Manual de políticas y normas de seguridad BASC

V13
SEGURIDAD • RESGUARDO • VIGILANCIA

MANUAL DE POLITICAS Y NORMAS DE SEGURIDAD BASC

Se prohíbe la reproducción total o parcial de éste documento sin autorización de la Gerencia.

Índice General

Capítulo 1: Introducción. 4

Capítulo 2: Conceptos importantes. 5

2.1 ¿Qué es la Certificación BASC? 5

2.2 ¿Cuál es el objetivo principal de la Certificación BASC? 5

2.3 ¿Qué es un Sistema de Gestión? 5

2.4 ¿Qué es una Política? 5

2.5 ¿Cuál es la Política de seguridad BASC de V 13 SAC? 6

2.6 ¿Cuáles son los objetivos de seguridad de V 13 SAC? 7

Capítulo 3: Órganos del Sistema de Gestión BASC 8

3.1. Comité BASC 8

3.2. Auditores Internos BASC 8

Capítulo 4: Administración segura de personal. 9

4.1. Políticas 9

Política de formación 9

Política de participación e incentivos 9

Política sobre Infracciones 9

Política de protección intelectual y derechos de autor 10

4.2. Procedimientos de seguridad BASC – Administración segura de personal 10

4.3. Normas de seguridad para la "Administración segura de personal" 11

Capítulo 5: Control de accesos y seguridad física. 12

5.1. Políticas 12

Política sobre la seguridad física 12

Política sobre recepción de paquetes y correos 12

5.2. Procedimientos de seguridad BASC - Control de accesos y seguridad física 12

5.3. Normas de seguridad para el "Control de accesos y seguridad física" 13

Capítulo 6: Control de la información. 14

6.1. Políticas 14

Política sobre uso adecuado de los sistemas informáticos 14

Política de firmas 14

Política de veracidad y protección de datos 14

6.2. Procedimientos de seguridad BASC – Control de la información 14

Se prohíbe la reproducción total o parcial de éste documento sin autorización de la Gerencia.

6.3. Normas de seguridad para el "Control de la información" 15

Capítulo 7: Reporte en caso de amenazas ilícitas. 16

7.1. Políticas 16

Política sobre manejo de amenazas ilícitas 16

7.2. Procedimientos de seguridad BASC – Reporte en caso de amenazas ilícitas 16

7.3. Normas de seguridad para "Reporte en caso de amenazas ilícitas" 16

Capítulo 8: Información Complementaria. 17

8.1. Seguridad de la Información - Ciberataques 17

8.2. Prácticas de prevención de corrupción y soborno 18

8.3. Alerta de actividades sospechosas - clientes 19

8.4. Alerta de actividades sospechosas - proveedores 19

8.5. Aspectos relevantes que presenta una persona que consume drogas 20

8.6. ¿Qué pasaría si a la empresa lo involucran en un acto ilícito? 20

8.7. Política de Responsabilidad Social Empresarial 21

Se prohíbe la reproducción total o parcial de éste documento sin autorización de la Gerencia.

Capítulo 1: Introducción.

El presente **Manual de Inducción BASC** es un documento de consulta y/o herramienta-guía, que servirá al empleado a conocer cuáles son los lineamientos de seguridad de la empresa y cómo cada trabajador se involucra en la aplicación y mejora continua del Sistema de Gestión en Control y Seguridad BASC.

Sirve también como un documento de referencia para manejar situaciones especialmente sospechosas relacionadas con alguna actividad ilícita que comprometa directa o indirectamente a la empresa.

Éste manual contiene información de temas específicos, tanto formal como informal, ha sido escrito en un lenguaje que resulte sencillo de leer para el usuario.

Refiere además sobre las políticas, procedimientos y normas de seguridad relacionados a: Administración segura de personal; Control de accesos y seguridad física, Control de la información; Reporte en caso de amenazas ilícitas.

Se prohíbe la reproducción total o parcial de éste documento sin autorización de la Gerencia.

Capítulo 2: Conceptos importantes.

2.1 ¿Qué es la Certificación BASC?

Es la validación que emite la Organización Mundial BASC, al verificar el cumplimiento de los estándares de seguridad BASC, dentro de los procesos que desarrolla la empresa.

La OMB es una alianza empresarial a nivel internacional, que en cooperación con gobiernos y otros organismos internacionales, promueven la implantación de estándares de seguridad en los procesos que se desarrollan dentro la cadena logística del comercio global.

2.2 ¿Cuál es el objetivo principal de la Certificación BASC?

El objetivo principal es **promover el comercio seguro** a través de la implantación de un Sistema de Gestión en Control y Seguridad, mediante el cual se evite el tráfico ilícito de drogas, terrorismo, lavado de activos, contrabando, corrupción, soborno u otros delitos conexos.

2.3 ¿Qué es un Sistema de Gestión?

Es un conjunto de elementos (Base documental, procedimientos, capacitación, equipos, personal, etc.), que interactúan entre sí bajo determinados lineamientos, normas y/o estándares, coordinando las acciones necesarias para lograr un objetivo específico dentro de los productos o servicios que brinda una organización.

2.4 ¿Qué es una Política?

La Política es una declaración formal de los dueños o accionistas de una organización, sobre los principios y valores que se comprometen a cumplir, en ella se dan una serie de reglas y directrices generales, las cuales regirán las actividades y esfuerzos de sus integrantes a fin de alcanzar los objetivos esperados.

La Política es un documento auditable y constituye la base fundamental del desarrollo de un Sistema de Gestión, por ello debe ser conocida y entendida por todos los integrantes de la organización en todos sus niveles.

Se prohíbe la reproducción total o parcial de éste documento sin autorización de la Gerencia.

2.5 ¿Cuál es la Política de seguridad BASC de V 13 SAC?

POLITICA DE GESTION EN CONTROL Y SEGURIDAD BASC

V13 S.A.C. brinda servicios especializados en el rubro de Seguridad, Resguardo y Vigilancia, siendo los siguientes nuestros lineamientos:

- ✓ **Prevenir** el tráfico ilícito de drogas, el contrabando, lavado de activos, corrupción, soborno entre otras actividades ilícitas.
- ✓ **Establecer** procedimientos que permitan identificar, prevenir y controlar los riesgos que puedan llegar a presentarse.
- ✓ **Cumplir** con los requisitos legales o de otra índole, que sean aplicables a los procesos o actividades, con el fin de satisfacer los requerimientos establecidos por el estado.
- ✓ **Promover** la seguridad en el uso de la tecnología de la información y la participación, consulta y desarrollo integral del personal.
- ✓ **Mejora continua** de nuestros procesos, infraestructura y tecnología.

Freddy Hurtado Niño de Guzmán
Gerente General

Octubre 2023

Se prohíbe la reproducción total o parcial de éste documento sin autorización de la Gerencia.

2.6 ¿Cuáles son los objetivos de seguridad de V 13 SAC?

OBJETIVOS DE SEGURIDAD BASC

- ✓ Actualizar y gestionar continuamente la base documental para prevenir los riesgos y amenazas asociados a las actividades que se desarrollan en la empresa con la finalidad de evitar que sea utilizada para realizar actividades ilícitas como: tráfico ilícito de drogas, contrabando, lavado de activos, fraude, corrupción, soborno, financiamiento al terrorismo, entre otras actividades ilícitas que perjudique a la empresa o la comunidad.
- ✓ Realizar la debida diligencia a los clientes de acuerdo al Sistema de Gestión BASC.
- ✓ Realizar la debida diligencia a los proveedores críticos de acuerdo al Sistema de Gestión BASC.
- ✓ Formar las competencias del personal en cuanto a la identificación riesgos, delitos asociados a la cadena logística, entre otros que puedan afectar el desarrollo de las actividades de la empresa.
- ✓ Mantener la integridad, disponibilidad, privacidad, control y autenticidad de la información de la empresa manejada por los usuarios.
- ✓ Asegurar a los asociados de negocios el cumplimiento de sus requisitos, los requisitos de la norma, requisitos legales y los requisitos definidos por la empresa.

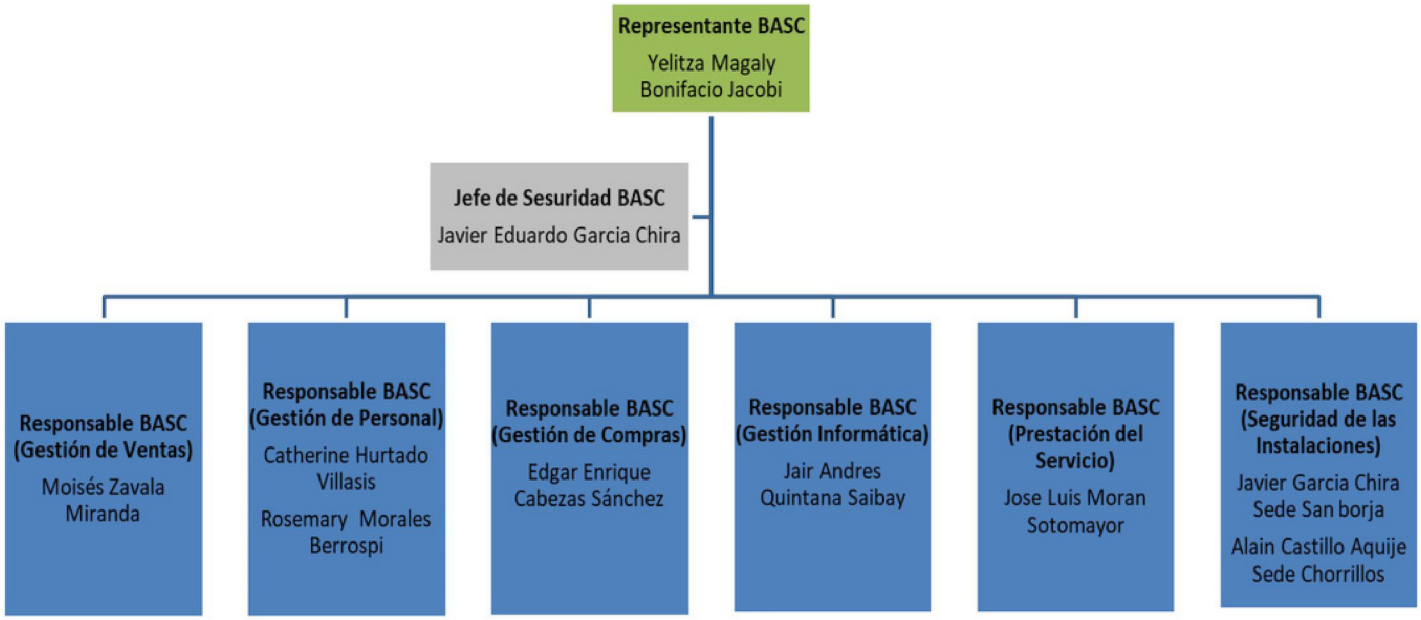
Freddy Hurtado Niño de Guzmán
Gerente General

Octubre 2023

Se prohíbe la reproducción total o parcial de éste documento sin autorización de la Gerencia.

Capítulo 3: Órganos del Sistema de Gestión BASC

3.1. Comité BASC



3.2. Auditores Internos BASC

Se prohíbe la reproducción total o parcial de éste documento sin autorización de la Gerencia.

Capítulo 4: Administración segura de personal.

4.1. Políticas

Política de formación

"V 13 SAC., se compromete a brindar la formación necesaria para el desarrollo de las competencias técnicas y profesionales de sus trabajadores, las cuales deben estar alineadas con las necesidades y objetivos estratégicos de la organización, logrando de ésta manera, el desarrollo profesional de sus colaboradores y un óptimo desempeño de las actividades laborales"

Las actividades de formación deberán seguir los siguientes lineamientos:

- Toda capacitación debe responder a una necesidad directamente relacionada con el desempeño de las actividades del trabajador.
- Todos los trabajadores tienen la misma oportunidad de acceder a cursos de formación cuando las circunstancias lo ameriten.
- Se brindará los cursos de capacitación a los trabajadores, en un proceso continuo y priorizando los objetivos estratégicos de la organización.
- Los trabajadores que son beneficiados con los cursos de formación, deberán compartir e impartir los conocimientos y/o habilidades adquiridas, contribuyendo a un mejor desempeño de las actividades en su área de trabajo y en otras áreas de la empresa.
- Establecer una cultura de Capacitación y Entrenamiento que promueva el desarrollo personal y profesional del trabajador.

Política de participación e incentivos

"V 13 SAC estimula la colaboración de todo el personal para reportar cualquier incidente o actividad sospechosa, así como el cumplimiento, desarrollo y mejora continua del Sistema de Gestión en Control y Seguridad BASC, mediante premios, distinciones u otros incentivos"

Política sobre Infracciones

"Todo empleado de V 13 SAC será sancionado por la gerencia general dependiendo del grado de infracción cometida al no cumplir con las

Se prohíbe la reproducción total o parcial de éste documento sin autorización de la Gerencia.

políticas y normas de la empresa en vías de salvaguardar y realizar actividades seguras"

Política de protección intelectual y derechos de autor

"Los empleados deben tener presente que la empresa pone a su disposición ciertas listas de clientes, datos de precios, fuentes de suministro, técnicas, información computarizada, métodos, información, etc., estos tienen un valor económico, real y/o potencial, que no es dado a conocer al público o a los otros que podrían obtener el valor económico de su descubrimiento o empleo y que esta información es sujeta a un esfuerzo razonable por V 13 SAC de mantener su secreto y confidencialidad.

Por lo tanto, el empleado:

- NO realizará la duplicación u otra copia de los documentos antes mencionados.
- NO realizará mal uso de estos.
- NO utilizará la información finalizado la relación laboral.
- NO realizará la instalación de software que no posee la licencia correspondiente.
- Devolverá inmediatamente se le solicite, todo material confidencial que se le haya dado.

4.2. Procedimientos de seguridad BASC – Administración segura de personal

4.2.1. Desarrollo de formatos BASC.-

Todo trabajador deberá actualizar anualmente su información personal, mediante el formato "Estudio de seguridad para empleados - Actualización"

4.2.2. Certificados de antecedentes. -

El trabajador deberá presentar sus certificados de antecedentes al momento de su contratación actualizándolos según procedimiento.

Se prohíbe la reproducción total o parcial de éste documento sin autorización de la Gerencia.

4.2.3. Exámenes toxicológicos o de Alcoholemia. -

Los estándares BASC exigen la realización de pruebas toxicológicas o alcoholemia al personal, a fin de detectar el consumo de drogas u otras sustancias tóxicas.

Las pruebas pueden realizarse de manera inopinada (sin previo aviso), la negación a éstas constituye una falta contra la política de seguridad de la empresa, en tal caso, la dirección de la empresa adoptará las acciones que estime conveniente.

4.2.4. Verificación domiciliaria. -

Todo trabajador deberá brindar las facilidades para la realización de la verificación domiciliaria, la cual se realiza en cumplimiento de los estándares de seguridad BASC.

4.3. Normas de seguridad para la "Administración segura de personal"

a) Todo trabajador deberá asistir obligatoriamente a las charlas de capacitación que la empresa organiza.

b) Cada trabajador deberá presentar físicamente o digital y con carácter obligatorio, los certificados de estudios y/o trabajo, que avalen lo mencionado en su currículo vitae.

c) Todos los implementos de trabajo entregados al trabajador, deberán ser devueltos al término de la relación laboral.

d) Todo trabajador deberá atender obligatoriamente, la realización de las auditorías BASC, ya sean internas o externas.

Se prohíbe la reproducción total o parcial de éste documento sin autorización de la Gerencia.

Capítulo 5: Control de accesos y seguridad física.

5.1. Políticas

Política sobre la seguridad física

"**V 13 SAC** considera que la seguridad física es un aspecto esencial en la implementación de un Sistema de Gestión BASC, mediante el cual se protege la integridad de sus trabajadores y asociados de negocios, así como la información relacionada con ellos"

Política sobre recepción de paquetes y correos

No se permite la recepción de correspondencia y/o paquetes personales dentro de las instalaciones de V 13 SAC

5.2. Procedimientos de seguridad BASC - Control de accesos y seguridad física

5.2.1. Uso de fotocheck.-

Durante la jornada de trabajo, todo trabajador deberá portar su fotocheck en un lugar visible.

"Cuida tu fotocheck, su uso es único e intransferible"

5.2.2. Control de llaves. -

La entrega de llaves se registra bajo un cargo, el cual responsabiliza al trabajador sobre su correcto uso. La entrega de llaves es un acto de confianza, por lo cual es intransferible, ningún trabajador deberá entregar sus llaves a terceros.

5.2.3. Atención de visitantes. -

El trabajador encargado de atender al visitante deberá acompañarlo en todo momento durante su permanencia dentro de las instalaciones y solicitar que el visitante porte en lugar visible su pase de visitante.

5.2.4. Enfrentamiento y retiro de personas. -

Si algún trabajador detecta alguna persona ajena a la empresa, sin su respectivo pase visitante; o con su pase visitante, en un área no

Se prohíbe la reproducción total o parcial de éste documento sin autorización de la Gerencia.

autorizada, preguntará a la persona el motivo de su presencia y la acompañará hasta el área de recepción, comunicando el incidente al Jefe de Seguridad BASC.

5.3. Normas de seguridad para el "Control de accesos y seguridad física"

a) Se encuentra terminantemente prohibido el ingreso de armas.

b) Todo visitante deberá registrar en recepción el ingreso y salida de equipos.

c) Las personas que requieran trabajar fuera del horario normal, deberán solicitar la respectiva autorización al responsable del área.

d) Todo el personal deberá participar activamente en el desarrollo de simulacros.

e) Si se detecta alguna actividad sospechosa o ilícita, cualquier trabajador deberá comunicarlo directamente al Representante BASC o al Comité BASC de la empresa.

f) Todo trabajador debe conocer el Plan de contingencia para casos de sismo o incendios.

g) Toda incidencia que atente contra la seguridad actual o futura deberá ser reportada al Comité de seguridad BASC.

h) El personal que conforma el Comité de seguridad BASC deberá contar con una lista actualizada de los números de emergencia.

NUMEROS DE EMERGENCIA	
POLICIA NACIONAL DEL PERU (Emergencias)	105
CUERPO GENERAL DE BOMBEROS	116
DIRANDRO	980163956 0800-19900
UDEX (Explosivos - PNP)	433-3333
DININCRI (Crímenes - PNP)	980121221 4317280
BASC Perú	612-8300

Se prohíbe la reproducción total o parcial de éste documento sin autorización de la Gerencia.

Capítulo 6: Control de la información.

6.1. Políticas

Política sobre uso adecuado de los sistemas informáticos

"Todo trabajador debe manejar en forma responsable la información física y electrónica de V 13 SAC protegiendo la confidencialidad de la misma y evitando su uso no autorizado"

Política de firmas

"Todo trabajador firmará, autorizará y/o avalará únicamente los documentos que corresponden a su cargo y función, bajo ninguna circunstancia podrá atribuirse funciones que no le correspondan"

Política de veracidad y protección de datos

V 13 SAC considera que uno de sus activos más importantes es el manejo y protección de la información de sus clientes, por lo cual:

- Los empleados garantizarán en todo momento la protección y confidencialidad de la información física y electrónica de la empresa, contra actos de adulteración, filtro, sustracción o pérdida.
- Los empleados deberán asegurar que toda la información proporcionada por el cliente se encuentre de manera clara y completa, de no ser así, se comunicarán con éste para la corrección de la información o de los documentos involucrados.
- Los empleados deberán asegurar que toda información transmitida a las autoridades, sea coherente con la información contenida en los documentos de la operación.

6.2. Procedimientos de seguridad BASC – Control de la información

6.2.1. Registro de sellos y firmas. -

Todo trabajador deberá registrar los sellos y firmas que son de su uso, a fin de establecer las responsabilidades sobre los procesos en los cuales participan.

Se prohíbe la reproducción total o parcial de éste documento sin autorización de la Gerencia.

6.2.2. Accesos al sistema de información. -

Los accesos al sistema de información se establecen de acuerdo a la función y cargo de cada trabajador.

Si usted detecta accesos a información que no forman parte de la función que desempeña, deberá comunicarlo inmediatamente al Jefe de Seguridad BASC.

6.2.3. Copia de respaldo (Back Up). -

Todos los empleados deben seguir el procedimiento para realizar adecuadamente el back up y estos son resguardados fuera de las instalaciones.

6.3. Normas de seguridad para el "Control de la información"

a) Ningún trabajador compartirá su usuario o contraseña con otro trabajador.

b) Se encuentra terminantemente prohibido la instalación de programas no autorizados por el área de Sistemas.

c) Todo trabajador deberá mantener su protector de pantalla activo y con contraseña.

d) Se prohíbe realización de trabajos personales, durante las horas de trabajo.

e) Todo trabajador deberá proteger y mantener la confidencialidad de la información relacionada a las operaciones, a los clientes, a los proveedores y/o a los trabajadores de la empresa.

f) Ningún trabajador deberá extraer o divulgar ningún tipo de información, sin la autorización de su jefe o responsable de área.

g) Todo documento deberá contener todas las firmas que se solicita en el mismo.

Se prohíbe la reproducción total o parcial de éste documento sin autorización de la Gerencia.

Capítulo 7: Reporte en caso de amenazas ilícitas.

7.1. Políticas

Política sobre manejo de amenazas ilícitas

"Bajo ninguna circunstancia de amenazas o extorsión, ningún integrante de V 13 SAC participará en actividades relacionadas con actos ilícitos"

7.2. Procedimientos de seguridad BASC – Reporte en caso de amenazas ilícitas

7.2.1. Reporte de actividades sospechosas.-

Si un trabajador es contactado para participar en actividades que puedan estar involucradas con actos ilícitos; o si observa alguna actividad sospechosa, deberá comunicarlo inmediatamente al Comité de Seguridad BASC.

7.2.2. Reporte de incidencias.-

Todo trabajador que observe algún incidente que pueda afectar la seguridad de la empresa, deberá reportarlo al Comité de seguridad BASC.

7.2.3. Sanción en caso de falso reporte.-

Todo trabajador será sancionado en caso de:

a) **Realizar reportes falsos en contra de compañeros de trabajo, clientes o proveedores.**
b) **Alterar las evidencias de una situación sospechosa.**

7.3. Normas de seguridad para "Reporte en caso de amenazas ilícitas"

a) Todo trabajador debe conocer el "procedimiento Plan en caso de amenazas ilícitas".
b) Está prohibido informar sobre alguna actividad sospechosa a otro trabajador.

Se prohíbe la reproducción total o parcial de éste documento sin autorización de la Gerencia.

Capítulo 8: Información Complementaria.

8.1. Seguridad de la Información - Ciberataques

Un ciberataque es un conjunto de acciones dirigidas contra sistemas de información, como pueden ser bases de datos o redes computacionales, con el objetivo de perjudicar a personas, instituciones o empresas. Este tipo de acción puede atentar tanto contra los equipos y sistemas que operan en la red, anulando sus servicios, como contra bases que almacenan información, siendo esta espiada, robada o, incluso, utilizada para extorsionar.

En un mundo digital, el número de ciberataques no cesa de aumentar. De hecho, según Kaspersky, empresa líder en ciberseguridad, durante la pandemia incrementaron en un 25 %. Como consecuencia, la preocupación y la inversión en sistemas de protección también lo hace. Y es que estos ataques pueden comprometer todo tipo de información, poniendo en jaque a empresas y particulares. Tipos de ciberataques.

- ✓ Phishing. - consiste en el envío de mensajes fraudulentos, usualmente a través de correo electrónico, que aparentemente proceden de fuentes fiables y seguras. El principal objetivo de este tipo de ciberataque es robar datos personales muy sensibles, como información sobre inicios de sesión o datos de tarjetas de crédito, entre otros.
- ✓ Malware. - software malicioso que incluye virus y gusanos. Básicamente, lo que hace es aprovechar las vulnerabilidades para infringir las redes y suele atacar cuando un usuario hace clic en un enlace o en un archivo adjunto a un email.
- ✓ Inyección de SQL. - se produce cuando un hacker inserta un código malicioso en un servidor que utiliza SQL, forzándolo a desvelar información protegida o que normalmente no revelaría.
- ✓ Ataque de denegación de servicio. - provoca la saturación de los sistemas, los servidores e, incluso, las redes con tráfico con el objetivo de agotar los recursos y el ancho de banda. Los hackers suelen utilizar distintos dispositivos preparados específicamente para lanzar el ataque y las consecuencias se traducen en la incapacidad para completar las solicitudes legítimas.

CÓMO PROTEGERSE DE UN CIBERATAQUE

❖ Actualización de los equipos.	❖ Uso de contraseñas largas y complejas.	❖ Comprobar la autenticidad de enlaces y perfiles.
❖ Denunciar ante las autoridades.	❖ No proporcionar datos personales	

Se prohíbe la reproducción total o parcial de éste documento sin autorización de la Gerencia.

8.2. Prácticas de prevención de corrupción y soborno

8.2.1. ¿Cómo prevenimos la corrupción y el soborno?

- Establecimiento de un Código de Ética.
- Establecimiento de procedimientos de control.
- Lista de infracciones y sanciones.
- Capacitaciones e inducciones contantes.
- Verificaciones aleatorias de cumplimiento.
- Auditorias.

8.2.2. Triangulo del fraude

El Triángulo del Fraude se define como: "un modelo que puede ser usado para explicar los factores que llevan a una persona a cometer un fraude laboral". El Triángulo del Fraude, se divide en tres componentes:

- Presión: Es la primera pata del triángulo del fraude, es lo que motiva el crimen en primera instancia. El individuo tiene problemas y no es capaz de resolverlos a través de acciones legítimas, por ello, empieza a considerar el cometer un acto ilegal, como robar dinero o falsificar estados financieros y ve en ellos una salida para resolver su problema.
- Oportunidad: Es la segunda pata del triángulo del fraude y se basa en la oportunidad que puede percibir una persona para cometer el crimen. El individuo debe tener alguna manera en la que su posición de confianza le pueda facilitar el cometer un abuso y así poder solucionar su problema.
- Racionalización: Es la tercera y última pata del triángulo del fraude y es donde la mayoría de los individuos fraudulentos que no tienen un pasado criminal caen. Ellos se ven como personas honestas, ordinarias y se justifican a sí mismos el acto ilegal como una manera correcta y necesaria de salir de sus problemas.

8.2.3. ¿Cómo combatir el soborno?

Las estrategias para combatir el soborno deben centrarse en la "tolerancia CERO" al soborno y deben empezar por la concientización, educación, compromiso de la alta gerencia, desarrollo de buenas prácticas, una adecuada gestión de riesgos, así como la existencia y cumplimiento de un régimen sancionatorio que se pueda ejemplarizar.

Se prohíbe la reproducción total o parcial de éste documento sin autorización de la Gerencia.

8.3. Alerta de actividades sospechosas - clientes

Tomar en cuenta cualquier indicio que indique alguna actividad sospechosa. A continuación, se señalan algunos ejemplos:

- El cliente proporciona datos no consistentes o falsos sobre los representantes, dirección, teléfonos, etc.
- El cliente es nuevo en el mercado y no tiene referencias comerciales.
- Los productos que exporta o importan el cliente no son frecuentes para ese punto de destino.
- El cliente intenta realizar los pagos al contado sin utilizar el sistema bancario.
- El Cliente rehúye a ser visitado en sus instalaciones.
- El Cliente rehúye a visitar nuestras oficinas, coordinando todo únicamente por teléfono y/o correo electrónico.
- Presencia de trabajadores de otras áreas, muy interesados en la información sobre el envío de alguna en carga en particular.
- Pérdida de los registros de seguridad y control.

8.4. Alerta de actividades sospechosas - proveedores

Tomar en cuenta cualquier indicio que indique alguna actividad sospechosa. A continuación, se señalan algunos ejemplos:

- El Proveedor proporciona datos no consistentes o falsos sobre los representantes, dirección, teléfonos, etc.
- El Proveedores nuevo en el mercado y no tiene referencias comerciales.
- Presencia de trabajadores de otras áreas, muy interesados en la contratación de un proveedor en particular.
- El Proveedor ofrece “Presentes” cuyo valor, excede un gesto de cortesía.
- Solicitud de algún trabajador u otra persona para direccionar un determinado servicio con un proveedor en particular.
- Insistencia de algún proveedor para manejar algún servicio específico en particular.
- Pérdida de los registros de seguridad y control.

Se prohíbe la reproducción total o parcial de éste documento sin autorización de la Gerencia.

8.5. Aspectos relevantes que presenta una persona que consume drogas

▪ **Euforia.**	▪ **Alucinaciones.**
▪ Alteraciones en la coordinación.	▪ Tos crónica.
▪ Somnolencia o hiperactividad.	▪ Agresividad.
▪ Pérdida de apetito.	▪ Risas inmotivadas.
▪ Pánico y ansiedad.	▪ Temblor, nauseas, vómitos.
▪ Falta de concentración y de memoria.	▪ Ausentismo laboral.

8.6. ¿Qué pasaría si a la empresa lo involucran en un acto ilícito?

A LA EMPRESA:

- Se paralizan los servicios.
- Probable cierre de la empresa.
- Pérdida de la confianza y credibilidad.
- Pérdida de clientes.
- Pérdida de imagen.

AL PERSONAL:

- Pérdida del empleo.
- Pérdida de la libertad.
- Exhaustiva y constante investigación policial.
- Problemas familiares.
- Antecedentes judiciales.
- Dificultad para conseguir nuevos trabajos.
- Tachados de por vida.

Se prohíbe la reproducción total o parcial de éste documento sin autorización de la Gerencia.

8.7. Política de Responsabilidad Social Empresarial

POLÍTICA DE RESPONSABILIDAD SOCIAL EMPRESARIAL

"V 13 SAC mantiene identificados a sus Grupos de Interés como: Directorio, Colaboradores, Clientes, Proveedores, Comunidad y Competencia. Quienes intervienen en el cumplimiento de los objetivos empresariales planteados por las acciones, decisiones, políticas o prácticas empresariales asumidas por V 13 SAC

V 13 SAC fundamenta su Política de Responsabilidad Social Empresarial, en principios y prácticas que atienden las necesidades y expectativas de sus Grupos de Interés, con el compromiso de:

- Ser eficientes en nuestras actividades con el fin de crear valor para nuestros Accionistas.
- Implementar prácticas del Buen Gobierno Corporativo; basadas en la transparencia y ética empresarial; así como la confianza mutua con los colaboradores.
- Respetar los derechos humanos y laborales de nuestros colaboradores evitando el abuso laboral, la discriminación de cualquier índole, el trabajo forzoso, el trabajo infantil y otras violaciones a los derechos humanos.
- Desarrollar un ambiente favorable de relaciones laborales basado en la igualdad de oportunidades, la no discriminación y el respeto a la diversidad, gestionando el desarrollo permanente de las competencias de nuestros colaboradores, promoviendo la prevención en los temas seguridad y salud en el trabajo, y facilitando la libre comunicación en todos los niveles.
- Difundir la información pública de la empresa dentro de un marco de transparencia, así como brindar la información relevante en forma veraz sobre el servicio que se brinda.
- Capacitar, formar y motivar al personal para que contribuya en el cumplimiento de lo establecido en la presente política.

Gerencia General
Octubre 2023

Se prohíbe la reproducción total o parcial de éste documento sin autorización de la Gerencia.