIENTO
INTRUSIÓN VIOLENTA	1	5	5	Aceptable	Prevenir
BLOQUEO DEL ACCESO A LAS INSTALACIONES	1	5	5	Aceptable	Prevenir
INUNDACIÓN	2	10	20	Tolerable	Prevenir, Proteger
TERREMOTO	1	5	5	Aceptable	Prevenir
ASONADA	1	5	5	Aceptable	Proteger

-) Inundación
-) Terremoto
-) Asonada
-) Bloqueo del Acceso a las Instalaciones
-) Intrusión violenta

5.4. ADMINISTRACIÓN DE RIESGO DE LAS INSTALACIONES

Con el fin de gestionar los riesgos en las instalaciones es necesario tener en cuenta, algunas medidas que ayudan a administrar el riesgo y no dejar que su escala de incidencia sea mayor al que actualmente se tiene.

	SECAP LTDA.	Página	Página 12 de 18
		Versión	7
		Fecha de Aprobación	10/07/2012
		Fecha Última Actualización	24/02/2017
CÓDIGO: PR-07-06	GESTIÓN INTEGRAL DEL RIESGO		

- ✓ Se tiene un encerramiento perimetral.
- ✓ Establecer un plan de emergencia y realizar simulacros por lo menos una vez cada seis meses.
- ✓ Se cuenta con un sistema de alarma monitoreado por **TELESENTINEL**, la cual posee unidades motorizadas de reacción inmediata y se encuentra comunicada directamente con la Policía Nacional.
- ✓ Se tiene en el ingreso a las instalaciones un bloqueo en la puerta principal por un electroimán el cual se deshabilita por parte de la recepcionista, previa identificación de la persona que solicita el ingreso a las instalaciones.
- ✓ En el segundo piso se tiene en el ingreso a las instalaciones un bloqueo por cantonera electromagnética.
- ✓ Se cuenta con una vigilancia comunitaria, cuya caseta de vigilancia está ubicada en diagonal a la entrada principal.
- ✓ En el momento de abrirse la puerta para el acceso del personal a laborar, la persona designada por la Gerencia General (Jefe Nacional de Operaciones), debe estar acompañada por uno o dos funcionarios más.
- ✓ Al cerrarse las instalaciones, una vez el personal salga de las instalaciones, la persona designada por la Gerencia General (Jefe Nacional de Operaciones), lo hará estando acompañada por uno o dos funcionarios.

5.5. RIESGO PARA LAS PERSONAS

Se determina que el riesgo para las personas se encuentra enmarcado y clasificado de acuerdo a su grado de vulnerabilidad así:

SEGURIDAD DE PERSONAS					
RIESGO	P	C	P XC	EVALUACIÓN	TRATAMIENTO
SECUESTRO	1	3	3	Aceptable	Prevenir
ROBO	2	5	10	Aceptable	Prevenir
ABUSO DE AUTORIDAD	1	5	5	Tolerable	Prevenir, Proteger

	SECAP LTDA.	Página	Página 13 de 18
		Versión	7
		Fecha de Aprobación	10/07/2012
		Fecha Última Actualización	24/02/2017
CÓDIGO: PR-07-06	GESTIÓN INTEGRAL DEL RIESGO		

-)] Robo.
-)] Abuso de Autoridad.
-)] Secuestro.

5.6. ADMINISTRACIÓN DE RIESGOS PARA LAS PERSONAS

Con el fin de gestionar los riesgos en las personas es necesario tener en cuenta, algunas medidas que ayudan a administrar el riesgo y no dejar que su escala de incidencia sea mayor al que actualmente se tiene.

-)] Se realizan capacitaciones relacionadas con la Cultura de Seguridad.
-)] Se realizan charlas de capacitación y entrenamiento en seguridad de personal.
-)] Se tiene en el ingreso a las instalaciones y al área de operaciones restringido y controlado.
-)] Se implementa un sistema para el control de los visitantes en la recepción del primer piso de la empresa.
-)] El acceso al segundo piso y el área de oficinas es restringido, para el personal de visitantes **(SOLO CON AUTORIZACIÓN)**.
-)] No se entrega la nómina del personal en efectivo, para lo anterior cada funcionario posee una cuenta bancaria a la cual se transfiere el valor mensual de la nómina.
-)] Realización de estudio de seguridad al personal de la empresa que se encuentra vinculado con contrato a término fijo, indefinido o prestación de servicios.

5.7. RIESGO PARA LA OPERACIÓN

De acuerdo al anterior cuadro se determina que el riesgo para la operación se encuentra enmarcado y clasificado de acuerdo a su grado de vulnerabilidad así:

SEGURIDAD DE LA OPERACIÓN			
RIESGO	VALORACION	IMPACTO	TRATAMIENTO
FALLA EN LA COMUNICACIÓN	10	leve	Prevenir, Proteger

	SECAP LTDA.	Página	Página 14 de 18
		Versión	7
		Fecha de Aprobación	10/07/2012
		Fecha Última Actualización	24/02/2017
CÓDIGO: PR-07-06	GESTIÓN INTEGRAL DEL RIESGO		

PERDIDA DE INFORMACIÓN	40	severo	Prevenir
DIFUSION DE INFORMACION CONFIDENCIAL.	20	Tolerable	Prevenir, Proteger
CONSPIRACIÓN INTERNA	20	Tolerable	Evitar, Prevenir
DESTRUCCION TOTAL DE LOS ELEMENTO DE TRABAJO	20	Severo	Transferir

-) Falla en la comunicación
-) Pérdida de Información
-) Conspiración interna
-) Infiltración
-) Destrucción total de los elementos de trabajo.

5.8. ADMINISTRACIÓN DEL RIESGO PARA LA OPERACIÓN

Con el fin de administrar los riesgos en la operación es necesario tener en cuenta, algunas medidas que ayudan a minimizar el riesgo y no dejar que su escala de incidencia sea mayor al que actualmente se administra.

- ✓ El acceso al cuarto de comunicaciones y servidor de internet solamente podrá realizar previa autorización de la Gerencia Nacional de Operaciones y Seguridad, siempre la persona que debe realizar trabajos en esta área será acompañado por algún funcionario designado por la misma Gerencia.
- ✓ La información que se trabaja en la compañía no se encuentra concentrada en una sola persona, la información se encuentra diseminada en 3 o más funcionarios.
- ✓ No se permita la salida de información en elementos grabación externa o propia de los funcionarios.
- ✓ No se permite el manejo de elementos ajenos a la operación en las áreas de trabajo, con el fin de evitar daños y/o deterioro de las órdenes de trabajo y los formatos de estudios de seguridad de personal.
- ✓ Las órdenes de trabajo enviadas por correo electrónico deben coincidir con los documentos físicos enviados.

	SECAP LTDA.	Página	Página 15 de 18
		Versión	7
		Fecha de Aprobación	10/07/2012
		Fecha Última Actualización	24/02/2017
CÓDIGO: PR-07-06	GESTIÓN INTEGRAL DEL RIESGO		

- ✓ El archivo y manipulación de la información está a cargo del proceso de Gestión documental.
- ✓ La información de antecedentes es solicitada a los agentes y fuentes de consulta por una persona destacada por la Gerencia General, quien a su vez recibirá la información para la difusión a las compañías y la verificación en páginas públicas es delegada a una investigación especializada en este tipo de temas.
- ✓ Realizar campañas con el personal de la compañía a todos los niveles operativos y administrativos con el fin de generar sentido de pertenencia.
- ✓ Mantener vigentes las pólizas de cubrimiento de las instalaciones y equipos de la sedes.

5.9. CONTINUIDAD DE LA OPERACIÓN:

- ✓ En caso de que exista falla de electricidad o fallas en los medios de comunicación se tendrán lugares alternos y equipos alternos para realizar las diferentes actividades que afecten esta amenaza.
- ✓ En caso de pérdida de la información se realizará la trazabilidad al documento en el transcurso del proceso para detectar el lugar de pérdida del documento y proceder a la búsqueda. En caso de que el documento se procederá a la adquisición nuevamente de la documentación y la sanción del directo responsable, ejecutando el acuerdo de confidencialidad y protección de la información.
- ✓ En caso de que se difunda a terceros no autorizados, información confidencial se debe proceder a la recuperación de la información difundida e iniciar frente al responsable las acciones pertinentes de

	SECAP LTDA.	Página	Página 16 de 18
		Versión	7
		Fecha de Aprobación	10/07/2012
		Fecha Última Actualización	24/02/2017
CÓDIGO: PR-07-06	GESTIÓN INTEGRAL DEL RIESGO		

acuerdo a la ley de protección de datos personales y acuerdo de confidencialidad firmado con la compañía.

- ✓ La conspiración interna
- ✓ La destrucción total de los elementos de trabajo será controlada con la continuidad de las operaciones en sedes alternas a nivel nacional las cuales apoyaran la operación y en la ciudad de Bogotá se tendrá un lugar alterno propiedad de la compañía ubicada en el barrio Ciudad Montes, en el cual se realizando la producción en su normalidad.

6. COMUNICACIÓN

El objetivo de la comunicación en la gestión integral del riesgo es la participación y diálogo entre los miembros de SECAP LTDA, esto con el fin de facilitar la identificación de riesgos y la implementación de medidas preventivas, correctivas y de mejora en la seguridad y control de la cadena de suministros como también en las condiciones de trabajo.

Cualquier miembro de SECAP LTDA, ya sea personal fijo, trabajadores free lance o asociados de negocio, podrá comunicar por escrito los nuevos factores de riesgo que se identifiquen, así como las propuestas para el mejoramiento continuo que crea pertinentes.

Cuando el personal fijo, trabajadores free lance o asociados de negocio quieran comunicar un factor de riesgo o manifestar una oportunidad de mejora en cuanto a los controles establecidos, deberá solicitar y diligenciar el registro RG-01-22. El periodo de respuesta para la estandarización del riesgo será de una semana.

El registro “**COMUNICACIÓN DE RIESGOS Y OPORTUNIDADES DE MEJORA**” se encuentra disponible en el proceso de direccionamiento estratégico en el área de sistemas de gestión; una vez realizado el registro los encargados del sistema de gestión ayudaran a la caracterización y valoración del riesgo como también se definirán e implementaran las medidas de control empleadas con el fin de mitigar la materialización de riesgos.

Si el riesgo encontrado hace referencia a las condiciones de trabajo el sistema de seguridad y salud en el trabajo se expondrá en las reuniones mensuales que lidera el COOPASST. Para asegurar el seguimiento de los comunicados y el análisis de lo identificado, se informará a la organización los resultados y las conclusiones de mencionada reunión.

6.1 DEFINICIONES y RESPONSABILIDADES

Comunicador: Cualquier miembro o asociado de la organización que identifique un factor de riesgo o que establezca una oportunidad para mejorar cualquier aspecto relacionado con el

	SECAP LTDA.	Página	Página 17 de 18
		Versión	7
		Fecha de Aprobación	10/07/2012
		Fecha Última Actualización	24/02/2017
CÓDIGO: PR-07-06	GESTIÓN INTEGRAL DEL RIESGO		

control y la seguridad de la cadena de suministros o las condiciones de trabajo en la organización.

- Cualquier miembro de SECAP LTDA estará obligado a comunicar de forma inmediata a los trabajadores pertinentes los factores de riesgo que haya podido identificar en sus actividades diarias y que afecten el control y seguridad en la cadena de suministros.

Direccionamiento estratégico y sistemas de gestión

- Deberá Colaborar con el comunicador en la identificación y valoración del riesgo detectado o en la sugerencia de oportunidades de mejora.
 - Deberán generar medidas de control que mitigue el riesgo comunicado.
 - Brindar seguimiento a las acciones correctivas.
 - Paralizar la actividad y evacuar la zona de peligro en caso de riesgo grave e inminente.
 - Informar al comunicador, en el menor tiempo las decisiones adoptadas y aprobadas para la minimización del riesgo.
 - Incorporar todos hallazgos en la matriz de riesgo institucional.
 - Archivar el original diligenciado y poner la información a disposición de los procesos involucrados
 - Elaborar un informe semestral de los nuevos riesgos presentarlo y comunicarlo
- ✓ **Comité de Seguridad y Salud en el trabajo:** Deberá recibir copia de las comunicaciones de riesgo. En las reuniones del COOPASST se podrá realizar un seguimiento de los comunicados y se informará de los resultados de esta reunión.

6.2 CAPACITACIONES

Con el fin de verificar que el personal de SECAP LTDA entienda, y aplique los controles establecidos para mitigar los riesgos, conozcan la forma de comunicar los riesgos encontrados en sus actividades diaria, identifiquen y conozcan los riesgos a los cuales este expuestos, se dictaran capacitación durante el año con los temas antes mencionados; adicionalmente en los procesos de inducción se destinara un día para brindar todo el conocimiento necesario en cuanto a riesgos al nuevo integrante de la organización.

	SECAP LTDA.	Página	Página 18 de 18
		Versión	7
		Fecha de Aprobación	10/07/2012
		Fecha Última Actualización	24/02/2017
CÓDIGO: PR-07-06	GESTIÓN INTEGRAL DEL RIESGO		

La matriz de riesgo se difundirá vía correo electrónico con el fin de facilitar información de los riesgos a los cuales se está expuesto; cuando la matriz se actualice con nuevos riesgos identificados se socializará a toda la organización.