**EVALUACION DE RIESGOS EN LAS INSTALACIONES, LAS PERSONAS Y LAS OPERACIONES DE TRANSBORDER S.A.S. AÑO 2012**

**DEFINICIONES**

* Aprovechamiento: medio de utilizar una vulnerabilidad para poner en peligro las instalaciones, el personal o la operación de la compañía.
* Exposición: acción de amenaza en la que la información es revelada sin autorización.
* Efecto: pérdidas previstas cuando una amenaza aprovecha una vulnerabilidad.
* Probabilidad: posibilidad de que se produzca un suceso o frecuencia en que ocurre.
* Riesgo: combinación de la probabilidad de un suceso y sus consecuencias.
* Evaluación de riesgos: proceso mediante el que se identifican los riesgos y se determinan sus efectos.
* Amenaza: causa posible de un efecto no deseado en una compañía.
* Vulnerabilidad: cualquier debilidad, proceso administrativo, acto o exposición física que permita que una amenaza ataque la compañía.

**OBJETIVO**

Identificar, clasificar y evaluar los riesgos en los bienes e instalaciones, funcionarios y operaciones de Transborder S.A.S., verificando el impacto de las acciones planteadas para contrarrestrar los riesgos identificados en la evaluación de riesgos del año 2011.

**1. IDENTIFICACION DE RIESGOS**

De acuerdo a la evaluación de riesgos del año anterior los riesgos más comunes en la cadena logística y en las operaciones de comercio exterior, según la *guía de buenas prácticas en seguridad en la cadena de suministro – Numeral 4.1.2 (Riesgos puros)*:

1. ***Robos***

*Amenazas: Filtración de información, hurto, abuso de confianza*

1. ***Tráfico ilícito***

*Amenazas:* *Contrabando, Narcotráfico, Lavado de activos*

1. ***Terrorismo***

*Amenazas:* *Extorsión, Atentados, Secuestro*

1. ***Piratería***

*Amenazas:* *Saqueos, Ataques contra la carga, Sabotaje*

**2. CALIFICACION DE LOS RIESGOS**

Determinación del impacto del riesgo de acuerdo a la probabilidad de ocurrencia y la severidad (impacto) del mismo en los bienes e instalaciones, funcionarios y operaciones de la compañía.

|  |  |  |  |
| --- | --- | --- | --- |
| **PROBABILIDAD** | **CLASIFICACION DE RIESGO** | | |
| *Alta (5)* | **5 Tolerable** | **15 Inaceptable** | **25 Inaceptable** |
| *Media (3)* | **3  Aceptable** | **9 Tolerable** | **15 Inaceptable** |
| *Baja (1)* | **1 Aceptable** | **3  Aceptable** | **5 Tolerable** |
| **SEVERIDAD** | *Leve (1)* | *Grave (3)* | *Catastrófico (5)* |

**3. ESTRATEGIAS Y/O PLANES DE ACCION 2011**

Los siguientes riesgos fueron identificados como *“inaceptables”* en la evaluación de riesgos 2011

| ***AREA EXPUESTA: OPERACIÓN*** | | | |
| --- | --- | --- | --- |
| ***RIESGO*** | ***AMENAZA*** | ***VULNERABILIDAD*** | ***ESTRATEGIA(S)*** |
| PIRATERIA | Sabotaje | Actividades mal desarrolladas intencionalmente por negligencia, apatía, revanchismo, rencillas, enfrentamientos laborales | *PREVENIR:* Reuniones periódicas dentro de los equipos de trabajo, seguimiento constante de las actividades de los funcionarios por parte de los gerentes y/o directores de proceso, reuniones entre procesos, reuniones gerenciales. *PROTEGER:* todos los funcionarios de la compañía han firmado el "Acuerdo sobre el uso de la información y buena conducta". |

***ESTADO DE LA ESTRATEGIA:*** Además de las previsiones legales con las que cuenta la compañía actualmente (selección de personal, acuerdos de confidencialidad, de buen uso de la información, políticas de comunicaciones, entre otros), se presentan dos refuerzos para el manejo de este riesgo:

1. el área de Talento Humano cambió el proveedor de pruebas psicotécnicas, a fin de mejorar el análisis de los perfiles ocupacionales de los nuevos ingresos, en los que se valoran rasgos de comportamiento tales como estabilidad, felicidad, compostura, seguridad, actividad, empuje, responsabilidad, tolerancia, empatía y comunicación. La valoración de los rasgos dan herramientas a la compañía para no seleccionar personas con perfiles contrarios a los requerimientos de la compañía o proclives a la vulnerabilidad descrita.
2. el área de tecnología formuló la política sobre el uso de recursos tecnológicos, la cual reglamenta el uso responsable y seguro de los equipos de cómputo de la compañía, a fin de evitar fugas de información (interna y externa), uso racional de los canales de navegación, minimizar el riesgo de contaminación de la red de información con virus, gusanos informáticos y malware. Para la ejecución de esta política se implementarán acciones tales como la restricción de puertos USB, monitoreo a e-mail y unidades de red, seguimiento a navegación en Internet y a conversaciones en mensajería instantánea, entre otros.

Además de los refuerzos a esta estrategia, cabe notar las siguientes acciones de impacto en otros riesgos clasificados como *“tolerables”:*

* Mejora de instalaciones:
  + compra de un archivador rodante, para mantener la seguridad de la información de la compañía (D.O., hojas de vida, información financiera)
  + instalación de lectores dentro de las oficinas para las tarjetas de proximidad, monitoreado bajo software, a fin de verificar el ingreso-salida de los funcionarios.
* Seguridad informática:
  + Instalación de servidores exclusivos para *“Firewall”* (control unificado de las amenazas de intrusión a los demás servidores de Transborder y otro para *“Blackberries.”*

**4. REEVALUACION DE RIESGOS**

Cada una de las áreas potenciales a exposición de riesgo es evaluada de acuerdo a la clasificación de los riesgos y las acciones adelantadas para contrarrestarlas

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | **AREAS POTENCIALES DE EXPOSICION** | | | | | | | | |
|  |  | **BIENES E INSTALACIONES** | | | **FUNCIONARIOS** | | | **OPERACIÓN** | | |
| **RIESGO** | **AMENAZA** | **PROBABILIDAD  (frecuencia)** | **SEVERIDAD  (impacto)** | **PROMEDIO** | **PROBABILIDAD  (frecuencia)** | **SEVERIDAD  (impacto)** | **PROMEDIO** | **PROBABILIDAD  (frecuencia)** | **SEVERIDAD  (impacto)** | **PROMEDIO** |
| **ROBOS** | *Filtración de información* | NA | NA | - | 3 | 3 | 9 | 1 | 3 | 3 |
| *Hurto* | 1 | 3 | 3 | 1 | 3 | 3 | NA | NA | - |
| *Abuso de confianza* | 1 | 5 | 5 | 3 | 3 | 9 | NA | NA | - |
| **TRAFICO ILICITO** | *Contrabando* | NA | NA | - | NA | NA | - | 3 | 3 | 9 |
| *Narcotráfico* | NA | NA | - | NA | NA | - | 3 | 3 | 9 |
| *Lavado de activos* | NA | NA | - | NA | NA | - | 1 | 5 | 5 |
| **TERRORISMO** | *Extorsión* | 1 | 3 | 3 | 1 | 5 | 5 | NA | NA | - |
| *Atentados* | 3 | 3 | 9 | 1 | 5 | 5 | NA | NA | - |
| *Secuestro* | NA | NA | - | 1 | 5 | 5 | NA | NA | - |
| **PIRATERIA** | *Saqueos* | 1 | 3 | 3 | NA | NA | - | 1 | 5 | 5 |
| *Ataques contra la carga* | NA | NA | - | NA | NA | - | 3 | 3 | 9 |
| *Sabotaje* | NA | NA | - | NA | NA | - | 3 | 5 | 15 |

Los riesgos inaceptables (en criterio Rojo) se identifican de acuerdo a la frecuencia con que estos pueden ocurrir y el impacto en las áreas expuestas al riesgo. Los riesgos tolerables y aceptables (en criterio amarillo y verde respectivamente), deben ser revisados de acuerdo a las mejoras de procesos y las actividades de capacitación y/o entrenamiento,

Una vez evaluados de acuerdo a la probabilidad y severidad, se identifica el porque es vulnerable cada una de las áreas potenciales de exposición, explicando los motivos por los cuales el riesgo puede ser perjudicial para la compañía. Los riesgos tolerables y aceptables den ser revisados en conjunto con los inaceptables y se administrarán en el momento en que se convierten en inaceptables, dado que el riesgo aumenta y se necesitan nuevos planes de acción para controlarlos y mitigar su impacto.

|  |  |  |
| --- | --- | --- |
|  |  | ***AREA EXPUESTA: OPERACIÓN*** |
| ***RIESGO*** | ***AMENAZA*** | **VULNERABILIDAD** |
| *PIRATERIA* | *Sabotaje* | *Actividades mal desarrolladas intencionalmente por negligencia, apatía, revanchismo, rencillas, enfrentamientos laborales* |

**5. ESTRATEGIAS Y/O PLANES DE ACCIÓN**

Para los riesgos de clasificados como *Inaceptables* se pueden presentar las siguientes alternativas:

1. Manejar el riesgo: (evitarlo, prevenirlo y/o mitigar el riesgo en las áreas expuestas)
2. Planear y disponer de recursos para subsanar las posibles pérdidas: (Aceptar el riesgo, tenerlo y/o transferirlo a terceros)

**6. CONCLUSIONES**

La administración de riesgos para 2012, respecto al panorama identificado en 2011 presenta mejoras el manejo a varios riesgos identificados como tolerables, impactando en la probabilidad (frecuencia) de su ocurrencia. Pese a que el riesgo identificado en 2011 como inaceptable no cambió su categoría, se han adelantado acciones con el fin de mantener controladas las condiciones del riesgo. Cabe anotar que es un riesgo que en su naturaleza depende de las condiciones personales del recurso humano de la compañía y que los cambios de estado/ánimo de las personas no pueden ser predecibles y poco controlables.

La definición de riesgo aceptable y sus probables implicaciones, se mantienen controladas bajo estrategias de manejo de riesgo, esta situación que puede variar de acuerdo a los cambios internos y/o del entorno.

**7. FUENTES DE CONSULTA**

* Evaluación de riesgos en las instalaciones, las personas y las operaciones de TRANSBORDER S.A.S. año 2011
* Guía de buenas prácticas en Seguridad en la Cadena de Suministro, BASC Colombia, disponible en <http://www.basc.org.do/PDF_files/Guiadebuenaspracticas.pdf>
* Mejía Quijano, Consuelo. Administración de riesgos: un enfoque empresarial. Fondo editorial Universidad EAFIT, 2006