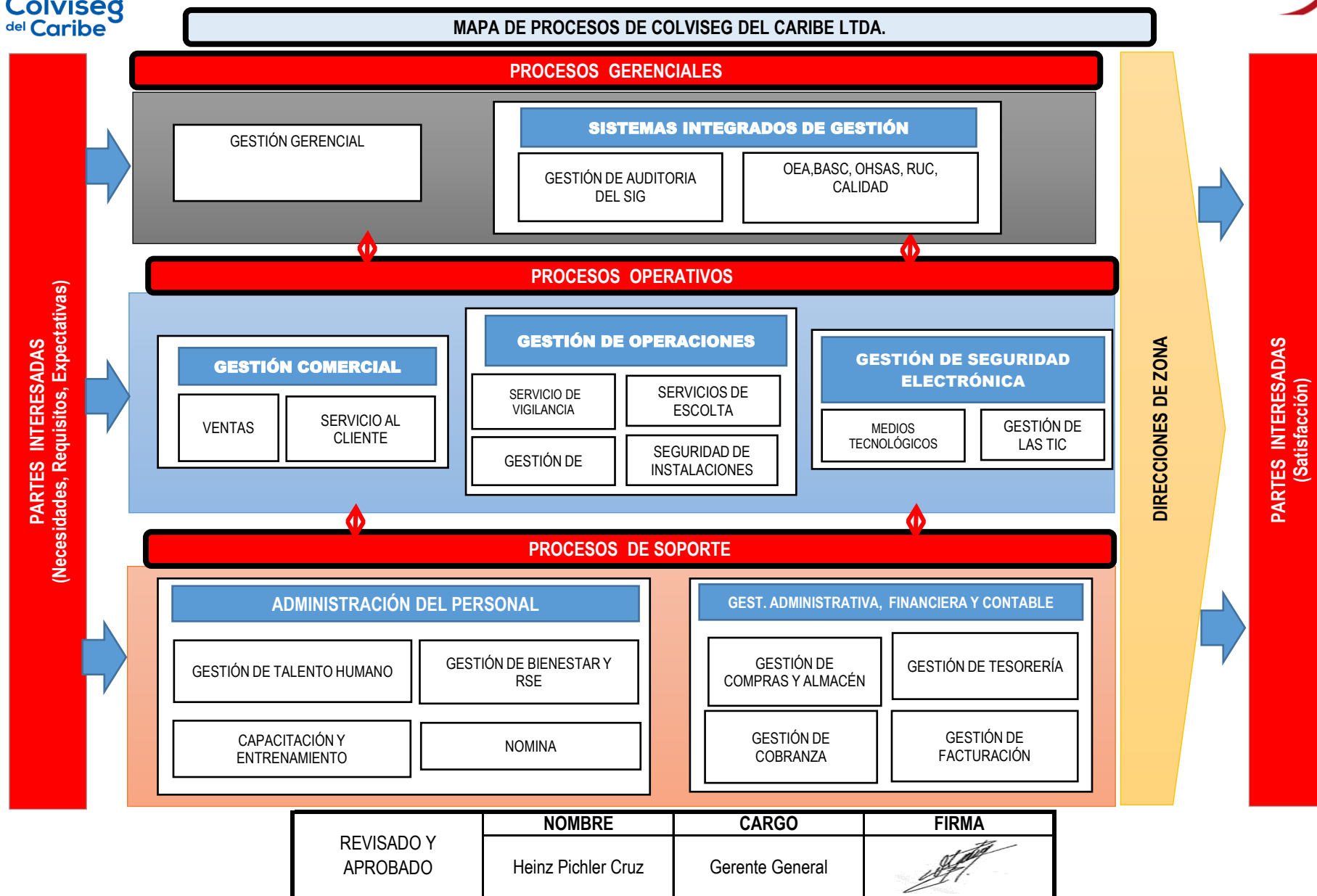




SISTEMA DE ADMINISTRACIÓN DE RIESGOS

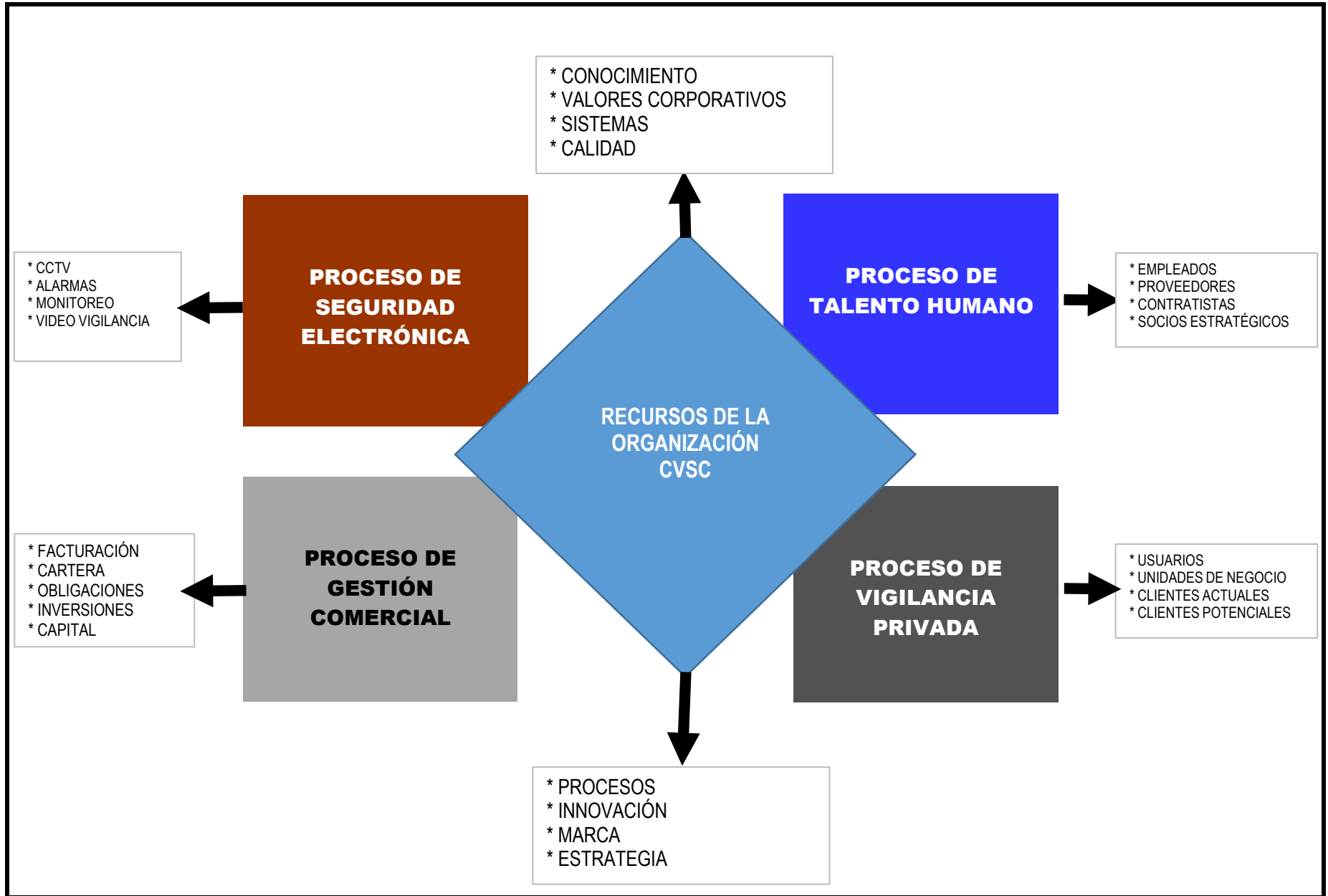
II: MAPA DE PROCESOS



CARACTERIZACIÓN DE PROCESOS ANTE EL SISTEMA DE GESTIÓN EN CONTROL Y SEGURIDAD

PROCESOS GERENCIALES			
GESTIÓN GERENCIAL (Heinz Pichler)		SISTEMAS INTEGRADOS DE GESTIÓN (Ever Polo)	
REQUISITOS DE LA NORMA BASC V4	ESTÁNDARES DE SEGURIDAD BASC V4	REQUISITOS DE LA NORMA BASC V4	ESTÁNDARES DE SEGURIDAD BASC V4
4.1 Requisitos del SGCS - BASC 4.2 Política de Control y Seguridad 4.3.4 Requisitos legales y de otra índole 4.4.1 Estructura, resp. y autoridad 4.6.1 Mejora continua 4.6.3 Compromiso de la Dirección	6.8 Criterios de seguridad	4.3.1 Planeación 4.3.2 Objetivos del SGCS 4.4.4 Documentación del sistema 4.4.5 Control de documentos 4.5.2 Auditoría	1.1 Procedimientos de seguridad 5. Seguridad en los procesos
PROCESOS OPERATIVOS			
GESTIÓN COMERCIAL (Nicolas González)		GESTIÓN DE RIESGOS (José Rivera)	SEGURIDAD DE INTALACIONES (José Rivera)
REQUISITOS DE LA NORMA BASC V4	ESTÁNDARES DE SEGURIDAD BASC V4	REQUISITOS DE LA NORMA BASC V4	ESTÁNDARES DE SEGURIDAD BASC V4
1. Requisitos de asociados de negocio	4.4.6 Control Operacional 4.5.1 Seguimiento y medición	2 Seguridad del contenedor y de la carga 2.1 Sellos del furgón y contenedor 3 Control de acceso físico 3.1 Acceso de empleados 3.2 Acceso de visitantes y proveedores 3.3 Verif. Correspondencia y paquetes 3.5 Personal de Seguridad 5.1 Información y documentos de carga 5.2 Entrega y recepción de carga	4.4.7 Prep. Resp. event critico 3.4 Ident y retiro persona no autorizada 4 Seg personal propio y temporal 6 Seguridad Física 6.1 Seguridad del perímetro 6.2 Puertas y casetas 6.3 Estacionamiento de vehículos 6.4 Estructura de los edificios 6.6 Iluminación
SEG. ELECTRONICA (Juan Delgado)			
REQUISITOS DE LA NORMA BASC V4	ESTÁNDARES DE SEGURIDAD BASC V4		
6.5 Control cerraduras y llaves 6.7 Sist. alarmas video vig. 7.2 Responsabilidad			
PROCESOS DE SOPORTE			
ADMINISTRACIÓN DEL PERSONAL (Yaneth Turriago)		ADMINISTRACIÓN FINANCIERA Y CONTABLE (Habib Simman)	
REQUISITOS DE LA NORMA BASC V4	ESTÁNDARES DE SEGURIDAD BASC V4	REQUISITOS DE LA NORMA BASC V4	ESTÁNDARES DE SEGURIDAD BASC V4
4.4.2 Entrena -Capac y toma conciencia	4 Seguridad personal propio, subcontratado y temporal 4.1 Verificación preliminar al empleo 4.2 Verific. y mnnto del personal después de contratado 4.3 Proc de terminación de vinculación laboral 8.1 Capacitación	4.3.5 Provisiones	1.2 Prevención del LA/FT
TODOS LOS PROCESOS			
REQUISITOS DE LA NORMA BASC V4	ESTÁNDARES DE SEGURIDAD BASC V4	REQUISITOS DE LA NORMA BASC V4	ESTÁNDARES DE SEGURIDAD BASC V4
4.3.3 Gestión del Riesgo 4.4.3 Comunicación	3.4 Identificación y retiro de persona no autorizada 6.5 Control de Cerraduras y llaves	4.5.3 Control de Registros 4.6.2 Acción correctiva y preventiva	7.1 Protección con contraseña 7.3 Protección a los sistemas y datos

FUENTES DE VALOR A PROTEGER



SISTEMA DE ADMINISTRACIÓN DE RIESGOS COLVISEG DEL CARIBE

III - MATRIZ DE DEFINICIÓN DE CRITICIDAD EN CARGOS

CRITERIOS DE ANÁLISIS →		IMPACTO: 1=Bajo - 3=Bajo - 7=Moderado - 10=Crítico						CALIFICACIÓN	NIVEL DE CRITICIDAD
		Manejo de la Carga	Acceso a Información Confidencial	Manejo de sistemas de información	Aplicación de medidas de protección	Toma de Decisiones	Control y Seguridad de la operación		
PROCESO	Cargo	20%	20%	10%	20%	10%	20%		100%
G. Gerencial	Gerente General	1	10	7	3	10	7	5,9	Cargo Crítico Medio
Sistemas integrados de gestión	Director Nacional SIG	3	10	10	7	7	3	6,7	Cargo Crítico Medio
Gestión Comercial	Director comercial	1	7	7	3	7	3	4,6	Cargo NO Crítico
Ventas	Director de zona	3	10	7	10	7	7	7,1	Cargo Crítico Alto
Servicio al Cliente	Asistente administrativo	7	7	10	7	10	7	8,2	Cargo Crítico Alto
Gestión de Operaciones	Director Nal. de Operaciones	10	7	10	10	7	10	9,1	Cargo Crítico Alto
Vigilancia Privada	Coordinador Operativo	7	10	7	10	7	10	8,2	Cargo Crítico Alto
Servicios de Escolta	Coordinador Operativo	1	10	3	10	1	7	4,7	Cargo NO Crítico
Gestión de Riesgos	Director Nacional SIG	1	10	3	3	10	7	5,1	Cargo Crítico Medio
Seguridad de instalaciones	Jefe de Seguridad	1	7	7	10	3	7	5,6	Cargo Crítico Medio
Gestión Seg. Electrónica	Director Nacional de IT	7	10	10	10	7	3	8,1	Cargo Crítico Alto
Medios Tecnológicos	Jefe de Seguridad	1	7	7	3	3	7	4,2	Cargo NO Crítico
Seguridad de las TIC	Jefe de Seguridad	1	7	7	7	10	10	6,7	Cargo Crítico Medio
Gestión del Talento Humano	Director Nacional de TTHH	3	10	10	7	10	3	7,3	Cargo Crítico Alto
Bienestar y RSE	Analista de Bienestar	1	10	3	7	3	3	4,1	Cargo NO Crítico
Capacitación y entrenamiento	Analista de Capacitación	1	10	10	7	10	10	7,6	Cargo Crítico Alto
Nomina	Analista de nomina	1	3	7	7	7	7	5,4	Cargo Crítico Medio
Gestión Adm. y Financiera	Director Adm. y Financiero	1	10	10	7	10	10	7,6	Cargo Crítico Alto
Tesorería	Tesorera	1	7	10	10	3	7	6,2	Cargo Crítico Medio
Compras y almacén	Coord. Administrativo Nal.	3	7	3	7	3	10	4,9	Cargo NO Crítico
Cobranzas	Coordinador de cartera	1	3	10	7	3	3	4,8	Cargo NO Crítico
Facturación	Analista de Facturación	1	7	10	7	3	7	5,6	Cargo Crítico Medio
RIESGO PROCESO ORGANIZACIÓN →		2,6	8,1	7,6	7,2	6,4	6,7	6,3	Cargo Crítico Medio

CRITERIO DE CALIFICACIÓN:

Se consideran como críticos aquellos con ponderación superior a 5.0

COLVISEG DEL CARIBE

CONTEXTO EXTERNO (Amenazas)

Factores económicos: Aparición de nuevos competidores - Interrupción de Servicios en el mercado

Factores geográficos y ambientales: Proximidad al mar y al río Magdalena - Aeropuerto Internacional - Inundación - Ambiente laboral desfavorable

Factores tecnológicos: Ataques cibernéticos - Sabotajes - Suplantación de proveedores

Factores políticos: Bloqueos de vías - Revueltas populares - Cambio de política fiscal

Factores sectoriales: Calidad de insumos - Competencias laborales deficientes

CONTEXTO INTERNO (Vulnerabilidades)

Factores humanos: Perfiles puestos para procesos críticos - Incorporación P. críticos - Negligencia - Desvinculación P. críticos

Factores técnicos: Incendios - Explosiones - Cambios de voltaje - Electrificación - Cambios de insumos - Daños de equipos - Apagones

Factores financieros: Evaluación inadecuada de Contratos - Errores en cotización - Insuficiencia de recursos - Sobrecostos

Factores operativos: Diseño inadecuado de procesos críticos - Procedimientos inadecuados - Incumplimiento de Compromisos

Factores de estructura: Sabotaje - Colapso - Corrosión - Agua estancada - Taponamientos

Factores de resultados: Fraude - Hurto - Contaminación de carga - Contaminación ambiental - Suspensión abrupta de contrato

SISTEMA DE ADMINISTRACIÓN DE RIESGOS
V - IDENTIFICACIÓN DE RIESGOS
COLVISEG DEL CARIBE

REQUISITO	PROCESO	SUBPROCESO O PROCEDIMIENTO	ACTIVIDAD O COMPROMISO	¿Qué puede suceder?	¿ Cuando o Donde?	¿Como o Porque puede suceder?	RIESGO	ENFOQUE DE PÉRDIDA
PROCESOS GERENCIALES								
GESTIÓN GERENCIAL (Heinz Pichler)								
N4.1	Gestión Gerencial	Procedimientos de la organización	Incorporación de los requisitos del SGCS a todos los procesos de la organización	Algunos procesos no están caracterizados de acuerdo con los requisitos del SGCS	Al presentarse una falla el algún cliente se determina que es por deficiencia de control en nuestro proceso.	No se tuvieron en cuenta los riesgos del entorno en el cual se opera.	Algún cliente OEA al verificar sus procesos puede detectar incumplimientos de parte nuestra	Alta Dirección
N4.2	Gestión Gerencial	Requisitos del sistema de gestión en control y seguridad OEA	Política de Control y Seguridad	No esta Documentada, comunicada, publicada o respaldada su política de control y seguridad.	Al verificar el servicio se evidencia desconocimiento de la política de Control y Seguridad	No se implemento o no fue clara la difusión de la política de Control y Seguridad	Falta de prevención de actividades ilícitas por falta de una política de seguridad claramente difundida y entendida	Alta Dirección
N4.3.4	Gestión Gerencial	Requisitos legales y de otra índole	Renovación de permisos y licencias ante la alcaldía y otros entes del gobierno.	Vencimiento de Licencia para Funcionamiento, inspecciones de bomberos y otros documentos obligatorios	Al termino del vencimiento de las actuales licencias.	Por descuido es posible que se omitan los tramites de renovación de los permisos legales.	Multas elevadas y/o cancelación temporal o definitiva de las licencias y permisos de funcionamiento.	Alta Dirección
N4.4.1	Gestión Gerencial	Estructura, responsabilidad y autoridad	La responsabilidad final por el control y seguridad de la organización	No designación del representante de la Alta Dirección para asegurar el SGCS	Deficiencias en el control y seguridad de la organización	Por detección de ineffecticia del SGCS en la practica.	No establecer y/o documentar funciones, responsabilidades y autoridad del personal que afecta la seguridad.	Alta Dirección
N4.6.1	Gestión Gerencial	Mejora Continua	Mejorar continuamente la eficacia del sistema de gestión de control y seguridad OEA	No tener establecida política u objetivos relacionados con la mejora continua	En desarrollo de tareas por parte de personal en misión o donde se suministren equipos	Controles son inadecuados u obsoletos	Incumplimiento de la política y objetivos del control y seguridad	Continuidad del negocio

REQUISITO	PROCESO	SUBPROCESO O PROCEDIMIENTO	ACTIVIDAD O COMPROMISO	¿Qué puede suceder?	¿ Cuando o Donde?	¿Como o Porque puede suceder?	RIESGO	ENFOQUE DE PÉRDIDA
N4.6.3	Gestión Gerencial	Compromiso de la Dirección	Realizar a intervalos planificados revisiones al SGCS	No se realizó ninguna revisión por parte de la alta dirección al SGCS en el ultimo año.	Desde que se tomo la decisión de implementar el sistema hasta la auditoria.	A pesar del requerimiento del área de SIG no se dispuso del tiempo.	Perder la certificación del SGCS por el OEA	Alta Dirección
E6.8.1	OEA	Otros criterios de seguridad	Tener un Jefe o responsable de la seguridad con funciones documentadas	El Jefe o responsable de la seguridad no tiene funciones documentadas	Ante un evento de pérdida o hurto no hay quien asuma la investigación administrativa	Descuido o falta en la implementación de controles.	Fallas en la protección de las instalaciones por no contar con responsable de la seguridad.	Seguridad Física
SISTEMAS INTEGRADOS DE GESTIÓN (Ever Polo)								
N4.3.1	Gestión de auditoria del SIG	Planeación Generalidades	El éxito o fracaso del SGCS depende de una adecuada planificación.	Falta de criterios de cumplimiento de los requisitos en los procedimientos de control y seguridad que tiene la compañía.	Desempeño de tareas específicas del personal en misión poco eficiente.	Falto definir que se debe hacer, quien es el responsable, cuando hacerlo y cual el resultado esperado.	Incumplimiento de requisitos en materia de control y seguridad	Administración y logística
N4.3.2	OEA	Objetivos del SGCS	Establecimiento y revisión de los objetivos del SGCS en las funciones y niveles pertinentes dentro de la Organización	Falta coherencia en algunos objetivos.	Algunos de los niveles de la organización desconocen sus funciones en cuanto al SGCS	Por falta de difusión del SGCS o por descuido del responsable.	Incumplimiento de la política de control y seguridad a través de indicadores de gestión.	Capacitación y Entrenamiento
N4.4.4	OEA	Documentación del sistema	Manual del Sistema de gestión en Control y Seguridad	No se implementó de manera efectiva el SGCS.	Al revisar el SGCS por un cliente puede encontrar inconsistencias que no son aplicables a nuestra organización.	No se Justificaron en el manual debidamente las exclusiones a normas o estándares.	Algunos procedimientos y registros requeridos por OEA que son responsabilidad del cliente pueden ser indiligados a Colviseg del Caribe.	Operaciones de carga
N4.4.5	Gestión de auditoria del SIG	Control de documentos	Listados Maestros aprobados documentados y revisados periódicamente.	El listado maestro no permite controlar los documentos requeridos para implementar el SGCS - OEA	Su localización es complicada por lo cual no es oportuna.	No se controlan documentos de origen externo o interno importantes para el SGCS	No disponer de un sistema para la protección y recuperación de documentos sensibles tanto físicos como magnéticos	Protección de documentos

REQUISITO	PROCESO	SUBPROCESO O PROCEDIMIENTO	ACTIVIDAD O COMPROMISO	¿Qué puede suceder?	¿ Cuando o Donde?	¿Como o Porque puede suceder?	RIESGO	ENFOQUE DE PÉRDIDA
N4.4.7	Gestión de auditoria del SIG	Implementación y operación	Preparación y respuesta a eventos críticos	Falta plan de contingencia y emergencia para dar adecuada respuesta a eventos críticos	En el momento de presentarse la crisis no hay procedimientos documentados generando caos.	Falta de prevención mediante ejercicios prácticos o simulacros.	Incrementar la criticidad del evento ante la imprevisión.	Seguridad y salud en el trabajo SST
N4.5.2	Gestión de auditoria del SIG	Auditoria	Tener un procedimiento documentado para realizar auditorias internas a los elementos del SGCS	No verificar el cumplimiento de las norma y estándares OEA	Durante por lo menos una auditoria interna.	Por incompetencia o falta de independencia de los auditores asignados.	No se elaboro o ejecuto el programa de auditorias internas	Control de Calidad
E1.1	OEA	Procedimientos de seguridad	Tener procedimientos documentados para evaluar a los Asociados de Negocio	No contar con documentación que indique si los asociados de negocio están certificados OEA o cuentan con un proceso documentado de gestión de riesgos	Al verificar programas de seguridad en asociados de negocio en la cadena de suministros que sean administrados por autoridad aduanera.	Por falta de acuerdos de seguridad para asociados de negocio no certificados OEA	Prestación de servicios a empresas que tienen graves deficiencias de seguridad para protección de sus mercancías.	Operaciones de carga
E5	Gestión de auditoria del SIG	Seguridad en los Procesos	Contar con procedimientos que establezcan medidas de seguridad	No asegurar la integridad de los procesos relevantes de la cadena de suministros	En servicios prestados a la cadena de suministros.	Como participantes en actividades de comercio exterior	Falta de competencia y confiabilidad del personal asignado para la prestación de servicios	Cadena de suministros
E6.8.2	Gestión de auditoria del SIG	Otros criterios de seguridad	Plano de ubicación de áreas críticas	No se han establecido las áreas críticas de las instalaciones.	Acceso de personal no autorizado a las áreas sensibles sin que nadie tome acción	Nadie sabe donde están ubicadas las áreas críticas de la organización.	Pérdida de información datos o sabotaje.	Seguridad Física
6.8.5	OEA	Otros criterios de seguridad	Sistemas adecuados para la comunicación oportuna con supervisores, encargados de seguridad de los clientes y con autoridades	No disponer de sistemas adecuados para la comunicación personal en servicio que cumple tareas criticas para la seguridad del cliente.	En caso de detectar alguna actividad sospechosa por parte del guarda o escolta.	No poderse comunicar el trabajador con la persona encargada de la seguridad de la empresa	Falta de medios para comunicación del personal de vigilancia o escolta con la empresa.	Medios tecnológicos

REQUISITO	PROCESO	SUBPROCESO O PROCEDIMIENTO	ACTIVIDAD O COMPROMISO	¿Qué puede suceder?	¿ Cuando o Donde?	¿Como o Porque puede suceder?	RIESGO	ENFOQUE DE PÉRDIDA
6.8.7	Gestión de auditoria del SIG	Otros criterios de seguridad	Plan de emergencia con procedimientos documentados y dispositivos de alerta, acción y evacuación.	Evento no deseado de tipo natural o provocado que obligue a la evacuación total o parcial de instalaciones.	Taponar cañerías o desagües sobrecargando la plancha generando goteo o inundación por rebosamiento	Falla en las medidas de protección	Suspensión temporal de actividades en la sede por incidente que obligue a la evacuación.	Mantenimiento
PROCESOS OPERATIVOS								
GESTIÓN COMERCIAL (Nicolas González)								
E1	Gestión Gerencial	Requisitos de asociados de negocio	Procedimientos documentados y verificables para la selección de clientes, proveedores y terceras partes	Prestación de servicios a empresas que tienen graves deficiencias de seguridad para protección de sus mercancías	Cuando se consulta en lista Clinton o den la Base de datos de la Fiscalía.	Omitir verificación en organismos de control nacional e internacional	Asociados de negocios con reporte negativo OFAC (Office of Foreign assets Control)	Comercialización y mercadeo
GESTIÓN DE RIESGOS (José Rivera)								
N4.4.6	Servicio de Vigilancia	Control Operacional	Asegurar con base en la evaluación de riesgos la participación en la cadena de suministro y actividades del comercio exterior	Que planes, programas y controles no estén integrados	Al verificar la efectividad al implementar la política y la gestión efectiva de control y seguridad	Las actividades relacionadas con el comercio internacional no se realizan de manera segura	Que los planes y programas de seguridad no estén totalmente integrados en toda la organización y sus actividades	Cadena de suministros
N4.4.7	Gestión de Riesgos	Preparación y respuesta a eventos críticos	Procedimiento documentado para identificar y responder ante amenazas y vulnerabilidades	No dar respuesta oportuna ante situaciones críticas.	Cuando la organización o el cliente carecen de planes de contingencia y emergencia.	Omitieron realizar ejercicios prácticos o simulacros	Falta de eficacia en las medidas de protección.	Seguridad Industrial
N4.5.1	Gestión de Riesgos	Seguimiento y Medición	Tener procedimientos para el seguimiento y medición de las características claves con impacto en el control y seguridad	No están documentados los procedimientos o no se ajustan para el seguimiento y medición de la organización	Que en verificación de auditoria se consideren ineficaces los instrumentos de medición y seguimiento.	No se dispone de indicadores claves para medir impacto significativo en el control y seguridad	Los indicadores no se ajustan a las necesidades de la organización o no determinan la eficacia del SGCS OEA	Monitoreo del SGCS

REQUISITO	PROCESO	SUBPROCESO O PROCEDIMIENTO	ACTIVIDAD O COMPROMISO	¿Qué puede suceder?	¿ Cuando o Donde?	¿Como o Porque puede suceder?	RIESGO	ENFOQUE DE PÉRDIDA
E2	Gestión de Riesgos	Seguridad al contenedor y de la carga	Convenir con asociados de negocio importadores o exportadores, sean o no OEA respecto a la importancia de tener procedimientos de seguridad en el lugar de la carga.	Llenar un contenedor que no es apto para ser cargado porque el encargado de inspeccionarlo no tiene las competencias necesarias	En el punto de embarque de origen o de destino encontrar la estructura del contenedor contaminada.	Incorrecta asignación del personal encargado de la inspección.	Contaminación de Contenedor o del medio de transporte antes del llenado.	Transporte unimodal
E2.1	Servicio de Vigilancia	Sellos del Furgón o contenedor / ULD	Convenir con los asociados de negocios el uso de sellos de alta seguridad que cumplan o excedan los requisitos ISO 17712	Que no se mantenga la integridad de los sellos por alteración o cambio	En el punto de control de acceso vehicular en la entrada o salida.	Uso de sellos no certificados, adulteración o cambio	Sellos manejados por personal que no tiene las competencias para ello o autorizaciones de salida o ingreso irregulares.	Protección de contenedores
E3	Servicio de Vigilancia	Control de acceso físico	Impedir la entrada no autorizada a las instalaciones	Ingreso de personas ajenas a las instalaciones	Cuando no se de cumplimiento a los protocolos	Evasión de los controles establecidos	Ingreso de personal no autorizado a áreas restringidas	Controles de Acceso
E3.1	Servicio de Vigilancia	Empleados	Identificación positiva de empleados	Ingreso a una área sensible de ex trabajador o mediante suplantación de empleado autorizado.	Área restringida de un cliente suplantando trabajador en misión o de las oficinas administrativas de Colviseg del Caribe.	Por deficiente señalización o incumplimiento del control de devolución de carnés.	Falta de control de la devolución de carnés de identificación de empleados.	Controles de Acceso
E3.2	Gestión de Riesgos	Visitantes, Vendedores y Proveedores	Registro diario de visitantes y proveedores.	Ingreso de personal no autorizado a las instalaciones de Colviseg del Caribe.	Burlando el control de la recepcionista de Colviseg del Caribe o ingresando por acceso no convencional	Aprovechando procesos de selección en CVSC o las salidas de técnicos en Colviseg del Caribe.	Intrusión diurna de banda con fines delictivos.	Controles de Acceso
E3.3	Gestión de Riesgos	Verificación de correos y paquetes de correspondencia	Registro de correos y paquetes recibidos antes de ser distribuidos.	Ingreso de paquetes con artefacto explosivo o incendiario a instalaciones de Colviseg del Caribe o de un cliente donde se tenga conserjería.	Cuando se tengan amenazas contra las personas o las instalaciones.	Por no examinar todo correo o paquete recibido.	Lesiones personales graves y caño a instalaciones por artefacto explosivo o incendiario.	Control de correspondencia

REQUISITO	PROCESO	SUBPROCESO O PROCEDIMIENTO	ACTIVIDAD O COMPROMISO	¿Qué puede suceder?	¿ Cuando o Donde?	¿Como o Porque puede suceder?	RIESGO	ENFOQUE DE PÉRDIDA
E3.5	Servicio de Vigilancia	Personal de seguridad	Asegurar que su personal de seguridad está controlando las puertas de entrada y salida de las instalaciones.	Falta de control en las áreas de almacenamiento, manejo de equipos, contenedores y carga.	En instalaciones de asociados de negocio donde se manejen envíos internacionales	Falta de control y protección contra personas no autorizadas puedan acceder a la carga para exportación.	Deficiencias del personal en el control de las áreas claves de manejo de la carga	Seguridad Física
E5.1	Gestión de Riesgos	Manejo y procesamiento de información y documentos	Garantizar la coherencia de la información en los registros de control de acceso y la del control de la carga.	Inconsistencias entre los documentos o de información en medio magnético o en papel.	Al comparar los documentos de transporte con los registros de las porterías	Falta de medidas de protección informática o de medidas de protección de la documentación crítica.	Descuidos en la verificación y comparación de los datos contenidos en registros de control led accesos y los documentos de carga	Protección de documentos
E5.2	Gestión de Riesgos	Entrega y Recepción de Carga	Verificar con exactitud la carga que entra o sale contra la información del manifiesto	Discrepancias en la carga o en la información contenida en el manifiesto	Durante el recibo de carga en el punto de destino por diferencia de datos.	Falta de identificación de conductores o vehículos de carga	Falta de registro fotográfico o filmico antes durante y después del proceso de cargue o descargue	Administración y logística
E.6	Seguridad de Instalaciones	Seguridad Física	Instalaciones donde manejen documentación, información crítica o elementos vitales para la prestación del servicio de carga deben resguardarse contra acceso no autorizado	Pérdida, daño o alteración de documentos e información	Inundación por taponamiento de cañerías o debido a filtraciones de agua goteras al archivo físico y por acción de ciberataque al archivo magnético.	Falta de barreras físicas y/o elementos de seguridad para evitar acceso no autorizado	Destrucción de la memoria de la empresa obligando a reconstrucción	Protección de documentos
E6.1	Seguridad de Instalaciones	Seguridad del perímetro	Contar con cerramiento perimetral, cercas, barreras interiores, inspeccionadas con regularidad verificando su integridad.	Intrusión por deficiencias en la barrera perimetral incluyendo techo y pisos	En horas de la noche y días no laborales	Neutralizando la seguridad electrónica	Sustracción de Bienes de propiedad de la organización	Seguridad Física
E6.2	Seguridad de Instalaciones	Puertas y casetas	Mantenerlas controladas, monitoreadas y supervisadas tanto las d entrada y salida de vehículos como las de personal.	Daño o deterioro del CCTV limitando la supervisión y control.	No poseer evidencia de la manera como los guardas realizan su labor.	Por fallas en los dispositivos de video grabación.	No mantenerse al mínimo necesario la cantidad de puestas y casetas habilitadas para entradas y salidas	Seguridad Física

REQUISITO	PROCESO	SUBPROCESO O PROCEDIMIENTO	ACTIVIDAD O COMPROMISO	¿Qué puede suceder?	¿ Cuando o Donde?	¿Como o Porque puede suceder?	RIESGO	ENFOQUE DE PÉRDIDA
E6.3	Seguridad de Instalaciones	Estacionamiento de Vehículos	Control en áreas de estacionamiento de vehículos privados.	Acto terrorista mediante carro bomba	En días laborales cuando es difícil detectar vehículos no habituales estacionando frente a la sede.	Permisividad de estacionamiento de vehículos particulares en cualquier sitio.	Dstrucción instalaciones críticas del negocio por carro bomba.	Continuidad del negocio
E6.4	Seguridad de Instalaciones	Estructura del Edificio	Resistencia a la entrada forzada o ilegal.	Colapso estructural	Del techo o las paredes laterales, permitiendo el fácil acceso	Por humedad debido a la retención de aguas lluvias por fallas en desagües y tuberías	Caída parcial de la estructura	Mantenimiento
E6.6	Seguridad de Instalaciones	Iluminación	Contar con una buena iluminación dentro y fuera de las instalaciones	Falta de efectividad de las cámaras y de la vigilancia humana en áreas oscuras	En caso de intrusión no habrá observación del hecho ni por el guarda ni por el CCTV	La oscuridad es un factor facilitador del actuar delincriminal.	Falta de iluminación en los accesos convencionales, barrera perimétrica o parqueaderos.	Administración y logística
SEG. ELECTRONICA (Juan Delgado)								
E6.5	Medios Tecnológicos	Seguridad Física	Control de cerraduras y llaves	Las áreas críticas no cuentan con mecanismos de cierre o no están controladas.	Se pierde el control de llaves o claves de acceso a áreas críticas	Permite el acceso de personal no autorizado o fuera de horarios estipulados	Perdida de información confidencial o de equipos de alto costo	Controles de Acceso
E6.7	Medios Tecnológicos	Sistema de alarmas y videocámaras de vigilancia	Supervisar y monitorear las instalaciones para prevenir acceso no autorizado a las áreas críticas.	Perdida, hurto o daño o daño a bienes	En una o varias áreas críticas de la compañía	Por la carencia de medios electrónicos de detección y respuesta a eventos de inseguridad.	Intrusión a áreas críticas no detectada con fines delictivos,	Medios tecnológicos
E7.2	Seguridad de las tecnologías de la información y comunicaciones	Responsabilidad y control de la información	Controlar la documentación e información en los medios magnéticos contra acceso no autorizado	Borrado o alteración de la información por pirata informático.	Desde dentro o mediante acceso remoto a la red local.	Manipulación indebida para alteración de datos del negocio.	Perdida de documentos o información en los equipos de computo.	Informática y sistematización de datos

REQUISITO	PROCESO	SUBPROCESO O PROCEDIMIENTO	ACTIVIDAD O COMPROMISO	¿Qué puede suceder?	¿ Cuando o Donde?	¿Como o Porque puede suceder?	RIESGO	ENFOQUE DE PÉRDIDA
PROCESOS DE SOPORTE								
ADMINISTRACIÓN DEL PERSONAL (Yaneth Turriago)								
N4.4.2	Gestión de Talento Humano	Entrenamiento, Capacitación y toma de Conciencia	Determinar y demostrar las competencias requeridas del personal y tomar las acciones necesarias.	El personal en no esta dando el rendimiento esperado en el puesto de trabajo debilitando la cadena de suministro	Al momento de realizar su evaluación de desempeño.	Por deficiencias en su inducción o entrenamiento.	Falta de conciencia de la responsabilidad y la influencia de su acción u omisión sobre la eficacia del SGCS OEA	Capacitación y Entrenamiento
E4	Gestión del Talento Humano	Seguridad del personal propio, subcontratado y temporal	Procedimiento documentado para evaluar los candidatos con posibilidad de ser contratados.	Suministro de personal con antecedentes judiciales.	Cuando ocurre un evento de hurto en el cual se vea nuestro trabajador comprometido.	No se verificaron antecedentes ni se realizo la vida domiciliaria.	Causar perjuicio a un cliente por comportamiento criminal de un trabajador en misión	Selección de personal
E4.1	Gestión del Talento Humano	Verificación preliminar al empleo	Procedimientos para verificar información de la solicitud de empleo e investigar antecedentes del candidato.	Contratar personal con antecedentes judiciales o documentación Falsa.	Auditorias del cliente evidencias irregularidad en la contratación	Falto la verificación de antecedentes laborales y referencias de la HDV	Pérdida del cliente por no cumplir los requisitos exigidos del personal asignado	Selección de personal
E4.2	Gestión del Talento Humano	Verificación y mantenimiento del personal después de la contratación	Lista actualizada de empleados propios y subcontratados con datos personales de relevancia.	No realizar revisiones periódicas permitiendo datos y fotos desactualizadas.	Como resultado de auditoria detección de trabajador retirado a quien lo le recogieron los uniformes.	Por falta de registros de fotos o datos que permitan su localización para reclamarlos.	Suplantación de empleados o trabajadores con fines delictivos.	Seguridad Física
E4.3	Gestión de Bienestar y RSE	Procedimiento de terminación de la vinculación laboral.	Retiro de la identificación, eliminación de permisos y claves de acceso a instalaciones y sistemas.	Ingreso no autorizado de ex trabajadores al sistema o a las instalaciones.	Utilizando ingreso remoto a la red interna o aprovechando visita después de desvinculado.	Al retiro no se bloquearon los accesos a la pagina de la empresa como trabajador activo o a las áreas citicas donde laboraba.	Perdida o adulteración de información o sustracción de documentación clasificada.	Controles de Acceso
E8	Capacitación y entrenamiento	Entrenamiento de seguridad y concientización sobre amenazas	Contar con un programa anual de capacitación sobre como reconocer y reportar amenazas y vulnerabilidades.	No reconocer conspiraciones internas o divulgar innecesariamente información confidencial.	Deficiencias en el control y seguridad de los procesos de seguridad durante cargue y descargue de mercancías.	No se dio capacitación adicional a personal de envíos y recibos de carga al desconocer procedimientos establecidos	Desconocer el procedimiento para considerar una situación y como reportarla.	Cadena de suministros

REQUISITO	PROCESO	SUBPROCESO O PROCEDIMIENTO	ACTIVIDAD O COMPROMISO	¿Qué puede suceder?	¿ Cuando o Donde?	¿Como o Porque puede suceder?	RIESGO	ENFOQUE DE PÉRDIDA
ADMINISTRACIÓN FINANCIERA Y CONTABLE (Habib Simman)								
N4.3.5	Gestión de Tesorería	Previsiones	Presupuesto para cubrir los objetivos, planes y controles operacionales.	La organización no podría implementar, mantener y mejorar controles	En los procesos de manejo de carga o almacenamiento seguro.	No contar con los medios adecuados para evitar posibles contaminaciones.	Limitaciones en medios o recursos para el control de la integridad de las mercancías de acuerdo a lo contratado.	Administración y logística
E1.2	Gestión de Compras y Almacén	Prevención del lavado de activos y financiación del terrorismo.	Aplicar proceso de selección y evaluación de asociados de negocio, antecedentes legales, penales financieros y reporte de operaciones sospechosas.	Prestación de servicios a empresas fachada de grupos terroristas u organizaciones dedicadas al lavado de activos.	Reporte e investigación de la UIAF que conlleven a acciones legales contra asociado de negocio.	Incumplimiento de normas estipuladas en la circular 170 de 2002	Prestación de servicios a clientes relacionados con Bandas Criminales u otras organizaciones al margen de la ley	Actividades de comercio exterior
TODOS LOS PROCESOS								
N4.3.3	Requisitos del Sistema de Gestión en Control y Seguridad	Gestión del Riesgo	Tener un procedimiento documentado de Gestión del Riesgo a nivel de toda la organización.	Desconocimiento de los riesgos dentro de cada uno de los procesos.	En procesos internos o de un cliente en el cual tengamos personal en servicio.	Desconocen o no se revalúan los riesgos por lo menos una vez al año	Fallas en el sistema de control y seguridad por no tener en cuenta nuevas amenazas o vulnerabilidades.	Seguridad Física
N4.4.3	Requisitos del Sistema de Gestión en Control y Seguridad	Comunicación	Condiciones para mantener la comunicación abierta y efectiva de información sobre el control y seguridad en el comercio internacional.	No lograr el compromiso de accionistas, directivos, empleados y asociados de negocio	En el control de los cargues o descargues y en la seguridad del contenidos.	Falta de competencias del personal asignado o de compromiso con el control y seguridad.	Limitaciones para comunicar acto sospechoso de contaminación de carga, contrabando o trafico de armas.	Operaciones
N4.5.3	Requisitos del Sistema de Gestión en Control y Seguridad	Control de Registros	Llevar los registros necesarios para demostrar conformidad con los requisitos del SGCS OEA	No contar con un listado maestro de registros	Durante la identificación, mantenimiento y disposición de estos registros	Los registros no son legibles, identificables y rastreables de acuerdo con la actividad.	Listado maestro de registros no contempla identificación, mantenimiento, disposición para entrega control y archivo de la información.	Protección de documentos

REQUISITO	PROCESO	SUBPROCESO O PROCEDIMIENTO	ACTIVIDAD O COMPROMISO	¿Qué puede suceder?	¿ Cuando o Donde?	¿Como o Porque puede suceder?	RIESGO	ENFOQUE DE PÉRDIDA
N4.6.2	Requisitos del Sistema de Gestión en Control y Seguridad	Acción correctiva y preventiva	Tener procedimientos documentados para la implementación de las acciones correctivas y preventivas	Se evidencia no conformidad real o potencial a la cual no se aplico ninguna acción	Al revisar desviaciones del SGCS o identificar causas de situaciones no conformes.	No verificar la eficacia de las acciones tomadas	No aplicar acción correctiva y preventiva ante una no conformidad real o potencial detectada en el SGCS.	Monitoreo del SGCS
E3.4	Control de Acceso físico	Identificación y retiro de personas no autorizadas	Procedimiento documentado para identificar, dirigirse y retirar a personas no autorizadas.	Agresión física contra intrusos sorprendidos en flagrancia.	Dentro de las instalaciones de cogiten o de un usuario en áreas donde se tenga personal en misión.	Desconocimiento o no existencia de procedimientos con personas sorprendidas dentro de la instalación.	Demandas de tipo penal por mal trato o lesiones a personas sorprendidas dentro de las instalaciones.	Controles de Acceso
E6.5	Seguridad Física	Control de Cerraduras y llaves	Mecanismos de cierre de puertas y ventanas, cerraduras llaves y claves de acceso	Acceso a área crítica por parte del personal no autorizado	Días y horas no laborales a oficinas donde se manejen datos con información confidencial	Por descuido en el cierre de ventanas y puertas de área crítica.	Ingreso a área crítica en horario no laboral por acceso no convencional	Controles de Acceso
E7.1	Seguridad en las tecnologías de la información	Protección con contraseña	Políticas, procedimientos y normas de tecnología de la información	Acceso desde un equipo de computo de la entidad por persona no autorizada	En ausencias temporales o en horario no laboral del asignado	Descuido al no apagarlo o suministro de clave de acceso a tercero.	Sustracción de información por desconocido desde un equipo de la organización	Medios tecnológicos
E7.3	Seguridad en las tecnologías de la información	Protección a los sistemas y datos	Actualización de Software anti virus y anti-espía	Infiltración por parte de competidores del mercado.	Cuando se preste servicio a clientes exportadores o importadores.	Desactualización de software de protección.	Infracción al sistema de seguridad de tecnologías de la información	Informática y sistematización de datos

RESULTADOS ESTIMADOS Y CONSIDERADOS EN EL MOMENTO DE SU MEDICIÓN

VI - MATRIZ DE EVALUACIÓN DEL RIESGO

RIESGO	Débil	Limitado	Notable	Fuerte	Extremo	IMPACTO	PROBABILIDAD
	1	2	3	4	5		
Permanente	20%	40%	60%	80%	100%	Evidente	
5	5	10	15	20	25	5	
Recurrente	16%	32%	48%	64%	80%	Factible	
4	4	8	12	16	20	4	
Periódica	12%	24%	36%	48%	60%	Moderada	
3	3	6	9	12	15	3	
Esporádica	8%	16%	24%	32%	40%	Remota	
2	2	4	6	8	10	2	
Muy Poca	4%	8%	12%	16%	20%	Ninguna	
1	1	2	3	4	5	1	
VULNERABILIDAD	Insignificante	Menor	Grave	Muy seria	Fatal		
	1	2	3	4	5		

MATRIZ DE TOLERANCIA

TOLERANCIA AL	ESCENARIO	DESCRIPCIÓN
Aceptable	$VR \leq 25 \%$	No representa un daño o pérdida significativa por lo que no amerita la inversión inmediata de recursos y no requiere de una acción específica para su gestión.
Afrontable	$VR > 25 \% \leq 50 \%$	Representa un daño o pérdida significativa pero que puede ser solucionada con la inversión de recursos ya presupuestados.
Crítica	$VR > 50 \% \leq 75 \%$	Representa un daño o pérdida de mayor nivel por lo que se requiere de un plan de acción específico y adición presupuestal con intervención de la alta dirección.
Desastrosa	$VR > 75 \% \leq 100 \%$	Se requiere desarrollar acciones de mayor nivel debido al alto impacto que tendría sobre los sistemas y procesos, se requiere de un plan de acción estratégico e inversiones de capital que son competencia de la junta de socios o accionistas.

#	SUBPROCESO O PROCEDIMIENTO	ACTIVIDAD O COMPROMISO	RIESGO	Controles Existentes	I	P	R.A.	Controles Sugeridos	RIESGO ESPERADO
PROCESOS GERENCIALES									
GESTIÓN GERENCIAL (Heinz Pichler)									
N4.1	Procedimientos de la organización	Incorporación de los requisitos del SGCS a todos los procesos de la organización	Algún cliente DEA al verificar sus procesos puede detectar incumplimientos de parte nuestra	* Procedimiento de control del Servicio ** Alertas del área comercial.	4,0	3,0	3,5	Llevar el conocimiento y aplicación de acuerdos contractuales de clientes críticos a las partes interesadas.	MEDIO
N4.2	Requisitos del sistema de gestión en control y seguridad DEA	Política de Control y Seguridad	Falta de prevención de actividades ilícitas por falta de una política de seguridad claramente difundida y entendida	* Política de Gestión del riesgo ** Capacitación y entrenamiento.	4,0	2,0	2,8	Establecer un medio de difusión de la política de seguridad a todos los niveles de la organización.	BAJO
N4.3.4	Requisitos legales y de otra índole	Renovación de permisos y licencias ante la alcaldía y otros entes del gobierno.	Multas elevadas y/o cancelación temporal o definitiva de las licencias y permisos de funcionamiento.	* Proc. Control de documentos ** Alertas de Asistente de Gerencia.	5,0	3,0	3,9	Diseñar programa de alerta previa para tramitación de permisos y licencias en equipo de la asistente de Gerencia.	MEDIO
N4.4.1	Estructura, responsabilidad y autoridad	La responsabilidad final por el control y seguridad de la organización	No establecer y/o documentar funciones, responsabilidades y autoridad del personal que afecta la seguridad.	* Procedimiento de instalación de servicios ** Procedimiento de gestión del riesgo	4,0	5,0	4,5	Establecer que cada contrato sea conocido por las partes interesadas de la organización para lo de su competencia.	ALTO
N4.6.1	Mejora Continua	Mejorar continuamente la eficacia del sistema de gestión de control y seguridad DEA	Incumplimiento de la política y objetivos del control y seguridad	* Procedimiento de mejora continua ** Acciones preventivas y correctivas	3,0	2,0	2,4	Continuar con la verificación de recomendaciones o acciones de mejora de seguridad en actividades críticas de la cadena de suministros	BAJO
N4.6.3	Compromiso de la Dirección	Realizar a intervalos planificados revisiones al SGCS	Perder la certificación del SGCS por el DEA	* Política de gestión del Riesgo ** Procedimiento de control de documentación	4,0	4,5	4,2	Incrementar las revisiones del SGCS con el fin de mantener las certificaciones pertinentes.	ALTO

#	SUBPROCESO O PROCEDIMIENTO	ACTIVIDAD O COMPROMISO	RIESGO	Controles Existentes	I	P	R.A.	Controles Sugeridos	RIESGO ESPERADO
EI	Requisitos de asociados de negocio	Procedimientos documentados y verificables para la selección de clientes, proveedores y terceras partes	Asociados de negocios con reporte negativo OFAC (Office of Foreign assets Control)	* Evaluación y selección de clientes ** Verificación con autoridades.	4,5	3,0	3,7	Verificar en archivos de organismos nacionales e internacionales.	MEDIO
SISTEMAS INTEGRADOS DE GESTIÓN (Ever Polo)									
N4.3.1	Planeación Generalidades	El éxito o fracaso del SGCS depende de una adecuada planificación.	Incumplimiento de requisitos en materia de control y seguridad	* Inspecciones periódicas al SGCS ** Análisis de riesgos.	3,0	4,0	3,5	Revisar el cubrimiento con cámaras de vigilancia de todo el perímetro	MEDIO
N4.3.2	Objetivos del SGCS	Establecimiento y revisión de los objetivos del SGCS en las funciones y niveles pertinentes dentro de la Organización	Incumplimiento de la política de control y seguridad a través de indicadores de gestión.	* Manual de funciones y responsabilidad ** Índices de gestión.	3,2	3,0	3,1	Establecimiento claro por escrito de las funciones y responsabilidades de los actores en cadenas de suministros.	MEDIO
N4.4.4	Documentación del sistema	Manual del Sistema de gestión en Control y Seguridad	Algunos procedimientos y registros requeridos por OEA que son responsabilidad del cliente pueden ser indilgados a Colviseg del Caribe.	* Inspecciones de riesgos ** Análisis de riesgos.	3,0	4,0	3,5	Revisión mensual de barreras de protección y posibles accesos no convencionales	MEDIO
N4.4.5	Control de documentos	Listados Maestros aprobados documentados y revisados periódicamente.	No disponer de un sistema para la protección y recuperación de documentos sensibles tanto físicos como magnéticos	* Proce. Control de documentos ** Manual de operaciones.	3,0	2,0	2,4	Establecer cronograma de actualización de listados maestros de registros y documentos.	BAJO
N4.4.7	Implementación y operación	Preparación y respuesta a eventos críticos	Incrementar la criticidad del evento ante la imprevisión.	* Proc. De contingencia y emergencia ** Vehículo de rescate	3,0	2,0	2,4	Verificación periódica de idoneidad y entrenamiento de Brigadas y equipos de emergencia.	BAJO
N4.5.2	Auditoria	Tener un procedimiento documentado para realizar auditorias internas a los elementos del SGCS	No se elaboro o ejecuto el programa de auditorias internas	* Plan de auditorias ** Procedimiento de gestión del riesgo	3,0	2,0	2,4	Hacer un plan de auditorias internas y externas en el mes de diciembre para dar cumplimiento todo el año y contar con auditores certificados	BAJO
EI.1	Procedimientos de seguridad	Tener procedimientos documentados para evaluar a los Asociados de Negocio	Prestación de servicios a empresas que tienen graves deficiencias de seguridad para protección de sus mercancías	* Procedimiento de gestión comercial ** Procedimiento de gestión del riesgo.	5,0	3,0	3,9	Actualizar el sistema de evaluación de asociados de negocios.	MEDIO
ES	Seguridad en los Procesos	Contar con procedimientos que establezcan medidas de seguridad	Falta de competencia y confiabilidad del personal asignado para la prestación de servicios	* Procedimiento de acciones correctivas y preventivas ** SGCS - OEA.	3,0	4,0	3,5	Adelantar planes de retrenamiento en los puestos de trabajo para mejorar competencias.	MEDIO

#	SUBPROCESO O PROCEDIMIENTO	ACTIVIDAD O COMPROMISO	RIESGO	Controles Existentes	I	P	R.A.	Controles Sugeridos	RIESGO ESPERADO
E6.8.2	Otros criterios de seguridad	Plano de ubicación de áreas críticas	Pérdida de información datos o sabotaje.	* Procedimiento de Seguridad de la información ** Procedimiento de control de documentos y registros.	3,1	7,7	4,9	Elaborar el plano de áreas críticas incluyendo los sitios de los servidores principal y espejo dentro de ellas.	ALTO
6.8.5	Otros criterios de seguridad	Sistemas adecuados para la comunicación oportuna con supervisores, encargados de seguridad de los clientes y con autoridades	Falta de medios para comunicación del personal de vigilancia o escolta con la empresa.	* Procedimiento de instalación de servicios ** Proc. De prestación del servicio	3,4	4,0	3,7	Suministrar medios alternos de comunicación para casos de fallas en radiotéfonos en puestos de importadores o exportadores.	MEDIO
6.8.7	Otros criterios de seguridad	Plan de emergencia con procedimientos documentos y dispositivos de alerta, acción y evacuación.	Suspensión temporal de actividades en la sede por incidente que obligue a la evacuación.	* Procedimiento de contingencia y emergencia ** Procedimiento Gestión del riesgo	3,0	4,0	3,5	Elaborar y documentar plan de manejo de crisis y continuidad de negocio.	MEDIO
PROCESOS OPERATIVOS									
GESTIÓN COMERCIAL (Nicolas González)									
E1	Requisitos de asociados de negocio	Procedimientos documentados y verificables para la selección de clientes, proveedores y terceras partes	Asociados de negocios con reporte negativo OFAC (Office of Foreign assets Control)	* Política de gestión del riesgo ** Evaluación de asociados de negocio	5,0	3,0	3,9	Realizar verificación consciente de la legalidad de los clientes, proveedores y contratistas.	MEDIO
GESTIÓN DE RIESGOS (José Rivera)									
N4.4.6	Control Operacional	Asegurar con base en la evaluación de riesgos la participación en la cadena de suministro y actividades de comercio exterior	Que los planes y programas de seguridad no estén totalmente integrados en toda la organización y sus actividades	* Evaluación, selección y control de clientes ** Procedimiento Gestión del Riesgo	3,0	4,0	3,5	Mejorar la capacitación y entrenamiento de servicios suministrados a clientes exportadores o importadores.	MEDIO
N4.4.7	Preparación y respuesta a eventos críticos	Procedimiento documentado para identificar y responder ante amenazas y vulnerabilidades	Falta de eficacia en las medidas de protección.	* Procedimiento de contingencia y emergencia ** Procedimiento de gestión del riesgo.	3,0	4,0	3,5	Considerar como eventos críticos aquellos en los cuales nuestro personal cumple tareas sensibles para el cliente.	MEDIO
N4.5.1	Seguimiento y Medición	Tener procedimientos para el seguimiento y medición de las características claves con impacto en el control y seguridad	Los indicadores no se ajustan a las necesidades de la organización o no determinan la eficacia del SGCS DEA	* Procedimiento de instalación de servicios ** Procedimiento de control de sellos y precintos	3,3	2,0	2,6	Mantener actualizados los indicadores de gestión del personal de coordinadores y supervisores.	BAJO

#	SUBPROCESO O PROCEDIMIENTO	ACTIVIDAD O COMPROMISO	RIESGO	Controles Existentes	I	P	R.A.	Controles Sugeridos	RIESGO ESPERADO
E2	Seguridad al contenedor y de la carga	Convenir con asociados de negocio importadores o exportadores, sean o no DEA respecto a la importancia de tener procedimientos de seguridad en el lugar de carga.	Contaminación de Contenedor o del medio de transporte antes del llenado.	* Procedimiento de instalación de servicios ** Procedimiento de control de sellos y precintos	2,5	6,2	4,0	Garantizar al cliente con manejo de contenedores el conocimiento por parte del personal en misión de los estándares norma ISO 17712	MEDIO
E2.1	Sellos del Furgón o contenedor / ULD	Convenir con los asociados de negocios el uso de sellos de alta seguridad que cumplan o excedan los requisitos ISO 17712	Sellos manejados por personal que no tiene las competencias para ello o autorizaciones de salida o ingreso irregulares.	* Instructivo de sellos y precintos ** Procedimiento de gestión del riesgo	3,0	4,0	3,5	Documentar instructivo donde se incluya verificación de sellos y controles de acceso de patios y bodegas de contenedores.	MEDIO
E3	Control de acceso físico	Impedir la entrada no autorizada a las instalaciones	Ingreso de personal no autorizado a áreas restringidas	* Inspección previa de las instalaciones ** Procedimiento de gestión del riesgo	2,9	3,0	2,9	Documentar instructivo donde se incluya verificación de barreras perimétricas y controles de acceso de patios y bodegas de contenedores.	BAJO
E3.1	Empleados	Identificación positiva de empleados	Falta de control de la devolución de carnés de identificación de empleados.	* Inspección previa de las instalaciones ** Procedimiento de gestión del riesgo	3,0	4,0	3,5	Actualizar el procedimiento de desvinculación donde se incluya la devolución del carnet, llaves y claves de accesos.	MEDIO
E3.2	Visitantes, Vendedores y Proveedores	Registro diario de visitantes y proveedores.	Intrusión diurna de banda con fines delictivos.	* Controles de acceso ** Procedimiento de gestión del riesgo	3,3	4,0	3,6	Llevar un registro en papel o en medio magnético de la hora de ingreso y salida del personal ajeno a la organización.	MEDIO
E3.3	Verificación de correos y paquetes de correspondencia	Registro de correos y paquetes recibidos antes de ser distribuidos.	Lesiones personales graves y caño a instalaciones por artefacto explosivo o incendiario.	* Inspección previa de las instalaciones ** Procedimiento de gestión del riesgo	4,0	2,0	2,8	Incluir dentro de las consignas la identificación y reporte de artefactos explosivos o extraños.	BAJO
E3.5	Personal de seguridad	Asegurar que su personal de seguridad está controlando las puertas de entrada y salida de las instalaciones.	Deficiencias del personal en el control de las áreas claves de manejo de la carga	* Proc. De control de accesos ** Procedimiento de gestión del riesgo	3,0	3,0	3,0	Capacitar al personal de porterías en el control de acceso de personal y vehículos.	MEDIO
E5.1	Manejo y procesamiento de información y documentos	Garantizar la coherencia de la información en los registros de control de acceso y la del control de la carga.	Descuidos en la verificación y comparación de los datos contenidos en registros de control led accesos y los documentos de carga	* Control Documental ** Procedimiento de gestión del riesgo	3,2	5,0	4,0	Documentar las inspecciones a los documentos de control en portearas.	ALTO

#	SUBPROCESO O PROCEDIMIENTO	ACTIVIDAD O COMPROMISO	RIESGO	Controles Existentes	I	P	R.A.	Controles Sugeridos	RIESGO ESPERADO
E5.2	Entrega y Recepción de Carga	Verificar con exactitud la carga que entra o sale contra la información del manifiesto	Falta de registro fotográfico o filmico antes durante y después del proceso de cargue o descargue	* Inspección de carga critica ** Procedimiento de gestión del riesgo	3,0	2,0	2,4	Documentar que los puntos de carga internacional deben contar con video vigilancia.	BAJO
E.6	Seguridad Física	Instalaciones donde manejen documentación, información critica o elementos vitales para la prestación del servicio de carga deben resguardarse contra acceso no autorizado	Destrucción de la memoria de la empresa obligando a reconstrucción	* Inspección previa de las instalaciones ** Procedimiento de gestión del riesgo	2,0	3,0	2,4	Verificar dentro del diagnostico inicial de seguridad las medidas de protección de la información que tiene el cliente.	BAJO
EB.1	Seguridad del perímetro	Contar con cerramiento perimetral, cercas, barreras interiores, inspeccionadas con regularidad verificando su integridad.	Sustracción de Bienes de propiedad de la organización	* Inspección de las instalaciones ** Procedimiento de gestión del riesgo	3,0	4,0	3,5	Documentar la verificación de barreras perimétricas y controles de acceso de patios y bodegas de contenedores.	MEDIO
EB.2	Puertas y casetas	Mantenerlas controladas, monitoreadas y supervisadas tanto las d entrada y salida de vehiculos como las de personal.	No mantenerse al mínimo necesario la cantidad de puestas y casetas habilitadas para entradas y salidas	* Inspección previa de las instalaciones ** Procedimiento de gestión del riesgo	3,3	4,0	3,6	Concientizar al personal de coordinadores y supervisores que a mayor numero de accesos se incrementa el riesgo.	MEDIO
EB.3	Estacionamiento de Vehículos	Control en áreas de estacionamiento de vehículos privados.	Destrucción instalaciones criticas del negocio por carro bomba.	* Vista técnica de control servicio ** Procedimiento de gestión del riesgo	4,0	3,0	3,5	Señalizar las áreas de estacionamiento e instalar cámara de video vigilancia	MEDIO
EB.4	Estructura del Edificio	Resistencia a la entrada forzada o ilegal.	Caída parcial de la estructura	* Inspección previa de las instalaciones ** Procedimiento de gestión del riesgo	3,0	3,0	3,0	Documentar las posibilidades de entrada forzada o ilegal en el diagnostico de seguridad.	MEDIO
EB.6	Iluminación	Contar con una buena iluminación dentro y fuera de las instalaciones	Falta de iluminación en los accesos convencionales, barrera perimétrica o parqueaderos.	*Visita técnica de control del servicio ** Procedimiento de gestión del riesgo	2,0	4,0	2,8	Revisión periódica de los sistemas de iluminación incluyendo las luces de emergencia.	BAJO
SEG. ELECTRONICA (Juan Delgado)									
EB.5	Seguridad Física	Control de cerraduras y llaves	Perdida de información confidencial o de equipos de alto costo	* Inspección previa de las instalaciones ** Procedimiento de gestión del riesgo	3,0	4,0	3,5	Las áreas de monitoreo de alarmas y servidores deben estar debidamente protegidas.	MEDIO

#	SUBPROCESO O PROCEDIMIENTO	ACTIVIDAD O COMPROMISO	RIESGO	Controles Existentes	I	P	R.A.	Controles Sugeridos	RIESGO ESPERADO
E6.7	Sistema de alarmas y videocámaras de vigilancia	Supervisar y monitorear las instalaciones para prevenir acceso no autorizado a las áreas críticas.	Intrusión a áreas críticas no detectada con fines delictivos.	* Inspección del CCTV ** Procedimiento de gestión del riesgo	4,0	3,0	3,5	Diariamente se debe verificar el CCTV y solucionar cualquier irregularidad.	MEDIO
E7.2	Responsabilidad y control de la información	Controlar la documentación e información en los medios magnéticos contra acceso no autorizado	Pérdida de documentos o información en los equipos de computo.	* Política de seguridad ** Procedimiento de gestión del riesgo	4,0	5,0	4,5	Elaborar y difundir documento sobre las normas de seguridad a seguir por parte de los usuarios de equipos de computo.	ALTO
PROCESOS DE SOPORTE									
ADMINISTRACIÓN DEL PERSONAL (Yaneth Turriago)									
N4.4.2	Entrenamiento, Capacitación y toma de Conciencia	Determinar y demostrar las competencias requeridas del personal y tomar las acciones necesarias.	Falta de conciencia de la responsabilidad y la influencia de su acción u omisión sobre la eficacia del SGCS DEA	* Procedimiento de selección de personal ** Procedimiento de instalación de servicios.	3,3	3,0	3,1	Revisar el método de inducción y entrenamiento en el puesto de trabajo.	MEDIO
E4	Seguridad del personal propio, subcontratado y temporal	Procedimiento documentado para evaluar los candidatos con posibilidad de ser contratados.	Causar perjuicio a un cliente por comportamiento criminal de un trabajador en misión	* Procedimiento de selección de personal ** Procedimiento de instalación de servicios.	2,0	4,0	2,8	Revisar periódicamente el método de validación de guardas para clientes críticos o potencialmente críticos.	BAJO
E4.1	Verificación preliminar al empleo	Procedimientos para verificar información de la solicitud de empleo e investigar antecedentes del candidato.	Pérdida del cliente por no cumplir los requisitos exigidos del personal asignado	* Procedimiento de selección de personal ** Procedimiento Evaluación, selección y control de clientes.	3,0	4,0	3,5	Revisar los archivos de la fiscalía general de la república al personal que presta servicios críticos.	MEDIO
E4.2	Verificación y mantenimiento del personal después de la contratación	Lista actualizada de empleados propios y subcontratados con datos personales de relevancia.	Suplantación de empleados o trabajadores con fines delictivos.	* Procedimiento de instalación de servicios ** Procedimiento selección de personal	4,0	2,0	2,8	Actualizar visita domiciliaria y fotos anualmente al personal que realiza labores críticas en el SGCS.	BAJO
E4.3	Procedimiento de terminación de la vinculación laboral.	Retiro de la identificación, eliminación de permisos y claves de acceso a instalaciones y sistemas.	Pérdida o adulteración de información o sustracción de documentación clasificada.	* Procedimiento de control de accesos ** Procedimiento control de cerraduras y llaves.	3,0	4,0	3,5	Revisar el método de suspensión de claves, permisos y cambiar guardas cuando haya retiro de cargos críticos.	MEDIO
E8	Entrenamiento de seguridad y concientización sobre amenazas	Contar con un programa anual de capacitación sobre como reconocer y reportar amenazas y vulnerabilidades.	Desconocer el procedimiento para considerar una situación y como reportarla.	* Evaluación de Capacitación ** Programa de capacitación	3,1	4,0	3,5	Incluir para el personal en cargos críticos de la cadena de suministro entrenamiento en seguridad y concientización sobre amenazas.	MEDIO

#	SUBPROCESO O PROCEDIMIENTO	ACTIVIDAD O COMPROMISO	RIESGO	Controles Existentes	I	P	R.A.	Controles Sugeridos	RIESGO ESPERADO
ADMINISTRACIÓN FINANCIERA Y CONTABLE (Habib Simman)									
N4.3.5	Previsiones	Presupuesto para cubrir los objetivos, planes y controles operacionales.	Limitaciones en medios o recursos para el control de la integridad de las mercancías de acuerdo a lo contratado.	* Procedimiento de control del servicio ** Presupuesto anual	3,0	3,0	3,0	Siempre que se haga una propuesta económica a un potencial cliente debe estar avalada por la Dirección Financiera	MEDIO
EI.2	Prevención del lavado de activos y financiación del terrorismo.	Aplicar proceso de selección y evaluación de asociados de negocio, antecedentes legales, penales financieros y reporte de operaciones sospechosas.	Prestación de servicios a clientes relacionados con Bandas Criminales u otras organizaciones al margen de la ley	* Procedimiento de ventas ** Procedimiento Evaluación, selección y control de clientes.	3,2	4,0	3,6	Revisar el método de evaluación de clientes potenciales a fin de evitar apoyo a lavado de activos o terrorismo.	MEDIO
TODOS LOS PROCESOS									
N4.3.3	Gestión del Riesgo	Tener un procedimiento documentado de Gestión del Riesgo a nivel de toda la organización.	Fallas en el sistema de control y seguridad por no tener en cuenta nuevas amenazas o vulnerabilidades.	* Sistemas integrados de gestión manual de SGCS - DEA. ** Procedimiento de gestión del riesgo	4,0	5,0	4,5	Difundir este documento por parte de cada dueño de proceso a todo su personal.	ALTO
N4.4.3	Comunicación	Condiciones para mantener la comunicación abierta y efectiva de información sobre el control y seguridad en el comercio internacional.	Limitaciones para comunicar acto sospechoso de contaminación de carga, contrabando o tráfico de armas.	* Sistemas integrados de gestión manual de SGCS - DEA. ** Procedimiento de gestión del riesgo	4,0	5,0	4,5	Revisar periódicamente las acciones preventivas y correctivas recomendadas en el análisis de riesgos.	ALTO
N4.5.3	Control de Registros	Llevar los registros necesarios para demostrar conformidad con los requisitos del SGCS DEA	Listado maestro de registros no contempla identificación, mantenimiento, disposición para entrega control y archivo de la información.	* Sistemas integrados de gestión manual de SGCS - DEA. ** Procedimiento de gestión del riesgo	2,0	4,0	2,8	Revisar cuidadosamente que cada uno de los procesos lleve sus registro del SGCS actualizados.	BAJO
N4.6.2	Acción correctiva y preventiva	Tener procedimientos documentados para la implementación de las acciones correctivas y preventivas	No aplicar acción correctiva y preventiva ante una no conformidad real o potencial detectada en el SGCS.	* Procedimiento de control documental ** Sistemas integrados de gestión manual de SGCS - DEA.	3,0	5,0	3,9	Demostrar la aplicación de las acciones preventivas y correctivas para mejorar la seguridad en cada uno de los procesos.	MEDIO

#	SUBPROCESO O PROCEDIMIENTO	ACTIVIDAD O COMPROMISO	RIESGO	Controles Existentes	I	P	R.A.	Controles Sugeridos	RIESGO ESPERADO
E3.4	Identificación y retiro de personas no autorizadas	Procedimiento documentado para identificar, dirigirse y retirar a personas no autorizadas.	Demandas de tipo penal por mal trato o lesiones a personas sorprendidas dentro de las instalaciones.	* Procedimiento de control de accesos ** Sistemas integrados de gestión manual de SGCS - DEA.	4,0	5,0	4,5	Todas las áreas deben estar en capacidad para detectar la presencia de personal no autorizado y abordarlos correctamente.	ALTO
E6.5	Control de Cerraduras y llaves	Mecanismos de cierre de puertas y ventanas, cerraduras llaves y claves de acceso	Ingreso a área crítica en horario no laboral por acceso no convencional	* Procedimiento de Gestión del Riesgo. ** Sistemas integrados de gestión manual de SGCS - DEA. .	2,8	4,0	3,3	Cada área es responde al termino de la jornada ventanas y puertas queden aseguradas, equipos apagados en prevención de incendios	MEDIO
E7.1	Protección con contraseña	Políticas, procedimientos y normas de tecnología de la información	Sustracción de información por desconocido desde un equipo de la organización	* Proc. seguridad informática ** Sistemas integrados de gestión manual de SGCS - DEA. .	3,0	4,0	3,5	Cada equipo debe estar asignado a una sola persona con contraseñas robustas que garanticen su uso exclusivo y seguro.	MEDIO
E7.3	Protección a los sistemas y datos	Actualización de Software anti virus y anti-espía	Infracción al sistema de seguridad de tecnologías de la información	* Proc. Seguridad informática ** Gestión del riesgos.	4,0	5,0	4,5	La Dirección de informática y tecnología es la responsable por la actualización de aplicaciones anti malware, virus y espía.	ALTO

RESULTADOS ESTIMADOS Y CONSIDERADOS EN EL MOMENTO DE SU MEDICIÓN

SISTEMA DE ADMINISTRACIÓN DE RIESGOS
VI - SEGUIMIENTO Y REVISIÓN DE MEJORA
COLVISEG DEL CARIBE

Revisión trimestral META: 85%

FECHA SEGUIMIENTO:

lunes, 09 de noviembre de 2015

Norma BASC V4 - 4.6.2 NTC-ISO 31000 - 5.5


RQ	RIESGO	CORRIGI		COMUNICACIÓN Y PERTINENCIA	ACCIÓN CORRECTIVA, PREVENTIVA O DE MEJORA	ENFOQUE	ESTADO
		SI	NO				
PROCESOS GERENCIALES							
GESTIÓN GERENCIAL (Heinz Pichler)							
N4.1	Algún cliente OEA al verificar sus procesos puede detectar incumplimientos de parte nuestra		X	Gestión Gerencial	Llevar el conocimiento y aplicación de acuerdos contractuales de clientes críticos a las partes interesadas.	Alta Dirección	PENDIENTE
N4.2	Falta de prevención de actividades ilícitas por falta de una política de seguridad claramente difundida y entendida		X	Gestión Gerencial	Establecer un medio de difusión de la política de seguridad a todos los niveles de la organización.	Alta Dirección	PENDIENTE
N4.3.4	Multas elevadas y/o cancelación temporal o definitiva de las licencias y permisos de funcionamiento.		X	Gestión Gerencial	Diseñar programa de alerta previa para tramitación de permisos y licencias en equipo de la asistente de Gerencia.	Alta Dirección	PENDIENTE
N4.4.1	No establecer y/o documentar funciones, responsabilidades y autoridad del personal que afecta la seguridad.		X	Gestión Gerencial	Establecer que cada contrato sea conocido por las partes interesadas de la organización para lo de su competencia.	Alta Dirección	PENDIENTE
N4.6.1	Incumplimiento de la política y objetivos del control y seguridad		X	Gestión Gerencial	Continuar con la verificación de recomendaciones o acciones de mejora de seguridad en actividades críticas de la cadena de suministros	Continuidad del negocio	PENDIENTE
N4.6.3	Perder la certificación del SGCS por el OEA		X	Gestión Gerencial	Incrementar las revisiones del SGCS con el fin de mantener las certificaciones pertinentes.	Alta Dirección	PENDIENTE
E6.8.1	Fallas en la protección de las instalaciones por no contar con responsable de la seguridad.		X	OEA	Verificar en archivos de organismos nacionales e internacionales.	Seguridad Física	PENDIENTE
SISTEMAS INTEGRADOS DE GESTIÓN (Ever Polo)							
N4.3.1	Incumplimiento de requisitos en materia de control y seguridad		X	Gestión de auditoria del SIG	Revisar el cubrimiento con cámaras de vigilancia de todo el perímetro	Administración y logística	PENDIENTE
N4.3.2	Incumplimiento de la política de control y seguridad a través de indicadores de gestión.		X	OEA	Establecimiento claro por escrito de las funciones y responsabilidades de los actores en cadenas de suministros.	Capacitación y Entrenamiento	PENDIENTE

RQ	RIESGO	CORRIGI		COMUNICACIÓN Y PERTINENCIA	ACCIÓN CORRECTIVA, PREVENTIVA O DE MEJORA	ENFOQUE	ESTADO
		SI	NO				
N4.4.4	Algunos procedimientos y registros requeridos por OEA que son responsabilidad del cliente pueden ser indilgados a Colviseg del Caribe.		X	OEA	Revisión mensual de barreras de protección y posibles accesos no convencionales	Operaciones de carga	PENDIENTE
N4.4.5	No disponer de un sistema para la protección y recuperación de documentos sensibles tanto físicos como magnéticos		X	Gestión de auditoria del SIG	Establecer cronograma de actualización de listados maestros de registros y documentos.	Protección de documentos	PENDIENTE
N4.4.7	Incrementar la criticidad del evento ante la imprevisión.		X	Gestión de auditoria del SIG	Verificación periódica de idoneidad y entrenamiento de Brigadas y equipos de emergencia.	Seguridad y salud en el trabajo SST	PENDIENTE
N4.5.2	No se elaboro o ejecuto el programa de auditorias internas		X	Gestión de auditoria del SIG	Hacer un plan de auditorias internas y externas en el mes de diciembre para dar cumplimiento todo el año y contar con auditores certificados	Control de Calidad	PENDIENTE
E1.1	Prestación de servicios a empresas que tienen graves deficiencias de seguridad para protección de sus mercancías.		X	OEA	Actualizar el sistema de evaluación de asociados de negocios.	Operaciones de carga	PENDIENTE
E5	Falta de competencia y confiabilidad del personal asignado para la prestación de servicios		X	Gestión de auditoria del SIG	Adelantar planes de rentrenamiento en los puestos de trabajo para mejorar competencias.	Cadena de suministros	PENDIENTE
E6.8.2	Pérdida de información datos o sabotaje.		X	Gestión de auditoria del SIG	Elaborar el plano de áreas criticas incluyendo los sitios de los servidores principal y espejo dentro de ellas.	Seguridad Física	PENDIENTE
6.8.5	Falta de medios para comunicación del personal de vigilancia o escolta con la empresa.		X	OEA	Suministrar medios alternos de comunicación para casos de fallas en radiotéfonos en puestos de importadores o exportadores.	Medios tecnológicos	PENDIENTE
6.8.7	Suspensión temporal de actividades en la sede por incidente que obligue a la evacuación.		X	Gestión de auditoria del SIG	Elaborar y documentar plan de manejo de crisis y continuidad de negocio.	Mantenimiento	PENDIENTE
PROCESOS OPERATIVOS							
GESTIÓN COMERCIAL (Nicolas González)							
E1	Asociados de negocios con reporte negativo OFAC (Office of Foreign assets Control)		X	Gestión Gerencial	Realizar verificación consciente de la legalidad de los clientes, proveedores y contratistas.	Comercialización y mercadeo	PENDIENTE
GESTIÓN DE RIESGOS (José Rivera)							
N4.4.6	Que los planes y programas de seguridad no estén totalmente integrados en toda la organización y sus actividades		X	Servicio de Vigilancia	Mejorar la capacitación y entrenamiento de servicios suministrados a clientes exportadores o importadores.	Cadena de suministros	PENDIENTE

RQ	RIESGO	CORRIGI		COMUNICACIÓN Y PERTINENCIA	ACCIÓN CORRECTIVA, PREVENTIVA O DE MEJORA	ENFOQUE	ESTADO
		SI	NO				
N4.4.7	Falto eficacia en las medidas de protección.		X	Gestión de Riesgos	Considerar como eventos críticos aquellos en los cuales nuestro personal cumple tareas sensibles para el cliente.	Seguridad Industrial	PENDIENTE
N4.5.1	Los indicadores no se ajustan a las necesidades de la organización o no determinan la eficacia del SGCS OEA		X	Gestión de Riesgos	Mantener actualizados los indicadores de gestión del personal de coordinadores y supervisores.	Monitoreo del SGCS	PENDIENTE
E2	Contaminación de Contenedor o del medio de transporte antes del llenado.		X	Gestión de Riesgos	Garantizar al cliente con manejo de contenedores el conocimiento por parte del personal en misión de los estándares norma ISO 17712	Transporte unimodal	PENDIENTE
E2.1	Sellos manejados por personal que no tiene las competencias para ello o autorizaciones de salida o ingreso irregulares.		X	Servicio de Vigilancia	Documentar instructivo donde se incluya verificación de sellos y controles de acceso de patios y bodegas de contenedores.	Protección de contenedores	PENDIENTE
E3	Ingreso de personal no autorizado a áreas restringidas		X	Servicio de Vigilancia	Documentar instructivo donde se incluya verificación de barreras perimétricas y controles de acceso de patios y bodegas de contenedores.	Controles de Acceso	PENDIENTE
E3.1	Falta de control de la devolución de carnés de identificación de empleados.		X	Servicio de Vigilancia	Actualizar el procedimiento de desvinculación donde se incluya la devolución del carnet, llaves y claves de accesos.	Controles de Acceso	PENDIENTE
E3.2	Intrusión diurna de banda con fines delictivos.		X	Gestión de Riesgos	Llevar un registro en papel o en medio magnético de la hora de ingreso y salida del personal ajeno a la organización.	Controles de Acceso	PENDIENTE
E3.3	Lesiones personales graves y caño a instalaciones por artefacto explosivo o incendiario.		X	Gestión de Riesgos	Incluir dentro de las consignas la identificación y reporte de artefactos explosivos o extraños.	Control de correspondencia	PENDIENTE
E3.5	Deficiencias del personal en el control de las áreas claves de manejo de la carga		X	Servicio de Vigilancia	Capacitar al personal de porterías en el control de acceso de personal y vehículos.	Seguridad Física	PENDIENTE
E5.1	Descuidos en la verificación y comparación de los datos contenidos en registros de control led accesos y los documentos de carga		X	Gestión de Riesgos	Documentar las inspecciones a los documentos de control en portearas.	Protección de documentos	PENDIENTE
E5.2	Falta de registro fotográfico o filmico antes durante y después del proceso de cargue o descargue		X	Gestión de Riesgos	Documentar que los puntos de carga internacional deben contar con video vigilancia.	Administración y logística	PENDIENTE
E.6	Destrucción de la memoria de la empresa obligando a reconstrucción		X	Seguridad de Instalaciones	Verificar dentro del diagnostico inicial de seguridad las medidas de protección de la información que tiene el cliente.	Protección de documentos	PENDIENTE
E6.1	Sustracción de Bienes de propiedad de la organización		X	Seguridad de Instalaciones	Documentar la verificación de barreras perimétricas y controles de acceso de patios y bodegas de contenedores.	Seguridad Física	PENDIENTE
E6.2	No mantenerse al mínimo necesario la cantidad de puestas y casetas habilitadas para entradas y salidas		X	Seguridad de Instalaciones	Concientizar al personal de coordinadores y supervisores que a mayor numero de accesos se incrementa el riesgo.	Seguridad Física	PENDIENTE

RQ	RIESGO	CORRIGI		COMUNICACIÓN Y PERTINENCIA	ACCIÓN CORRECTIVA, PREVENTIVA O DE MEJORA	ENFOQUE	ESTADO
		SI	NO				
E6.3	Dstrucción instalaciones criticas del negocio por carro bomba.		X	Seguridad de Instalaciones	Señalizar las áreas de estacionamiento e instalar cámara de video vigilancia	Continuidad del negocio	PENDIENTE
E6.4	Caída parcial de la estructura		X	Seguridad de Instalaciones	Documentar las posibilidades de entrada forzada o ilegal en el diagnostico de seguridad.	Mantenimiento	PENDIENTE
E6.6	Falta de iluminación en los accesos convencionales, barrera perimétrica o parqueaderos.		X	Seguridad de Instalaciones	Revisión periódica de los sistemas de iluminación incluyendo las luces de emergencia.	Administración y logística	PENDIENTE
SEG. ELECTRONICA (Juan Delgado)							
E6.5	Perdida de información confidencial o de equipos de alto costo		X	Medios Tecnológicos	Las áreas de monitoreo de alarmas y servidores deben estar debidamente protegidas.	Controles de Acceso	PENDIENTE
E6.7	Intrusión a áreas criticas no detectada con fines delictivos,		X	Medios Tecnológicos	Diariamente se debe verificar el CCTV y solucionar cualquier irregularidad.	Medios tecnológicos	PENDIENTE
E7.2	Perdida de documentos o información en los equipos de computo.		X	Seguridad de las tecnologías de la información y comunicaciones	Elaborar y difundir documento sobre las normas de seguridad a seguir por parte de los usuarios de equipos de computo.	Informática y sistematización de datos	PENDIENTE
PROCESOS DE SOPORTE							
ADMINISTRACIÓN DEL PERSONAL (Yaneth Turriago)							
N4.4.2	Falta de conciencia de la responsabilidad y la influencia de su acción u omisión sobre la eficacia del SGCS OEA		X	Gestión de Talento Humano	Revisar el método de inducción y entrenamiento en el puesto de trabajo.	Capacitación y Entrenamiento	PENDIENTE
E4	Causar perjuicio a un cliente por comportamiento criminal de un trabajador en misión		X	Gestión del Talento Humano	Revisar periódicamente el método de validación de guardas para clientes críticos o potencialmente críticos.	Selección de personal	PENDIENTE
E4.1	Pérdida del cliente por no cumplir los requisitos exigidos del personal asignado		X	Gestión del Talento Humano	Revisar los archivos de la fiscalía general de la republica al personal que presta servicios críticos.	Selección de personal	PENDIENTE
E4.2	Suplantación de empleados o trabajadores con fines delictivos.		X	Gestión del Talento Humano	Actualizar visita domiciliaria y fotos anualmente al personal que realiza labores criticas en el SGCS.	Seguridad Física	PENDIENTE

RQ	RIESGO	CORRIGI		COMUNICACIÓN Y PERTINENCIA	ACCIÓN CORRECTIVA, PREVENTIVA O DE MEJORA	ENFOQUE	ESTADO
		SI	NO				
E4.3	Perdida o adulteración de información o sustracción de documentación clasificada.		X	Gestión de Bienestar y RSE	Revisar el método de suspensión de claves, permisos y cambiar guardas cuando haya retiro de cargos críticos.	Controles de Acceso	PENDIENTE
E8	Desconocer el procedimiento para considerar una situación y como reportarla.		X	Capacitación y entrenamiento	Incluir para el personal en cargos críticos de la cadena de suministro entrenamiento en seguridad y concientización sobre amenazas.	Cadena de suministros	PENDIENTE
ADMINISTRACIÓN FINANCIERA Y CONTABLE (Habib Simman)							
N4.3.5	Limitaciones en medios o recursos para el control de la integridad de las mercancías de acuerdo a lo contratado.		X	Gestión de Tesorería	Siempre que se haga una propuesta económica a un potencial cliente debe estar avalada por la Dirección Financiera	Administración y logística	PENDIENTE
E1.2	Prestación de servicios a clientes relacionados con Bandas Criminales u otras organizaciones al margen de la ley		X	Gestión de Compras y Almacén	Revisar el método de evaluación de clientes potenciales a fin de evitar apoyo a lavado de activos o terrorismo.	Actividades de comercio exterior	PENDIENTE
TODOS LOS PROCESOS							
N4.3.3	Fallas en el sistema de control y seguridad por no tener en cuenta nuevas amenazas o vulnerabilidades.		X	Requisitos del Sistema de Gestión en Control y Seguridad	Difundir este documento por parte de cada dueño de proceso a todo su personal.	Seguridad Física	PENDIENTE
N4.4.3	Limitaciones para comunicar acto sospechoso de contaminación de carga, contrabando o trafico de armas.		X	Requisitos del Sistema de Gestión en Control y Seguridad	Revisar periódicamente las acciones preventivas y correctivas recomendadas en el análisis de riesgos.	Operaciones	PENDIENTE
N4.5.3	Listado maestro de registros no contempla identificación, mantenimiento, disposición para entrega control y archivo de la información.		X	Requisitos del Sistema de Gestión en Control y Seguridad	Revisar cuidadosamente que cada uno de los procesos lleve sus registro del SGCS actualizados.	Protección de documentos	PENDIENTE
N4.6.2	No aplicar acción correctiva y preventiva ante una no conformidad real o potencial detectada en el SGCS.		X	Requisitos del Sistema de Gestión en Control y Seguridad	Demostrar la aplicación de las acciones preventivas y correctivas para mejorar la seguridad en cada uno de los procesos.	Monitoreo del SGCS	PENDIENTE
E3.4	Demandas de tipo penal por mal trato o lesiones a personas sorprendidas dentro de las instalaciones.		X	Control de Acceso físico	Todas las áreas deben estar en capacidad para detectar la presencia de personal no autorizado y abordarlos correctamente.	Controles de Acceso	PENDIENTE
E6.5	Ingreso a área critica en horario no laboral por acceso no convencional		X	Seguridad Física	Cada área es responde al termino de la jornada ventanas y puertas queden aseguradas, equipos apagados en prevención de incendios	Controles de Acceso	PENDIENTE

RQ	RIESGO	CORRIGI		COMUNICACIÓN Y PERTINENCIA	ACCIÓN CORRECTIVA, PREVENTIVA O DE MEJORA	ENFOQUE	ESTADO
		SI	NO				
E7.1	Sustracción de información por desconocido desde un equipo de la organización		X	Seguridad en las tecnologías de la información	Cada equipo debe estar asignado a una sola persona con contraseñas robustas que garanticen su uso exclusivo y seguro.	Medios tecnológicos	PENDIENTE
E7.3	Infracción al sistema de seguridad de tecnologías de la información		X	Seguridad en las tecnologías de la información	La Dirección de informática y tecnología es la responsable por la actualización de aplicaciones anti malware, virus y espía.	Informática y sistematización de datos	PENDIENTE
TOTALES :		0		56	PENDIENTES	56	
CUMPLIMIENTO A LA FECHA:		0%				100%	
 ANALISTA		REPRESENTANTE DEL CLIENTE					

RESULTADOS ESTIMADOS Y CONSIDERADOS EN EL MOMENTO DE SU MEDICIÓN