1 Resumen

Esta política de amenazas internas (la "Política") se centra principalmente en la "amenaza interna", es decir, cuando una persona participa o facilita el terrorismo, el crimen organizado, el espionaje corporativo e industrial, el activismo, las actividades extremistas u otras actividades similares en su posición como empleado o subcontratista de Securitas.

Debido al mayor riesgo de terrorismo y la exposición de amenazas internas, todas las entidades deben tomar las siguientes medidas. El objetivo es garantizar, en la mayor medida posible, que Securitas pueda evitar y/o detectar empleados/subcontratistas que potencialmente puedan representar una amenaza para Securitas, sus clientes y el público, por ejemplo, estando involucrados en el crimen organizado, el terrorismo u otras actividades extremistas.

Cada país deberá:

1. Llevar a cabo un taller de riesgos en el que se realice una evaluación de la amenaza interna para diferentes tipos de tareas y diferentes tipos de empleados/subcontratistas. El taller de riesgos debe ser documentado: la "Matriz de Riesgos de Asignación". La matriz de riesgos de la asignación se revisará y actualizará anualmente y cuando se incremente el nivel de amenaza terrorista del país establecido por las autoridades
2. Asegúrese de que la selección de los empleados/subcontratistas se realice según lo decidido en la Matriz de Riesgo de Asignación.
3. Crear conciencia en la empresa sobre el riesgo de terrorismo en general, incluyendo más específicamente el riesgo de amenaza interna.
4. Implementar medidas operativas.
5. Asegúrese de que existan canales de denuncia adecuados para informar inquietudes.
6. Establezca un proceso sobre cómo actuar cuando se han planteado sospechas de amenazas internas.

Resumen de los principales cambios desde la última revisión:

Se agregaron aclaraciones menores a las secciones 3.3 (Creación de conciencia) y 4 (Canales de notificación y gestión de casos de amenazas internas)

2 Antecedentes y propósito

Debido al mayor riesgo de terrorismo, crimen organizado, riesgo de espionaje corporativo e industrial, activismo, fraudes de ingeniería social, extremistas u otras actividades similares, Securitas debe asegurarse de proporcionar un entorno seguro para sus empleados, clientes y la comunidad.

La "amenaza interna" se define como:

- una persona que participe o facilite el terrorismo, la delincuencia organizada, el espionaje corporativo e industrial, el activismo, las actividades extremistas u otras actividades similares en su puesto como empleado o subcontratista de Securitas y
- utilizar el puesto para realizar sabotajes, robos (incluido el robo de propiedad intelectual), interrupciones, etcétera, en Securitas o sus clientes, lo que podría tener graves implicaciones para Securitas y sus clientes.

Securitas necesita asegurarse de que tiene toda la información razonable requerida y disponible sobre las personas que Securitas está a punto de reclutar o asignar a las asignaciones, y que Securitas puede identificar cambios de comportamiento sospechoso durante el empleo. Esto también es válido para los "consultores clave", es decir, los consultores que podrían causar una amenaza para Securitas o sus clientes. El nivel de información relevante es diferente según el tipo de encargo y las diferentes categorías de empleados/subcontratistas.

También es crucial que las personas tengan la posibilidad de informar sobre el cambio de comportamiento de los empleados/subcontratistas.

Como parte de la tarea, los empleados/subcontratistas de Securitas a menudo se encuentran en sitios sensibles y pueden tener acceso a información confidencial. Por lo tanto, para cada encargo se debe decidir:

1. qué comprobaciones se deben realizar antes de que un empleado/subcontratista sea asignado a un sitio en particular,
2. qué comprobaciones de empleados/subcontratistas deben realizarse durante una asignación, y
3. Cómo los empleados pueden denunciar comportamientos sospechosos de otros empleados y subcontratistas.

Tal y como exige la ley, la mayoría de las entidades de Securitas realizan comprobaciones antes y durante el empleo. Además, la mayoría de las entidades de Securitas cuentan con procedimientos a través de los cuales los empleados pueden expresar sus inquietudes. Desde el punto de vista del Grupo Securitas, es importante asegurarse de que se realiza el análisis de riesgos adecuado y que el cribado se documenta cuando procede.

Además, es importante crear conciencia de riesgo dentro de esta área en la empresa.

3 Política de amenazas internas

Todas las entidades de Securitas deben asegurarse de que se aplican los siguientes procedimientos:

3.1 Taller de Riesgo de Asignación

La dirección del país llevará a cabo un taller de evaluación de riesgos en el que se decidirá el nivel de las actividades de selección que deben realizarse para cada tipo de empleado (por ejemplo, oficial de seguridad, gerente de sucursal, personal de apoyo, técnico) y subcontratista, y para cada tipo de tarea, véase el ejemplo de matriz de riesgos para la selección de empleados, Apéndice A (adjunto más adelante en esta sección). En la definición de subcontratista de esta política se incluyen los "consultores clave", es decir, los consultores

que podrían suponer una amenaza para Securitas. Un ejemplo podría ser que los consultores de TI tengan acceso a los sistemas de TI internos de Securitas y/o tengan la posibilidad de introducir códigos maliciosos en los procesos de TI de Securitas.

El taller de riesgos se centrará en evaluar el riesgo asociado a la tarea en particular desde la perspectiva de una amenaza interna, es decir, asignaciones en las que la posición como empleado/subcontratista de Securitas podría explotarse para llevar a cabo o facilitar actividades terroristas o actividades similares, por ejemplo, en aeropuertos, grandes eventos públicos o mediante el uso indebido del acceso a la información sensible de Securitas o de sus clientes ("espionaje industrial").

Además, al realizar el análisis se debe tener en cuenta el riesgo país global en cualquier momento. Se prestará especial atención a las advertencias de un aumento de las amenazas internas, por ejemplo, cuando se incremente el nivel de terrorismo en el país, según lo establecido por las autoridades, o cuando se cumplan aniversarios de incidentes terroristas anteriores u otros incidentes.

En función del riesgo de amenazas internas para una tarea en particular, se debe evaluar el tipo de selección de empleados/subcontratistas que se requiere. Desde esta perspectiva, una asignación con un menor riesgo de amenaza interna justifica menos selección de empleados/subcontratistas que las asignaciones con mayor amenaza interna.

No hace falta decir que las actividades de selección siempre deben estar en línea con la legislación local, las prácticas de la industria, el Código de Valores y Ética de Securitas y la política de Privacidad e IA Responsable del Grupo Securitas.

También hay que tener en cuenta la frecuencia con la que se deben realizar las actividades de selección, por ejemplo, solo antes de la asignación o con una cierta frecuencia durante la asignación. Se debe considerar si es necesario renovar la selección para los empleados/subcontratistas que cambian de asignación.

- En el apéndice A se incluyen ejemplos de matrices de riesgo
- El Apéndice B incluye ejemplos de posibles actividades de investigación de antecedentes

Tenga en cuenta que el cuadro del Apéndice A es un ejemplo de actividades de selección y que cada país debe decidir el formato de la(s) matriz(es) de riesgo que se utilizará.

La conclusión de la evaluación de riesgos anterior se denomina "Matriz de **riesgos de asignación**". Se documentará y se revisará y actualizará **anualmente**.

3.2 Evaluación antes y durante el empleo/asignación

Antes y durante el empleo/asignación, se deben cumplir los procedimientos de la Matriz de Riesgo de Asignación.

Por lo tanto, el país debe asegurarse de que:

— La Matriz de Riesgo de Asignación se comunica a los empleados relevantes.

- La selección se lleva a cabo de acuerdo con la Matriz de Riesgo de Asignación.
- En el caso de las tareas en las que se incremente la amenaza interna, se documentarán las actividades de cribado.

3.3 Creando conciencia

Cada entidad de Securitas debe asegurarse de que haya conciencia en la empresa del riesgo de amenaza interna. Los empleados deben estar informados sobre la amenaza interna y cómo comunicar los problemas a la gerencia.

Todo el personal debe someterse a la formación sobre amenazas internas de Securitas (Insider threat -Stay alert). Hay una formación adicional disponible en el centro de aprendizaje de Securitas dirigida a los responsables de seguridad (Amenaza interna: ver algo, decir algo), que no es obligatoria, pero se recomienda implementar para aumentar la conciencia y el conocimiento sobre el riesgo de amenaza interna. Además, se recomienda que todos los oficiales en sitios de alto riesgo se sometan a una sesión de capacitación o concientización sobre amenazas internas.

3.4 Implementar medidas operativas

Se deben tomar medidas operativas para evitar que ocurran incidentes. Dichas medidas incluyen el acceso limitado a las instalaciones del cliente y a los sistemas informáticos, lo que limita la previsibilidad de las tareas y las rutinas. Estas medidas existen en general dentro de las prácticas operativas, pero se considerará si se deben tomar precauciones adicionales a la luz del riesgo de amenaza interna, incluido el riesgo de espionaje industrial, el aumento del riesgo de ingeniería social, etc.

También debe haber procesos para mitigar este riesgo en relación con el momento en que los empleados abandonan la empresa, como contar con procesos para cancelar las tarjetas de identificación y garantizar que la devolución de los uniformes y otros suministros se realice al final del empleo.

Cuando la administración del país cumpla con la ley, garantizará una actividad de red suficiente con los servicios públicos (por ejemplo, la policía) para organizar una recopilación de inteligencia adecuada.

Para más información sobre las medidas operativas, véase "19.1. Directriz de política de amenazas internas" y la sección de amenazas internas en el "Equipo de ERM del administrador de riesgos" en Teams.

4 Canales de denuncia y gestión de casos de amenazas internas

El país se asegurará de que, como parte de los procedimientos y canales normales para informar de preocupaciones, por ejemplo, a un gerente, un representante de recursos humanos o el gerente legal o de riesgos, los empleados puedan informar a la gerencia sobre preocupaciones relacionadas con amenazas internas relacionadas con los empleados/subcontratistas de Securitas (o de otro tipo). Además, es posible reportar

inquietudes utilizando la Línea de Integridad de Securitas (Línea Directa de Securitas en los EE. UU. y Canadá, Línea de Alerta en México).

El país se asegurará de que todos los empleados estén informados sobre el procedimiento de presentación de informes (véase también *26. Política de Denuncia de Irregularidades del Grupo*). Dicho proceso deberá estar documentado.

Las siguientes reglas se aplican a cómo administrar los casos de amenazas internas:

El país establecerá y documentará un proceso sobre cómo actuar cuando se hayan planteado sospechas de amenazas internas, incluido cuándo ponerse en contacto con las autoridades encargadas de hacer cumplir la ley y cuándo relevar al empleado o a un subcontratista del puesto. Es obligatorio investigar cada sospecha para determinar si está justificada y, a partir de entonces, tomar las medidas adecuadas. No basta con informar de una preocupación a las autoridades.

- Si existe alguna sospecha en relación con los empleados de Securitas por amenaza interna, independientemente de cómo se hayan planteado dichas sospechas, dicha sospecha debe tratarse de inmediato y con la máxima atención.
- Cada país se asegurará de que se designe a una persona o comité con los conocimientos adecuados, que investigará todas esas sospechas y formulará una recomendación sobre las medidas apropiadas.
- Sólo el presidente del país, o una persona designada por el presidente del país, está autorizado a tomar decisiones sobre las medidas apropiadas en caso de sospechas fundadas. Las acciones pueden ser: investigación adicional del caso, transferencia, suspensión, despido, denuncia a la policía o cierre del caso sin ninguna otra acción.
- Dicha decisión deberá documentarse con las razones adecuadas. Para evitar dudas, la decisión de no tomar ninguna medida también debe documentarse.
- Si la decisión es continuar con la investigación o trasladar a la persona en cuestión, se requiere un seguimiento continuo hasta que el asunto pueda cerrarse definitivamente.
- Los casos graves, es decir, por ejemplo, casos confirmados de amenazas internas que supongan un grave riesgo para la seguridad de los empleados/clientes/sociedad de Securitas, o casos con potencial exposición a los medios de comunicación, deben informarse al Gestor de Riesgos del Grupo (group.risk@securitas.com) y a la División de forma continua.

Los informes al Grupo y a la División no incluirán información sobre la persona involucrada, como nombre, número de identificación del empleado, etcétera.

5 Aplicabilidad

Esta Política es aplicable a todos los países de Securitas.

6 Implementación y responsabilidad

Es responsabilidad de todos los presidentes de división y de cada presidente de país garantizar que esta Política (y la legislación local pertinente) se comprenda e implemente plenamente en sus áreas o países de responsabilidad. Debe haber una función dedicada en

cada empresa con la responsabilidad de garantizar que la entidad cumpla continuamente con la Política.

7 Capacitación

Es responsabilidad de los presidentes de división y los presidentes de país garantizar que se proporcione un nivel adecuado de información y concienciación a los empleados pertinentes para garantizar el cumplimiento de esta Política. En el centro de aprendizaje global de Securitas se ofrece un curso de formación en línea obligatorio para el personal («Amenaza interna – Mantente alerta») y una formación no obligatoria para los empleados de primera línea («Amenaza interna – Ver algo, decir algo»). La formación obligatoria para el personal debe ser realizada por todo el personal nuevo dentro de los 3 meses siguientes a la fecha de inicio y, a partir de entonces, todo el personal deberá recibir formación sobre amenazas internas cada 24 meses.

8 Informes, investigaciones y consecuencias de la violación

Todas las entidades y empleados de Securitas están obligados a informar de cualquier sospecha de comportamiento inapropiado contrario a esta Política a sus gerentes inmediatos o, cuando esto no sea posible, a un gerente superior, gerente de riesgo país, defensor del pueblo local, asesor legal o representante de Ética Empresarial, según corresponda en cada jurisdicción. Ningún empleado sufrirá consecuencias negativas por cumplir con esta Política, incluso si dicho cumplimiento resulta en la pérdida de negocios o por informar sobre el incumplimiento. Todos los eventos o sospechas reportados serán investigados de forma independiente y se les dará seguimiento.

Si una persona informante no desea, o no puede, informar de una sospecha a su jefe inmediato o a otro funcionario de su organización, todos estos problemas deben informarse a través de la Línea de Integridad de Securitas en https://securitas.integrityline.com/ (securitashotline.com para los EE. UU., securitashotline.ca para Canadá y lineadealerta.com.mx para México), por correo electrónico en integrity@securitas.com o al Director de Cumplimiento de Ética Empresarial de Securitas. La información de contacto actualizada se puede encontrar en el sitio web de Securitas, www.securitas.com.

Cualquier violación de esta Política o de las leyes locales aplicables dará lugar a medidas disciplinarias, que pueden incluir la terminación del empleo.

9 Revisión y seguimiento

El cumplimiento de esta política por parte de todas las entidades y empleados de Securitas será supervisado como parte del proceso de gestión de riesgos empresariales de Securitas, que incluye autoevaluaciones, revisiones legales y seguimientos rutinarios de todos los asuntos denunciados. El cumplimiento de esta política también debe ser supervisado dentro de las entidades de forma regular, por ejemplo, mediante auditorías internas.

10 Referencia a las Directrices

Véase 19.1. Directrices de la política de amenazas internas, para obtener consejos sobre las medidas operativas para mitigar el riesgo de amenazas internas y la sección de amenazas internas en el "Equipo de ERM del administrador de riesgos" en Teams.

19.1 Procedimientos de amenazas internas

1. OBJETIVO

Establecer las actividades y responsabilidades para gestionar los eventos que puedan generar riesgo que involucra la determinación del contexto y la identificación, análisis y tratamiento en las áreas y/o procesos, clientes, proveedores y/o contratistas de mayor criticidad en la organización.

2. ALCANCE

Este procedimiento aplica para todas las áreas y/o procesos, clientes, proveedores y/o contratistas de Securitas Colombia S.A., y va desde la identificación de los riesgos hasta la implementación de los planes de acción o los controles para mitigar el riesgo.

3. DEFINICIONES

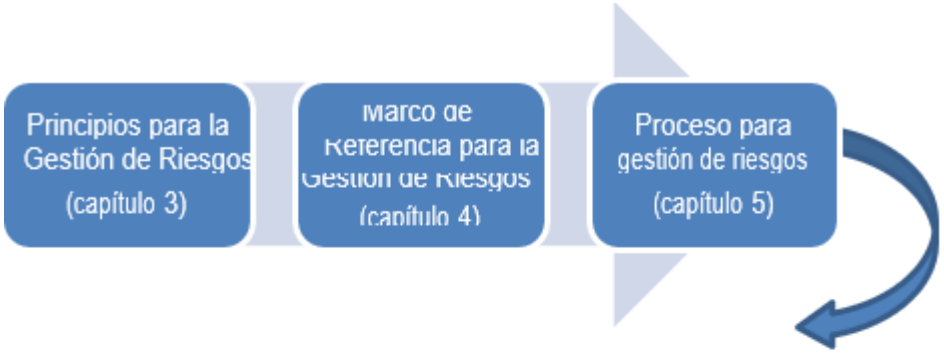
- ✓ **ANALISIS DE LOS RIESGOS**: Etapa en la que se identifica y evalúa los controles existentes con el propósito de determinar consecuencias y probabilidades, así como Nivel del riesgo.
- ✓ **AMENAZA**: Situación, objeto o persona que puede generar o causar riesgo a las instalaciones, procesos u otras personas.
- ✓ **VULNERABILIDAD**: Está relacionado con el riesgo y la amenaza y se puede definir como la debilidad o grado de exposición de un sujeto, objeto o sistema. También son aquellas fallas, omisiones o deficiencias de seguridad que puedan ser aprovechadas por terceros.
- ✓ **PROBABILIDAD**: Posibilidad de ocurrencia del riesgo, esta puede ser medida con criterios de frecuencia si se ha materializado o de factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque este se haya materializado.
- ✓ **CONSECUENCIA**: Es todo hecho o acontecimiento que resulta de un evento cualquiera, la consecuencia puede ser positiva o negativa.
- ✓ **IMPACTO**: Efecto dejado en alguien o en algo por cualquier acción o suceso, también puede referirse al impacto como un conjunto de consecuencias provocadas por un hecho o actuación que afecta a un entorno o ambiente social o natural.
- ✓ **CONTEXTO EXTERNO**: Ambiente externo en el cual la organización busca alcanzar sus objetivos.
- ✓ **CONTEXTO INTERNO**: Situaciones internas de la organización a través de las cuales se busca alcanzar los objetivos.
- ✓ **ESTABLECIMIENTO DEL CONTEXTO**: Definición de los 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 gestión del riesgo.
- ✓ **EVALUACIÓN DE RIESGOS**: Proceso usado para determinar las prioridades de gestión del riesgo mediante la comparación del nivel de riesgo frente a normas

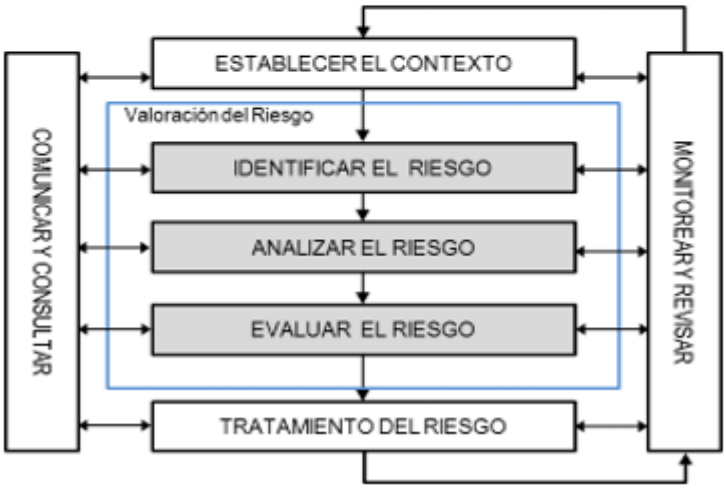
existentes, niveles de riesgo objeto y otros criterios.

- ✓ **FRECUENCIA**: Hace referencia a la cantidad de veces que un evento se repite en un tiempo determinado.
- ✓ **FRAUDE**: acción que resulta contraria a la verdad y a la rectitud, se comete contra otra persona u organización, constituyendo un delito castigado por la ley.
- ✓ **GESTIÓN DEL RIESGO**: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo
- ✓ **MARCO DE REFERENCIA PARA LA GESTIÓN DEL RIESGO**: Conjunto de componentes que brindan las bases y las disposiciones de la organización para diseñar, implementar, monitorear, revisar y mejorar continuamente la gestión del riesgo a través de toda la organización.
- ✓ **GESTION DEL RIESGO**: Proceso sistemático y documentado para gestionar la identificación, análisis y evaluación, tratamiento seguimiento, actualización y comunicación de los riesgos.
- ✓ **RIESGO**: Efecto de la incertidumbre sobre los objetivos.

4. NORMAS GENERALES

Securitas Colombia S.A. implementa las actividades de gestión del riesgo tomando como referente en enfoque genérico estructurado en los tres elementos claves que describe la NTC-ISO 31000:2018.





4.1 Para la gestión de los riesgos la Organización tiene como punto de partida los principios definidos en la norma:

- ✓ Crea valor
- ✓ Integra los procesos de la organización
- ✓ Forma parte de la toma de decisiones de la Alta Gerencia
- ✓ Trata la incertidumbre
- ✓ Es sistemática, estructurada y adecuada
- ✓ Basada en la mejor información disponible
- ✓ Hecha a la medida
- ✓ Tiene en cuenta factores humanos y culturales
- ✓ Es transparente e inclusiva
- ✓ Es dinámica, interactiva y sensible al cambio
- ✓ Facilita la mejora continua

4.2 El marco de referencia para la gestión del riesgo de Securitas Colombia es:

- ✓ Business Plan
- ✓ Filosofía Securitas (Caja de Herramientas y Caja de Diamantes)
- ✓ Normativa legal vigente para el sector de la Vigilancia y Seguridad Privada
- ✓ Código de ética y valores
- ✓ Minuta de Contrato
- ✓ La rendición de cuentas a la división y el Corporativo
- ✓ Política integrada de gestión
- ✓ Visión
- ✓ Misión

4.3 Determinación del Contexto: Securitas Colombia S.A., define su contexto para la identificación de riesgos, los parámetros internos y externos que se van a considerar al gestionar el riesgo y establece el alcance y los criterios del riesgo para el resto del proceso:

CONTEXTO	FACTORES	VARIABLES
Interno	PERSONAL	Habilidades, comunicación, experiencia, conocimientos, competencias
Interno	POLITICO y LEGAL	Procedimientos, políticas internas de la Empresa, corrupción, políticas de casa matriz, normatividad Colombiana u otra que aplique.
Interno	ECONÓMICO	Recursos con los que cuenta el área/proceso, presupuesto del área/proceso, falta de dinero, precios muy altos en el mercado, tasas de interés, tasas de inflación, entre otros.
Interno	TECNOLÓGICO E INFRAESTRUCTURA	Equipos de comunicación, innovación y desarrollo, automatización productiva, infraestructura, parque automotor, plataformas, acceso tecnológico, tendencias tecnológicas, espacios de trabajo, ambientes de trabajo, herramientas, entre otros.

Externo	AMBIENTAL y/o SEGURIDAD Y SALUD EN EL TRABAJO	Ambiental: Cambio climatico, escases de recursos, contaminación, normativas ambientales, conciencia ambiental de la población SST: Normativa en materia de seguridad y salud en el trabajo, riesgos y peligros de tareas y actividades desempeñadas en clientes.
Externo	CLIENTES	Rentabilidad, precios, descuentos, nuevos productos/servicios, negociación, marketing, calidad y valor agregado de productos/sevicios, acuerdos pactados en el servicio, entre otros.
Externo	COMPETENCIA	Competidos del sector, experiencia y cobertura en el mercado, nuevos competidores, tarifas del mercado.
Externo	PROVEEDORES	Negociación , precios, calidad, variedad de proveedores en el mercado, canales de distribución y cobertura.
Externo	TECNOLÓGIA	Plataformas, acceso tecnológico, infraestructura, tendencias tecnológicas a la vanguardia, entre otros.
Externo	PRODUCTOS Y SERVICIOS OFRECIDOS	Tecnologia, vangardia del mercado, servicio postventa, satistacción, entre otros.
Externo	SOCIAL	Variables demográficas, patrones culturales, estilos de vida (Costumbres, tradiciones), nivel de educación, nichos de mercado, entre otros.
Externo	LEGAL	Derechos, legislación, reglamentación nacional, local, regulación, precios, etc.

Nota: El Comité Directivo, en la revisión anual analiza y determina si existen cambios en el marco de referencia y contexto, sobre el cual la Organización gestiona los riesgos mediante la valoración de los riesgos ERM (Administración de la Evaluación de Riesgos) que pueden impactar la continuidad de Securitas Colombia S.A.

4.4 **Metodología**: El proceso de gestión del riesgo para Securitas Colombia S.A., toma como referente la metodología NTC-ISO 31000:2018 y se direcciona en tres frentes:

- ✓ Riesgos de la seguridad de las áreas y/o procesos: Gestionados por cada Líder de Proceso.
- ✓ Riesgos de los Clientes: Gestionados por el Gerente Comercial, Gerentes Regionales y Coordinadores de Seguridad.
- ✓ Riesgos de los Proveedores y/o Contratistas: Gestionados por la Directora Financiera y Administrativa - Controller y el Gerente de Servicios Administrativos & Compras.

4.5 Normas para la Gestión de Riesgos de la seguridad de las áreas y/o procesos:

- ✓ Los líderes de área identificarán para los procesos de su responsabilidad, los riesgos críticos que pudieran afectar los objetivos y/o estrategias definidas para el área. Dicha identificación puede ser realizada a través de reuniones con el equipo de trabajo para documentar en la Matriz de Gestión del Riesgo Integrada SIG-F28, clasificando los riegos identificados de acuerdo con el impacto (de imagen, económico, operativo, etc.)

- ✓ Los cambios realizados en la Matriz de Gestión del Riesgo Integrada SIG-F28 deberán ser notificados al área de Sistemas Integrados de Gestión.

- ✓ La actualización de la matriz se realizará cada vez que se identifique un riesgo que afecte el área/proceso y/o anualmente.

4.6 Normas para la Gestión de Riesgos con los Clientes: (Seguridad Física y Mobile):
La Gerencia de Gestión de Seguridad Física y la Gerencia Mobile (para esta línea de negocio) es responsable por el cumplimiento de la Valoración de riesgos con los clientes.

- ✓ La valoración del riesgo para un nuevo cliente (incluyendo escoltas y Mobile), se realiza dentro de los treinta (30) días de haberse instalado el servicio contratado.

- ✓ Las recomendaciones para el tratamiento de los riesgos valorados son referidas al cliente para consideración, siendo su responsabilidad determinar si las ejecuta o no.
- ✓ Anualmente o si la planta física del cliente o su distribución cambia, se realiza la actualización de la valoración de riesgos de los contratos vigentes que tenga la Organización.

- ✓ En el evento de siniestros con los clientes, el Gerente y Coordinador que tiene el contrato asignado, realiza la investigación, tomando como punto de partida las recomendaciones derivadas de la Gestión del Riesgo, referidas al cliente.

- ✓ A través del contrato de servicios GCO-F05 se tiene incluida la cláusula de "Acuerdo de Seguridad" para aquellos Asociados de Negocio que no estén certificados por BASC, para asegurar el cumplimiento de los criterios BASC establecidos por Securitas; como también la cláusula de "Cadena de Suministro" para asegurar la responsabilidad frente a la aplicación de políticas de prevención para evitar la comisión de actividades ilícitas que afecten la cadena de suministro, cuando el personal operativo participe en las actividades de importación o exportación del cliente, dentro de sus funciones para la prestación del servicio de vigilancia y seguridad privada.

- ✓ El Jefe de Seguridad de cada sede Securitas Colombia S.A., es quien realiza la valoración de riesgos de la sede asignada y garantiza el cumplimiento del tratamiento propuesto.

4.7 Normas para la Gestión de Riesgos con los Proveedores y/o Contratistas:

- ✓ La Directora Financiera y Administrativa - Controller y el Gerente de Servicios Administrativos & Compras, tienen la responsabilidad de gestionar el proceso de selección de los mismos y de asegurar el tratamiento de los riesgos que presentan

los proveedores y/o contratistas según lo establecido en el Procedimiento de Compras GAC-P01.

- ✓ Exigir a los proveedores críticos un plan de contingencia de su actividad que permita el desarrollo óptimo de las operaciones contratadas.
- ✓ Establecer cláusulas de confidencialidad y de responsabilidad en los contratos
- ✓ Exigir a través del Acuerdo de Cumplimiento y Confidencialidad de Socios Comerciales GAC-F09, la ética y transparencia para los ejercicios de sus actividades.
- ✓ Programar visitas a los proveedores críticos para verificar donde desarrollan sus operaciones con el fin de verificar el cumplimiento de requisitos mínimos de seguridad de la cadena de suministro.

4.8 Cumplimiento de los Acuerdos de Seguridad: Se validará y clasificaran los clientes críticos y no críticos de Securitas de acuerdo con su actividad (Ver matriz de cargos críticos RH-F53). Se tendrá en cuenta el personal operativo que tenga relación indirecta con la carga. Si la actividad del cliente es importar o exportar y el personal operativo NO se encuentra involucrado con la carga, no se considerará cliente crítico. Anualmente a través de auditorías de segunda parte se dará cumplimiento de los acuerdos de seguridad pactados con los clientes críticos.

Se gestionarán las acciones correctivas correspondientes para asegurar el seguimiento a los resultados de dicha verificación.

4.9 Simulacros: Se realizará de forma aleatoria simulacros a los clientes críticos con base a la prioridad de los riesgos y la criticidad, para evitar que estos se materialicen o en caso de que sucedan, su impacto sea menor.

5. DESCRIPCIÓN DEL PROCESO

No	ACTIVIDAD	RESPONSABLES	DESCRIPCIÓN DE LA ACTIVIDAD	DOCUMENTOS/ REGISTROS UTILIZADOS
1	IDENTIFICAR EL RIESGO	Líderes de Proceso Gerente Comercial Gerentes Regionales Coordinadores de Seguridad Directora Financiera y Administrativa - Controller Gerente de Servicios Administrativos & Compras	Procede con la identificación de riesgos: • **Áreas y/o Procesos:** Se identifican los aspectos a evaluar según la actividad, procesos, personas y espacios donde se realiza la labor, se deja el registro en la matriz de gestión del riesgo integrada SIG- F28. • **Clientes:** Los Coordinadores de Seguridad programan visita al predio del	SIG-F28 Matriz de Gestión del Riesgo Integrada GSF-F02 Guía de Encuesta para Seguridad Física GSF-F08 Matriz de Gestión del Riesgo SF GAC-F01 Selección Inicial de proveedores GAC-F11 Evaluación y Reevaluación de Proveedores

			cliente e identifican los riesgos a través de la Guía de Encuesta para Seguridad Física GSF-F02 y la Matriz de Gestión del Riesgo de Seguridad Física GSF-F08. • **Proveedores:** A través de los parámetros definidos en los formatos GAC-F01 Selección Inicial de Proveedores y GAC-F11 Evaluación y Reevaluación de Proveedores, se identifican los aspectos y cumplimiento de estos. También clasifica al proveedor en crítico y no crítico.	

2	ANALIZAR EL RIESGO	Líderes de Proceso Gerente Comercial Gerentes Regionales Coordinadores de Seguridad	Luego de identificados los riesgos críticos brinda la entrada para la evaluación del riesgo que conduce a la toma de acciones para disminuir su probabilidad de ocurrencia. El análisis involucra la consideración de las causas y las fuentes de riesgo.	GSF-F08 Matriz de Gestión del Riesgo SF SIG-F28 Matriz de Gestión del