BUSINESS ALLIANCE FOR SECURE COMMERCE

ESTÁNDAR INTERNACIONAL DE SEGURIDAD BASC

6.0.1

EMPRESAS CON RELACIÓN DIRECTA CON LA CARGA, LAS UNIDADES DE CARGA Y LAS UNIDADES DE TRANSPORTE DE CARGA

Versión 6 – 2022
Fecha de aprobación: 2 de marzo de 2022

TABLA DE CONTENIDO

0. INTRODUCCIÓN

El Estándar Internacional de Seguridad BASC contiene las medidas de control operacional para los principales elementos que se relacionan con la seguridad de la cadena de suministro y complementarios con la Norma Internacional BASC. Tiene como objetivo contribuir con las empresas para que sus actividades se desarrollen a través de una cultura integral de seguridad y generación de confianza, con el fin de proteger las partes interesadas, instalaciones y carga, entre otros.

Se emitieron tres documentos con la intención de consolidar los requisitos correspondientes a la interacción con la carga definida en el alcance del SGCS. El Estándar Internacional de Seguridad BASC 6.0.1 aplica a las empresas que tienen relación directa con la carga, con las unidades de carga o las unidades de transporte de carga.

El Estándar Internacional de Seguridad BASC 6.0.2 aplica a las empresas que tienen una relación indirecta con la carga, con las unidades de carga o las unidades de transporte de carga.

El Estándar Internacional de Seguridad BASC 6.0.3 es aplicable a todo tipo de empresas que deseen gestionar los riesgos y controles operacionales mínimos que les permitan una operación segura de productos y prestación de servicios, que no apliquen al Estándar Internacional 6.0.1 y 6.0.2.

Este documento es el resultado de la gestión de:

Junta Directiva WBO 2021-23: Emilio Aguiar (BASC Ecuador), Presidente; Ricardo Sanabria (BASC Colombia), Vicepresidente; Patricia Siles (BASC Perú), Secretaria; Armando Rivas (BASC República Dominicana), Tesorero; Álvaro Alpízar (BASC Costa Rica), Vocal.

Comité Técnico WBO 2021-23: Fermín Cuza, Presidente Internacional WBO; Directores Ejecutivos: Giomar González, BASC Panamá; Luis Bernardo Benjumea, BASC Colombia; Omar Castellanos, BASC República Dominicana; Fabricio Muñoz, BASC Guayaquil; César Venegas, BASC Perú; Jorge Wellmann, BASC Guatemala; María Andrea Caldas, Coordinadora de Certificaciones WBO y Luis Renella, Director de Operaciones WBO.

1 REQUISITOS DE ASOCIADOS DE NEGOCIO

1.1 Gestión de asociados de negocio

1.1.1 La empresa debe establecer un procedimiento documentado para la selección, evaluación, contratación y sensibilización de asociados de negocio respecto al SGCS BASC, con base en la gestión del riesgo, la debida diligencia y la legislación vigente. Debe incluir:

a) El nivel de criticidad con base en la gestión del riesgo.
b) Evidencia del cumplimiento de los requisitos legales de sus asociados de negocio.
c) Evidencia de la certificación BASC (autenticidad del certificado). En caso de no contar con esta, mantener evidencia de otras certificaciones o iniciativas de seguridad vigentes y reconocidas internacionalmente por una autoridad aduanera (CTPAT, Operador Económico Autorizado) y otros entes, que constituyan evidencia de cumplimiento de criterios de seguridad aceptables. En caso de no contar con estas certificaciones o iniciativas de seguridad, la empresa debe suscribir acuerdos de seguridad.
d) Cumplimiento de los acuerdos de seguridad mediante una verificación, mínimo una vez al año.
e) Lista actualizada de los asociados de negocio.
f) Lineamientos de capacitación que incluyan prácticas de prevención de delitos en el comercio internacional y de corrupción y soborno.
g) Evidencia de datos de los beneficiarios finales, de acuerdo con la legislación vigente.

1.2 Prevención del lavado de activos y financiamiento del terrorismo

1.2.1 La empresa debe establecer un procedimiento, de acuerdo con la legislación vigente, para prevenir el lavado de activos, financiamiento del terrorismo y otros delitos relacionados con el comercio internacional. La empresa debe nombrar un responsable del cumplimiento de estos procedimientos. Este procedimiento debe incluir:

a) Conocimiento de sus asociados de negocio, que incluya: identidad y legalidad de la empresa, socios y representantes.
b) Antecedentes legales, penales y financieros teniendo en cuenta las listas nacionales e internacionales.
c) Reporte oportuno a las autoridades competentes cuando se identifiquen operaciones sospechosas (ver 3.7).
d) Verificación de pertenencia a gremios o asociaciones reconocidos.

1.2.2 El procedimiento documentado para la selección de los asociados de negocio (ver 1.1) debe, con base en la gestión del riesgo, contemplar como mínimo los siguientes factores (señales de alerta) para la identificación de operaciones sospechosas:

a) Origen y destino de la operación de comercio.
b) Frecuencia de las operaciones.
c) Valor y tipo de mercancías.
d) Modalidad de la operación de transporte.
e) Forma de pago de la transacción.
f) Inconsistencias en la información proporcionada por los asociados de negocio.
g) Requerimientos que salen de lo establecido.

2. SEGURIDAD DE LAS UNIDADES DE CARGA Y UNIDADES DE TRANSPORTE DE CARGA

2.1 Generalidades

Debe establecer procedimientos documentados con base en la gestión del riesgo y su rol en la cadena de suministro, para establecer los controles operacionales que permitan proteger las unidades de carga y unidades de transporte de carga contra la introducción de personas y materiales no autorizados. La empresa debe:

a) Identificar áreas para la realización de las inspecciones.
b) Definir criterios para inspeccionar las unidades y rechazarlas cuando corresponda.
c) Inspeccionar las unidades al entrar y salir de las instalaciones y antes de realizar el proceso de cargue.
d) Establecer los controles necesarios para mantener la integridad de las unidades.
e) Mantener registros de las inspecciones realizadas y del personal involucrado.
f) Notificar a las partes interesadas pertinentes y autoridades competentes en caso de incidentes (ver 3.7).

2.2 Inspecciones a las unidades de carga

La inspección debe incluir como mínimo, tanto en el interior como en el exterior, los siguientes puntos:

- Pared frontal.
- Lado izquierdo.
- Lado derecho.
- Piso.
- Techo.
- Puertas (mecanismo de cierre).
- Exterior y bastidor (vigas desde la pared frontal hasta las puertas).
- Sistema de refrigeración (si aplica) y sus compartimentos accesibles.

Para tráiler, inspeccionar adicionalmente:

- Pata mecánica.
- Llantas, parachoques y luces.
- Placa del patín (estructura de fijación del pin que ingresa en la quinta rueda).

Para otras unidades de carga (por ejemplo, unidades de carga aérea), se debe efectuar una inspección que considere otros puntos y elementos de riesgo identificados.

2.3 Inspecciones a las unidades de transporte de carga

Esta inspección debe incluir como mínimo los siguientes puntos:

Para plataformas, chasís y similares:
- Pata mecánica.
- Llantas, parachoques y luces.
- Placa del patín (estructura de fijación del pin que ingresa en la quinta rueda).
- Verificar puntos de anclaje (4 pines) o seguro del tráiler al contenedor (twist lock).
- Inspección del generador para carga refrigerada (si aplica).

Para camiones (tractores / cabezales):
- Parachoques, luces, llantas y aros.
- Puertas y compartimientos de herramientas y mecanismos de bloqueo.
- Caja de batería.
- Filtro de aire.
- Tanques de combustible y agua.
- Compartimiento del interior y piso de la cabina y litera.
- Sección de pasajeros y techo de la cabina.

Para furgones:
- Pared frontal.
- Lado izquierdo.
- Lado derecho.
- Piso.
- Techo.
- Puertas (mecanismo de cierre).
- Sistema de refrigeración (si aplica).
- Exterior y bastidor (vigas desde la pared frontal hasta las puertas).

Para otras unidades de transporte de carga, se debe efectuar una inspección que considere los puntos anteriores y cualquier otro elemento de riesgo identificado.

2.4 Prevención de contaminación cruzada y seguridad agrícola

Se deben limpiar las unidades de carga antes del proceso de cargue y garantizar que estas son inspeccionadas para evitar la contaminación visible por plagas, restos de desechos, residuos y otros materiales, incluyendo elementos naturales como insectos y roedores.

a) Si se encuentra contaminación durante la inspección, se debe proceder de acuerdo con la normatividad vigente.
b) Se debe conservar información documentada de este proceso y la eficacia de su aplicación.

2.5 Trazabilidad de las unidades de carga y unidades de transporte de carga

La empresa debe establecer un procedimiento documentado para evidenciar la trazabilidad de la unidad de carga o unidad de transporte de carga durante la custodia y mantener los registros correspondientes.

2.6 Sellos de seguridad

La empresa debe:

a) Establecer un procedimiento documentado para registrar, controlar y manipular los sellos de seguridad para las unidades de carga y transporte de carga en sus operaciones. Este procedimiento debe estar basado en la gestión del riesgo e incluir, como mínimo, los controles necesarios para mantener la integridad y trazabilidad del sello en toda la cadena de custodia.
b) Autorizar la gestión de los sellos únicamente a colaboradores designados y capacitados.
c) Almacenar los sellos en lugares seguros, resguardados y con control de acceso limitado.
d) Instalar un sello de alta seguridad que cumpla como mínimo con los requisitos de la norma ISO17712 a todas las unidades de carga con destino internacional cuando sea necesario durante sus operaciones o ruta.
e) Utilizar para los destinos locales sellos como mínimo de tipo indicativo.
f) Contar con registros fotográficos o fílmicos que evidencien la manipulación de los sellos antes, durante y después de sus operaciones.
g) Verificar el inventario de sellos de acuerdo con las operaciones de la empresa.
h) Documentar y reportar a las autoridades pertinentes y partes interesadas cuando estos hayan sido comprometidos, reemplazados o ante cualquier incidente que comprometa su integridad, siguiendo los lineamientos establecidos para la comunicación de actividades sospechosas o eventos críticos (ver 3.7).

2.7 Control de ruta

La empresa debe, con base en la gestión del riesgo:

a) Establecer los controles necesarios durante la ruta para mantener la integridad de las unidades de carga y las unidades de transporte de carga, propios o subcontratados, manteniendo registros.
b) Establecer y verificar rutas predeterminadas que incluyan el tiempo de tránsito estimado, zonas críticas, cruces fronterizos, lugares de parada y descanso autorizados.
c) Contar con un sistema de geolocalización o GPS, que permita la trazabilidad y monitoreo durante la ruta.
d) Documentar y reportar a las autoridades pertinentes y partes interesadas ante cualquier incidente o actividad sospechosa detectada, siguiendo los lineamientos establecidos para la comunicación de actividades sospechosas o eventos críticos (ver 3.7).
e) Identificar unidades de transporte y conductores autorizados por la empresa antes de que reciban o entreguen la carga.

3. SEGURIDAD EN LOS PROCESOS DE MANEJO DE LA CARGA Y OTROS PROCESOS DEFINIDOS EN EL ALCANCE DEL SGCS

3.1 Parámetros y criterios

La empresa debe establecer procedimientos documentados que contemplen los parámetros y criterios de seguridad aplicados en los procesos de manejo de la carga y otros procesos identificados, de acuerdo con el alcance establecido en el SGCS BASC, la gestión del riesgo y su rol en la cadena de suministro.

3.2 Control de materia prima, material de empaque y embalaje

Debe establecer un procedimiento documentado para gestionar el manejo, custodia, almacenamiento, control, disposición y revisión de:

a) Materia prima.
b) Material de empaque y embalaje, incluyendo pallets (tarimas o similares).
c) Residuos, desechos y sobrantes que afecten la seguridad de las operaciones de la empresa.

3.3 Precursores químicos y sustancias controladas

Debe establecer un procedimiento documentado para el manejo y control de precursores químicos y sustancias controladas, de conformidad con los requisitos legales y la gestión del riesgo. Debe incluir:

a) Control, manejo y almacenamiento durante la custodia.
b) Registros de su uso e inventario.
c) Responsables de su manipulación.
d) Vigencia de las autorizaciones legales aplicables.

3.4 Controles en el manejo de la carga

Debe establecer un procedimiento documentado para:

a) Mantener registros que identifiquen el personal involucrado en el proceso de manejo de la carga.
b) Separar y proteger el área de carga, descarga y almacenamiento.
c) Verificar que los elementos corresponden a lo indicado en las listas de empaque, facturas comerciales y otra información documentada que aplique.
d) Mantener un registro fotográfico o fílmico del proceso (antes, durante y después). Estos registros deben permanecer disponibles, basados en la gestión del riesgo y legislación local vigente.
e) Asegurar la carga con elementos de protección que permitan mantener su integridad y trazabilidad, antes, durante y después del proceso de cargue y mientras se mantenga la custodia de esta.

3.5 Procesamiento de información y documentos de la carga

3.5.1 Debe establecer un procedimiento documentado para el manejo y control de la carga y su documentación, al ingreso o salida de las instalaciones.

3.5.2 La empresa debe:

a) Verificar la coherencia de la información transmitida a las autoridades, de acuerdo con la registrada en los documentos de la operación de la carga.
b) Asegurar que la información documentada relacionada a la gestión de la carga sea legible, completa, precisa y protegida contra modificaciones, pérdida o introducción de datos erróneos.
c) Informar oportunamente a las partes interesadas pertinentes el manejo de la carga durante su custodia.
d) Mantener los registros que evidencien la trazabilidad de la carga de acuerdo con su responsabilidad en la cadena de custodia.

3.6 Novedades con la carga

Debe establecer un procedimiento documentado para gestionar todos los casos relacionados con discrepancias relacionadas con la carga, el material de empaque, embalaje, residuos, desechos y sobrantes que afecten la seguridad de las operaciones de la empresa.

3.7 Comunicación de actividades sospechosas o eventos críticos

Debe establecer un procedimiento documentado para comunicar oportunamente a las autoridades competentes y partes interesadas involucradas cuando ocurran actividades sospechosas o eventos críticos que puedan afectar la integridad de las operaciones definidas en el alcance del SGCS BASC, asegurando el cumplimiento de la legislación vigente. La empresa debe:

a) Documentar la información relacionada con las gestiones realizadas.
b) Hacer una evaluación y análisis posterior con el fin de generar las acciones pertinentes para su tratamiento.
c) Formar y capacitar permanentemente al personal para identificar o reconocer actividades sospechosas que se relacionen con sus funciones.

3.8 Controles en los procesos operativos no relacionados con la carga

Debe establecer un procedimiento documentado para todos aquellos procesos operativos identificados en el alcance del SGCS BASC. Estos deben contemplar:

a) Criterios adecuados para mitigar los riesgos y su impacto en esos procesos.
b) Todas las evidencias necesarias para la trazabilidad en los procesos, a fin de poder identificar las potenciales desviaciones en caso de que se presenten.

4. SEGURIDAD EN LOS PROCESOS RELACIONADOS CON EL PERSONAL

4.1 Procedimiento para la gestión del personal

La empresa debe establecer un procedimiento documentado, con base en la gestión del riesgo y la legislación vigente, que regule las siguientes actividades:

4.1.1 Selección del personal

La empresa debe verificar y analizar en el proceso de selección:

a) Información suministrada por el candidato.
b) Referencias laborales y personales.

c) Antecedentes de los candidatos que ocuparán cargos críticos.
d) Las competencias requeridas para el cargo determinadas por la empresa.
e) Los resultados de:
    i. Pruebas de confiabilidad.
    ii. Pruebas para detectar el consumo de alcohol y drogas ilícitas.
    iii. Visitas domiciliarias.

4.1.2 Contratación del personal

La empresa debe:

a) Mantener un archivo fotográfico actualizado del personal e incluir un registro de huellas dactilares y firma.
b) Expedir y controlar la entrega y uso de carné de identificación con áreas de acceso determinadas y uniformes con distintivos de la empresa, en caso de que aplique.
c) Documentar la entrega de los recursos de seguridad que disponga la empresa, asociados al desempeño del cargo.
d) Registrar la entrega del código de ética, conducta y política de compromiso social de la empresa al colaborador.
e) Incluir en el proceso de inducción el compromiso con el SGCS BASC.
f) Definir requisitos de seguridad asociados al perfil del cargo, para todos los cargos críticos determinados por la empresa y cuando se presenten cambios.

4.1.3 Administración del personal

La empresa debe:

a) Actualizar los datos del personal al menos una vez al año.
b) Verificar los antecedentes del personal que ocupa cargos críticos, como mínimo una vez al año.
c) Aplicar pruebas para detectar el consumo de alcohol y drogas al personal que ocupa cargos críticos, como mínimo cada dos años o cuando se presenten sospechas.
d) Realizar una visita domiciliaria al personal que ocupa cargos críticos, basada en la gestión del riesgo y las regulaciones locales, mínimo cada dos años.
e) Expedir y actualizar el carné de identificación con fotografía, de acuerdo con los procedimientos de la empresa.
f) Evidenciar el uso adecuado de los recursos de seguridad que disponga la empresa, asociados al desempeño del cargo.
g) Evidenciar el cumplimento del código de ética, conducta y política de compromiso social de la empresa.

4.1.4 Terminación de la vinculación laboral

La empresa debe:

a) Eliminar el acceso a las instalaciones y tecnologías de la información de la empresa.
b) Retirar el carné de identificación, uniformes y demás recursos de seguridad con base en los registros generados en la entrega de éstos.
c) Comunicar a las partes interesadas pertinentes la desvinculación del colaborador, con base en la gestión del riesgo.

4.2 Programa de Formación, Capacitación y Concientización

4.2.1 La empresa debe documentar y evaluar anualmente la eficacia de programas relacionados a:

a) Prevención de delitos relacionados con el comercio internacional.
b) Prevención de adicciones que incluyan avisos visibles y/o material de lectura.
c) Responsabilidad social empresarial.
d) Prevención del riesgo de corrupción y soborno.

4.2.2 Debe establecer y mantener un programa anual documentado de capacitación para concientizar al personal en su responsabilidad de reconocer las vulnerabilidades de la empresa relacionadas al SGCS BASC, que incluya como mínimo:

a) Políticas relacionadas con el SGCS BASC.
b) Cumplimiento de compromiso social.
c) Gestión del riesgo, controles operacionales, preparación y respuesta a eventos.
d) Cumplimiento de los requisitos legales relacionados con la empresa.
e) Evaluación de los indicadores de gestión relacionados con los procesos de la empresa.
f) Inspección de unidades de carga y unidades de transporte de carga (ver 2) y seguridad en los procesos de manejo de carga (ver 3).
g) Controles de acceso y seguridad física de las instalaciones (ver 5).
h) Manejo de sellos de seguridad (ver 2.6).
i) Prevención de delitos relacionados a la ciberdelincuencia. (Ver 6).

5. CONTROL DE ACCESO Y SEGURIDAD FÍSICA

5.1 Control de acceso y permanencia en las instalaciones

La empresa debe establecer un procedimiento documentado para los controles de accesos de los colaboradores, visitantes y terceros, que incluya las siguientes actividades:

5.1.1 Acceso de colaboradores:
- a) Identificación positiva.
- b) Controlar su ingreso a las instalaciones.
- c) Restringir el acceso a las áreas críticas determinadas por la empresa.

5.1.2 Acceso a los visitantes, contratistas y terceros:
- a) Solicitar autorización para su ingreso.
- b) Presentar una identificación oficial vigente con fotografía.
- c) Mantener un registro del ingreso y salida de las personas.
- d) Registrar, con base en la gestión del riesgo, los elementos que ingresan a las instalaciones.
- e) Entregar y controlar una identificación temporal.
- f) Asegurar que estén acompañados o controlados por personal de la empresa.
- g) Limitar el acceso a las áreas autorizadas para su visita.

5.1.3 Inspeccionar el correo y paquetes recibidos antes de distribuirlos, manteniendo un registro que incluya la identificación de quién recibe y a quién está destinado.

5.1.4 Inspeccionar los vehículos que entren y salgan de su instalación, conservando los registros correspondientes.

5.1.5 Acceso a autoridades y vehículos de atención a emergencias de acuerdo con el plan y preparación de respuesta a eventos o cuando amerite.

5.1.6 Mantener el control operacional en las instalaciones, que incluya:

- a) Exhibir el carné o identificación temporal en un lugar visible, bajo las normas de seguridad industrial aplicables. Aplica para colaboradores, visitantes, contratistas y terceros.
- b) Controlar las áreas de casilleros (lockers) de los colaboradores y estas deberían estar separadas del área de manejo y almacenaje de carga.
- c) Identificar y retirar a personas no autorizadas.
- d) Asegurar que el personal de seguridad está controlando las puertas de entrada y salida de las instalaciones.

5.2 Seguridad física

5.2.1 Generalidades

La empresa, con base en la gestión del riesgo y su rol en la cadena de suministro, debe establecer procedimientos documentados correspondientes a la seguridad física que incluyan:

a) Estructuras y barreras perimetrales que impidan el acceso no autorizado.
b) Cerraduras en puertas y ventanas.
c) Iluminación que permita el control de las instalaciones en:
    1. Entradas y salidas.
    2. Áreas de almacenamiento y manejo de carga o información.
    3. Cercas perimetrales.
    4. Áreas de estacionamiento.
    5. Otras áreas críticas definidas.
d) Tener un servicio de seguridad competente de conformidad con los requisitos legales y que garantice una acción de respuesta oportuna, preferiblemente certificado BASC.
e) Áreas de estacionamiento para empleados, visitantes y vehículos que entregan o recogen carga.
f) Inspecciones de funcionamiento y mantenimiento con sus respectivos registros.
g) Uso de tecnologías de seguridad:
    1. Sistema operativo de alarma que identifique el acceso no autorizado.
    2. Sistema de videovigilancia que cubra las áreas críticas identificadas y monitoreado por personal competente.
    3. Sistema de respaldo de imágenes y video (grabación) con la capacidad de almacenamiento suficiente para responder a posibles eventos.
    4. Otros que la empresa considere para el SGCS BASC.

5.2.2 La empresa debe establecer, documentar y mantener actualizado:

a) Plano(s) con la ubicación de las áreas críticas de las instalaciones.
b) Control de llaves, dispositivos y claves de acceso.

5.2.3 La empresa debe realizar inspecciones para evaluar la implementación, funcionamiento y mantenimiento de los controles de seguridad física, conservando registro de los hallazgos.

6. SEGURIDAD DE LA INFORMACIÓN

6.1 Generalidades

La empresa debe establecer un procedimiento documentado, con base en la gestión del riesgo y su rol en la cadena de suministro, para:

a) Gestionar y proteger el manejo de la información y los recursos informáticos de la empresa, incluyendo las medidas a aplicar en caso de incumplimiento.
b) Salvaguardar la información y su confidencialidad, integridad y disponibilidad, en sus diferentes formas y estados.
c) Proteger la infraestructura de las tecnologías de la información.

6.2 Ciberseguridad y las tecnologías de la información

La empresa debe:

a) Establecer, documentar y mantener criterios de seguridad que permitan identificar y proteger los sistemas de las tecnologías de la información y recuperarla oportunamente en caso de ser necesario.
b) Identificar partes interesadas y su nivel de criticidad en la infraestructura informática (hardware y software) de la empresa.
c) Comunicar oportunamente información sobre amenazas de ciberseguridad identificadas a las partes interesadas correspondientes.
d) Clasificar la información de acuerdo con la legislación vigente, sistemas y accesos según el nivel de criticidad y establecer políticas de acceso a la misma.
e) Utilizar cuentas asignadas para cada usuario que acceda al sistema, con sus propias credenciales de acceso mediante contraseñas u otras formas de autenticación que generen accesos seguros. Estas deben actualizarse periódicamente, cuando existan indicios o sospechas razonables de que están comprometidas.
f) Limitar los accesos y permisos de los usuarios de acuerdo con las funciones y tareas asignadas, revisándolos periódicamente.
g) Eliminar el acceso a la información a todos los colaboradores, terceros y usuarios externos al terminar su contrato o acuerdo.
h) Impedir la instalación de software no autorizado.
i) Utilizar y mantener hardware y software licenciados y actualizados para proteger la infraestructura de TI contra amenazas informáticas tales como virus, programas espías, gusanos, troyanos, malware, ransomware, entre otros.
j) Realizar copias de seguridad de la información sensible, manteniendo un respaldo fuera de las instalaciones (física o virtual) con las medidas de seguridad necesarias para impedir que terceros accedan a la información.
k) Mantener un registro actualizado de los usuarios, su nivel de criticidad y accesos asignados.
l) Cerrar/bloquear la sesión en equipos desatendidos.
m) Evaluar mínimo una vez al año la seguridad de la infraestructura de TI (hardware y software), implementando acciones pertinentes cuando se hayan detectado vulnerabilidades.
n) Establecer procedimientos y controles para identificar y revisar el acceso no autorizado a los sistemas de información, sitios webs o el incumplimiento de las

políticas y procedimientos (incluyendo la manipulación o alteración de los datos comerciales por parte de los colaboradores o contratistas).

o) Revisar las políticas y los procedimientos de ciberseguridad al menos una vez al año y actualizarlas cuando se presenten cambios en el contexto interno o externo, o cuando se materialice algún riesgo.

p) Emplear tecnologías seguras, como redes privadas virtuales (VPN) o autenticación multifactor para el acceso seguro de los colaboradores y usuarios externos a los sistemas informáticos de la empresa, incluyendo accesos para trabajo remoto o teletrabajo.

q) Establecer procedimientos para evitar el acceso remoto de usuarios no autorizados, desde dispositivos personales u otros.

r) Controlar mediante la realización de inventarios periódicos, los medios u otros equipos que hagan parte de la infraestructura informática de la empresa. La eliminación o desecho de los mismos se hará de acuerdo con la legislación vigente.

s) Restringir la conexión de dispositivos personales y elementos periféricos no autorizados para cualquier dispositivo que forme parte de la infraestructura informática de la empresa.

t) Vigilar el cumplimiento de las políticas de ciberseguridad y seguridad de la información establecidas en el uso de plataformas y contenido digital, herramientas de videoconferencia, comercio electrónico, entre otras.

u) Realizar ejercicios prácticos y/o simulacros relacionados con la seguridad de las tecnologías de la información, que permitan determinar la eficacia de las acciones establecidas (ver Norma 6.1 e).

v) Establecer controles para super usuarios que permitan la continuidad de credenciales de los equipos activos, en caso que aplique.