Página de firmas

Nombre	Motivo	Fecha (dd/mm/aaaa UTC)
Geode Plus	Mass Import	01/11/2016 14:24:00

Historia del Documento

Versión	Fecha (dd/ mm/aaaa UTC)	Descripción
1.0	05/10/2016	HS-SGC-007

1. OBJETIVO:

Establecer la metodología para la valoración y manejo de todos los procesos de gestión de Riesgos en seguridad de la cadena de suministro de acuerdo a los requerimientos de la norma ISO 28001. La gestión de riesgos es parte integral del sistema de seguridad, y debe ser integrada a las operaciones existentes y documentada apropiadamente.

2. ALCANCE:

Éste procedimiento tiene como alcance los procesos relacionados con la seguridad de la cadena de suministro de Genfar Villarica.

3. DOCUMENTOS ASOCIADOS O DE REFERENCIA:

3.1 NTC ISO 28001
3.2 NTC ISO 31000

4. RESPONSABILIDADES:

4.1 EL DIRECTOR INDUSTRIAL es responsable por asegurar que los recursos apropiados son disponibles para cumplir con este procedimiento.

4.2 EL GERENTE NACIONAL DE SEGURIDAD: Responsable de gestionar los recursos necesarios para el cumplimiento de los estándares de seguridad en la cadena de suministro.

4.3 EL RESPONSABLE DEL SISTEMA DE GESTIÓN EN SEGURIDAD: Es la persona designada por parte de la empresa del desarrollo de planes de seguridad basados en la identificación, análisis, evaluación y tratamiento del riesgo.

4.4 JEFE DE SEGURIDAD: es la persona encargada de coordinar la ejecución de las actividades descritas en los planes de seguridad.

4.5 EL PERSONAL DE SEGURIDAD: Responsable(s) de ejecutar las actividades y procedimientos definidos para dar cumplimiento a los estándares de seguridad en la cadena de suministro.

5. DEFINICIONES:

5.1. AGUAS ABAJO: Se refiere a las acciones, procesos y movimientos de la carga en la cadena de suministro, que ocurren después de que la carga sale del control operacional directo de la organización, incluidas la gestión de seguros, las finanzas y los datos, el empaque, almacenamiento y transferencia de la carga entre otros.

5.2. AGUAS ARRIBA: Se refiere a las acciones, procesos y movimientos de la carga en la cadena de suministro, que ocurren antes de que la carga se encuentre bajo el control operacional de

la organización, incluidas la gestión de datos, las finanzas y los seguros y el empaque, almacenamiento y transferencia de la carga entre otros.

5.3 CADENA DE SUMINISTRO: Conjunto enlazado de recursos y procesos que comienza al colocarse la orden de compra, con el suministro de la materia prima y se extiende a la fabricación, manipulación y despacho de mercancías y servicios relacionados, al comprador.

5.4 RIESGO: Combinación de la probabilidad de ocurrencia del daño y la severidad del mismo.

6. REQUERIMIENTOS: N/A

7. ACTIVIDADES:

7.1. PROCESO DE GESTIÓN DE RIESGOS DE SEGURIDAD

La gestión de riesgos de seguridad en la cadena de suministro permite a la organización establecer, documentar e implementar niveles de seguridad mínimos en sus cadenas de suministro internacional; además, incluye el compromiso de cumplir con la legislación actual aplicable, los requisitos de reglamentación y otros que suscribe la organización. Es indispensable tener definidas las áreas vulnerables y así prevenir los riesgos de seguridad en la compañía.

7.1.1. Identificación del riesgo

Corresponde a las amenazas a la seguridad y riesgos relacionados con la gestión de seguridad (NTC 28001) tales como:

a) Amenazas y riesgos de falla física, tales como falla funcional, daño incidental, daño malicioso o terrorista o acción criminal;

b) Amenazas y riesgos operacionales, incluidos el control de la seguridad, los factores humanos y otras actividades que afectan el desempeño, la condición o la seguridad de las organizaciones;

c) Eventos del medio ambiente natural (tormentas, inundaciones, etc.) que pueden hacer que las medidas y equipos de seguridad resulten ineficientes;

d) Factores por fuera del control de la organización, tales como fallas en el equipo y servicios suministrados externamente.

e) Amenazas y riesgos de las partes involucradas, tales como falla en cumplir los requisitos de reglamentación o daño a la reputación o la marca;

f) Diseño e instalación del equipo de seguridad, incluido su reemplazo, mantenimiento, etc.

g) Gestión de datos e información y comunicaciones.

h) Una amenaza a la continuidad de las operaciones.

Nota: En la identificación de los escenarios de amenazas a la seguridad no participan funcionarios del gobierno.

7.1.2. Análisis del riesgo

El análisis del riesgo es la estimación del riesgo asociado con el peligro identificado.
Las bases del análisis de riesgos es la investigación e identificación de la causa raíz, o la revisión analítica de un proceso o sistema establecido.
Los pasos del análisis de riesgo concluyen y documenta:

- La causa raíz más probable de la falla potencial o detectada

7.1.3. Evaluación del riesgo

Describe los posibles impactos o consecuencias que se pueden esperar razonablemente de cada escenario potencial de amenaza para la seguridad.
Establece el nivel de vulnerabilidad para cada escenario de amenaza a la seguridad por medio de los controles de seguridad establecidos que permiten prevenir o detectar una amenaza o riesgo a la seguridad.
Describe los controles actuales que aplican a la cadena de suministro definida en el alcance.
Los pasos de la evaluación del riesgo concluyen y documenta:

- Impactos o consecuencias
- Nivel de vulnerabilidad
- Controles actuales

7.1.4. Tratamiento del riesgo

Responde al tratamiento y/o manejo que se le dará al riesgo, teniendo en cuenta su priorización.
Describe las contramedidas de seguridad que son necesarias para el mantenimiento, y mejora de la seguridad.
Los pasos del tratamiento del riesgo concluyen y documenta:

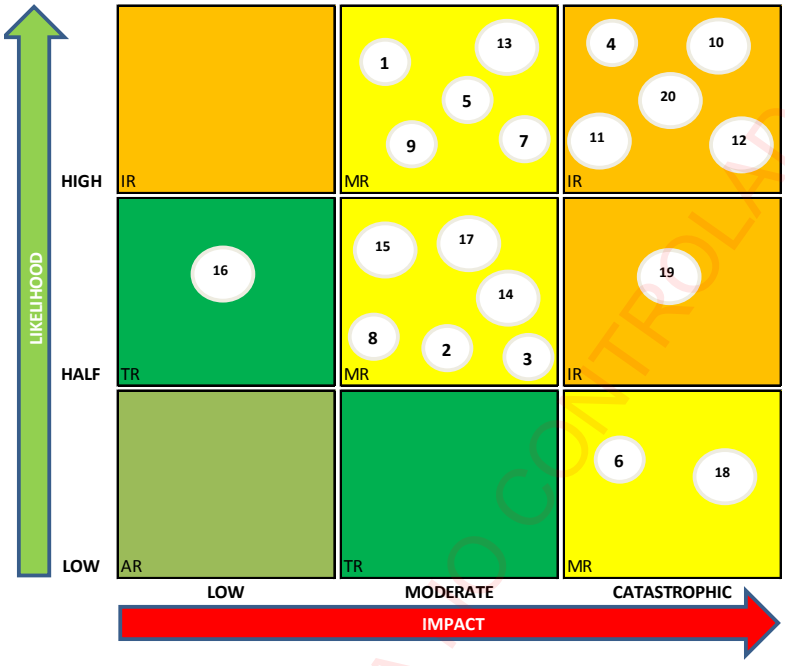
- Tratamiento: El tratamiento del riesgo puede implicar:

  a. Evitar el riesgo: decidiendo no iniciar o continuar la actividad que lo originó.
  b. Controlar: Los controles incluyen procesos, políticas, dispositivos, prácticas u otras acciones que modifican el riesgo.
  c. Transferir: Compartir el riesgo con una o varias de las partes.
  d. Asumir/Tolerar: Implica que la organización no puede emprender ninguna acción.

- Contramedidas: Acciones tomadas para reducir la posibilidad de que un escenario de amenaza para la seguridad tenga éxito en sus objetivos o para reducir las posibles consecuencias de un escenario de amenaza a la seguridad

- Responsables: Persona(s) encargada de la implementación de las contramedidas.

7.2. CONTRUCCIÓN DE LA MATRIZ DE RIESGOS



1	Asalto
2	Intrusión
3	Falsedad en documentos
4	Contaminación de la carga
5	Fuga de información
6	Fraude
7	Hurto de medicamentos
8	Hurto de equipos
9	Piratería terrestre
10	Extorsión
11	Secuestro
12	Atentado
13	Falsificación de marca
14	Sabotaje
15	Daño a vehículo de carga
16	Espionaje industrial
17	Lesiones personales
18	Homicidio
19	Hurto Continuado
20	Accidente en transporte personal de la empresa

RISK LEVEL
UNACCEPTABLE
IMPORTANT
MODERATE
TOLERABLE
ACCEPTABLE

7.2.1. Severidad/Impacto:

Catastrófico (20): Pérdida de la vida, consecuencias graves para los bienes e instalaciones de la empresa, afectación grave al negocio, pérdida de valores de difícil recuperación, destrucción completa de múltiples aspectos en un ecosistema, consecuencias graves a la seguridad, Impacto legal grave, el evento es de conocimiento e la empresa, la administración, las autoridades, medios de comunicación regional, nacional e internacional.

Moderado (10): Lesiones físicas graves e irreparables (Incapacidad permanente parcial o invalidez), consecuencias moderadas para los bienes, la infraestructura, los documentos, la

información, impacto legal moderado, el evento es de conocimiento de la empresa, la administración y las autoridades según sea el caso.

Leve (5): Lesiones con incapacidad temporal o que no generen incapacidad, daño mínimo a un activo y/o a la infraestructura de la empresa, solo de conocimiento de la empresa.

7.2.2. Probabilidad de ocurrencia:

Muy probable (alta 3): Probable ocurrencia dentro de 1 y 2 años, y/o se han presentado eventos en la empresa atribuibles a esta fuente de riesgo.

Probable (media 2): Puede ocurrir dentro de 2 a 5 años y/o se ha presentado eventos en instalaciones vecinas o de similares características atribuibles a esta fuente de riesgo.

Improbable (baja 1): No probable que ocurra dentro de 5 años, y/o no se han presentado eventos relacionados con esta fuente de riesgo.

		VALOR	ZONA DE RIESGO	ZONA DE RIESGO	ZONA DE RIESGO
PROBABILIDAD	ALTA	3	MODERADO 15	ALTO 30	MUY ALTO 60
	MEDIA	2	MEDIO 10	MODERADO 20	ALTO 40
	BAJA	1	BAJO 5	MEDIO 10	MODERADO 20
			LEVE	MODERADO	CATASTROFICO
			5	10	20
			IMPACTO		

CALIFICACIÓN DE RIESGO: Probabilidad de ocurrencia x severidad o Impacto

Riesgos del 60 serán considerados Riesgos de Clase 50 (Riesgo Muy Alto)
Riesgos del 30 - 40 serán considerados Riesgos de Clase 40 (Riesgo Alto)
Riesgos del 15-20 serán considerados Riesgos de Clase 30 (Riesgo Moderado)
Riesgos del 10 serán considerados Riesgos de Clase 20 (Riesgo Medio)
Riesgos del 5 serán considerados Riesgos de Clase 10 (Riesgo Bajo)

Los riesgos entonces serán priorizados por la multiplicación de la valoración del nivel de Vulnerabilidad x la Clase de Riesgo

7.2.3. Nivel de vulnerabilidad:

Alta (3): No se han establecido controles de seguridad para evitar la materialización del riesgo. Existen controles de seguridad establecidos y aplicados pero son ineficaces.
Requiere atención por parte de las directivas. Requiere implementar medidas urgentes.

Media (2): Los controles de seguridad actuales ofrecen resistencia moderada a la materialización del riesgo. Requiere medidas adicionales al control actual. Requiere la atención por parte de los líderes de procesos.

Baja (1): Los controles actuales y/o sistemas de seguridad establecidos permiten que las amenazas o riesgos a la seguridad sean fácilmente detectables.

NIVEL DE RIESGO: Calificación de riesgo x Vulnerabilidad

- 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.
- 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.
- Moderado: Se controla
- Tolerable: 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.
- Aceptable: El riesgo o amenaza está controlado, se debe mantener el monitoreo sobre los controles establecidos no requiere de medidas adicionales.

	VULNERABILIDAD		
CALIFICACIÓN DE RIESGO	**Baja (1)**	**Media (2)**	**Alta (3)**
Clase 50: Riesgo Muy alto	50	100	150
Clase 40: Riesgo alto	40	80	120
Clase 30: Riesgo Moderado	30	60	90
Clase 20: Riesgo medio	**20**	**40**	**60**
clase 10: Riesgo bajo	10	20	30

NIVEL DE RIESGO		
150	INACEPTABLE	
100 A 120	IMPORTANTE	
50, 60, 80 Y 90	MODERADOS	
30 A 40	TOLERABLE	
10 A 20	ACEPTABLE	

Priorización Nivel de Riesgo: Calificación de Riesgo X Vulnerabilidad

7.3. ACTIVIDADES GESTIÓN DE RIESGOS DE SEGURIDAD EN LA CADENA DE SUMINISTRO

De acuerdo a la NTC 28001, Seguridad en la cadena de suministro establece:

7.3.1. Revisar el estado actual de la seguridad en la cadena de suministro. Con base en los hallazgos de ésta revisión, usar el criterio profesional para identificar la vulnerabilidad de la cadena de suministro para cada escenario de amenaza.
7.3.2. Para escenarios de amenaza inaceptables desarrollar procedimientos adicionales (contramedidas) o cambios operacionales para reducir la posibilidad, la consecuencia o ambas.
7.3.3. Priorizar los riesgos, e incorporar las contramedidas al plan de seguridad para reducir la amenaza a un nivel aceptable.
7.3.4. Documentar el proceso de gestión de riesgos.
7.3.5. Desarrollar e implementar un plan de seguridad o plan operacional de seguridad.

7.4. MATRIZ REGULATORIA

Conforme a la norma NTC 28001, la matriz regulatoria establece los requerimientos legales que las áreas de la empresa, vinculadas directamente con la cadena de suministro, deben cumplir para mitigar riesgos y problemas en la seguridad.

Las áreas consideradas bajo este distintivo son: Seguridad y salud ocupacional, Medio ambiente, Asuntos regulatorios y Recursos humanos, las cuales son las responsables de actualizar y documentar la información.

8. REGISTROS GENERADOS:

IDENTIFICACIÓN	Matriz de riesgos de seguridad.
ALMACENAMIENTO	Documento Físico.
PROTECCIÓN	En custodia de la central de Monitoreo Villa Rica.
RECUPERACIÓN	Carpetas central de Monitoreo.

TIEMPO DE RETENCIÓN	1 Año – Actualización anual.
DISPOSICIÓN	Destrucción.

IDENTIFICACIÓN	Matriz Regulatoria – Identificación y Evaluación de requisitos legales.
ALMACENAMIENTO	Documento Físico y magnético en el área correspondiente.
PROTECCIÓN	En el archivo de cada área responsable.
RECUPERACIÓN	Carpetas del área correspondiente.
TIEMPO DE RETENCIÓN	3 Años.
DISPOSICIÓN	Destrucción física y magnética.

IDENTIFICACIÓN	Matriz de áreas críticas de la compañía.
ALMACENAMIENTO	Documento magnético y físico.
PROTECCIÓN	En el archivo del área de seguridad.
RECUPERACIÓN	Carpeta en el área de seguridad.
TIEMPO DE RETENCIÓN	3 Años.
DISPOSICIÓN	Destrucción física y magnética.

IDENTIFICACIÓN	Cronograma de capacitaciones – Área de seguridad.
ALMACENAMIENTO	Documento magnético y físico.
PROTECCIÓN	En el archivo del área de seguridad.
RECUPERACIÓN	Carpeta en el área de seguridad.
TIEMPO DE RETENCIÓN	1 Año.
DISPOSICIÓN	Destrucción física y magnética.

IDENTIFICACIÓN	Cronograma de pruebas de vulnerabilidad
ALMACENAMIENTO	Documento magnético y físico.
PROTECCIÓN	En el archivo del área de seguridad.
RECUPERACIÓN	Carpeta en el área de seguridad.
TIEMPO DE RETENCIÓN	1 Año.

DISPOSICIÓN	Destrucción física y magnética.

9. ANEXOS:

- Anexo # 2: Proceso de seguridad en la cadena de suministro.
- Anexo # 3: Valoración de Riesgos de seguridad.

.

HOJA DE CONTROL DE CAMBIOS:

Revisión	Motivo del cambio	Fecha	Elaborado/cargo	Modificado / cargo
0	Procedimiento nuevo acorde a los requisitos de la Norma ISO 28001.	22-07-2015	Luis Fernando Bohorquez/Supervisor de Seguridad.	N/A.
1	Anexo de la Matriz Regulatoria y la de Áreas críticas de la compañía – requeridas por la norma NTC ISO 281001.	18-11-15	Aseguramiento de la calidad.	N/A.
2	Incluir grafica de Matriz resumen y Modificar Formatos anexos	30-09-16	Luis Fernando Bohorquez/Jefe de Seguridad	N/A.