TECNISEG Tecnologías Integrales de Seguridad de Colombia Ltda.	**DECLARACION DE APLICABILIDAD EN DERECHOS HUMANOS DEL SISTEMA DE GESTION PARA OPERACIONES DE SEGURIDAD PRIVADA**	**Código: SIG-E-22** **Versión: 02** **Fecha: 04/05/2024**

TECNISEG DE COLOMBIA LTDA., Empresa prestadora del servicio de Vigilancia y Seguridad privada, en la modalidad de vigilancia fija, móvil, con arma y sin arma, escoltas, asesoría, consultoría y medios tecnológicos, reconoce la importancia de generar un compromiso dentro de la organización relacionada para respetar los Derechos Humanos de acuerdo al Sistema de Gestión de Operaciones de Seguridad en la cadena de suministro (SGOS), para ello se tiene en cuenta la siguiente declaración de aplicabilidad para el sistema de operaciones de seguridad:

- ***TECNOLOGÍAS INTEGRALES DE SEGURIDAD DE COLOMBIA LTDA, establece como campo de aplicación de la certificación para ISO 18788:***

  "Prestación de Servicios de vigilancia y seguridad privada, en las modalidades de fija, móvil, con arma y sin armas, con uso de medios tecnológicos, uso de caninos; servicio de escolta a personas, vehículos y mercancías; servicio de asesoría y consultoría en seguridad. Todos los servicios se tienen controlados donde se garantiza un impacto positivo en el desempeño de la seguridad y salud en el trabajo, adicional se garantiza el control de las cuestiones internas y externas, control de los riesgos y oportunidades para continuidad del negocio, control de las necesidades y expectativas de las partes interesadas".

SEDE	ALCANCE
Bogotá (Principal) Calle 152 A #17-04 Barrio Cedritos	Prestación del Servicios de vigilancia y seguridad privada, en las modalidades: 1. Fija, móvil, con y sin armas, 2. Con uso medios tecnológicos, 3. Con uso de medios caninos; 4. Escolta a personas, 5. Asesoría y consultoría en seguridad
Barrancabermeja: Calle 57 # 23-24 Barrio Galán	Prestación del Servicios de vigilancia y seguridad privada, en las modalidades: 1. Fija, móvil, con y sin armas, 5. Asesoría y consultoría en seguridad
Bucaramanga Calle 104 # 19-21 Barrio Provenza	Prestación del Servicios de vigilancia y seguridad privada, en las modalidades: 1. Fija, móvil, con y sin armas, 5. Asesoría y consultoría en seguridad
Valledupar Calle 12 #5-55 Barrio Novalito	Prestación del Servicios de vigilancia y seguridad privada, en las modalidades: 1. Fija, móvil, con y sin armas, 5. Asesoría y consultoría en seguridad

Cali Avenida 6 A Norte # 24-53 Piso 2 Barrio Santa Mónica	Prestación del Servicios de vigilancia y seguridad privada, en las modalidades: 1. Fija, móvil, con y sin armas, 5. Asesoría y consultoría en seguridad
Medellín Carrera 78 A # 48 B -69 Barrio Sector Estadio	Prestación del Servicios de vigilancia y seguridad privada, en las modalidades: 1. Fija, móvil, con y sin armas, 5. Asesoría y consultoría en seguridad
Pereira Carrera 11 # 44-18 Barrio Maraya	Prestación del Servicios de vigilancia y seguridad privada, en las modalidades: 1. Fija, móvil, con y sin armas, 2. Con uso medios tecnológicos, 4. Escolta a personas, 5. Asesoría y consultoría en seguridad
Tunja Carrera 9 # 26-31 Local 4 Barrio Las Nieves	Prestación del Servicios de vigilancia y seguridad privada, en las modalidades: 1. Fija, móvil, con y sin armas, 3. Con uso de medios caninos; 5. Asesoría y consultoría en seguridad
Tuluá Calle 17 #30-67 con Cra. 31 Esq.	Prestación del Servicios de vigilancia y seguridad privada, en las modalidades: 1. Fija, móvil, con y sin armas, 5. Asesoría y consultoría en seguridad
Barranquilla Calle 82 #41E-39-Ciudad Jardín	Prestación del Servicios de vigilancia y seguridad privada, en las modalidades: 1. Fija, móvil, con y sin armas, 5. Asesoría y consultoría en seguridad

1. EXCLUSIONES ISO 18788

TECNOLOGÍAS INTEGRALES DE SEGURIDAD DE COLOMBIA LTDA, establece como ***Exclusiones*** de la certificación ISO 18788:

- **8.3.6 Uso de la fuerza como apoyo de las fuerzas del orden:** De acuerdo con la regulación colombiana las empresas de vigilancia no están autorizadas para apoyar operaciones de las fuerzas del orden. **No aplicabilidad valida.**

- **8.5.1 Apoyo a las fuerzas del orden:** De acuerdo con la regulación colombiana las empresas de vigilancia no están autorizadas para apoyar operaciones de las fuerzas del orden. **No aplicabilidad valida.**

- **8.5.2 Operaciones de detención:** De acuerdo con la regulación colombiana las empresas de vigilancia no están autorizadas para apoyar operaciones de detención. **No aplicabilidad valida.**

2. CONTEXTO DE LA ORGANIZACIÓN

TECNOLOGÍAS INTEGRALES DE SEGURIDAD DE COLOMBIA Ltda., es una empresa legalmente constituida el 19 de octubre de 1999 bajo escritura pública No. 0003476 de la Notaria 25 de Bogotá e Inscrita ante Cámara de Comercio el día 26 de Octubre de 1999 bajo el número 00701244 del libro IX.

OBJETIVO GENERAL SGOS

Proteger en términos contractuales los derechos humanos, como respeto por la vida, la dignidad humana y las libertades fundamentales.

OBJETIVOS ESPECIFICOS SGOS

- Establecer mecanismos para reportar toda no conformidad, los incidentes y los eventos indeseados y perturbadores. (OP-PQRSF- SSTA-Reporte incidente)
- Promover la responsabilidad ante el uso apropiado de la fuerza. (CAPACITA-OP).
- Promover una cultura de implementación de los principios y compromisos del código ICOC. (CAPACITA-OP).
- Implementar en los procesos de la organización la transformación empresarial con enfoque en seguridad con sentido humano en defensa de los Derechos Humanos. (CAPACITA-OP)
- Apoyar los objetivos del Documento Montreux, no admitiendo el genocidio, crímenes de la humanidad, la tortura, el tratamiento inhumano, degradante, la esclavitud, desigualdad, juicio injusto, discriminación por pensamiento, conciencia, religión y todos los relacionados con el Derecho Internacional Humanitario, respetando las libertades fundamentales, derechos humanos y leyes nacionales e internacionales. (NOVEDADES DELICTIVA-OP)
- Gestionar la inclusión equidad como principios de la compañía. (RF-Entrega de dotación)
- Gestión de riesgo y seguridad enfocada en los clientes en defensa de los DDHH con generación de valor en nuestras partes interesadas. (RIESGO Y OPORTUNIDADES)

APLICABILIDAD DE LA NORMA ISO 18788 Y ANEXA A

ITEM DE LA NORMA ISO 18788	CRITERIO	ISO 18788, CUMPLE-NO CUMPLE -NO APLICA	ANEXO "A" ISO 18788, CUMPLE, NO CUMPLE-NO APLICA	OBSERVACIONES
4.	**CONTEXTO DE LA ORGANIZACIÓN**			
4.1	**4.1 COMPRENSIÓN DE LA ORGANIZACIÓN Y SU CONTEXTO**			
4.1.1	**4.1.2 GENERAL**			
	La Organización **debe** definir y documentar su contexto interno y externo, incluyendo su cadena de suministro y subcontratistas. Estos factores deben ser tomados en cuenta cuando se establezca, implemente y mantenga el SGOS de la organización y se asignen sus prioridades. La organización **debe** evaluar los factores internos y externos que puedan influenciar la manera en la que la organización gestiona el riesgo.	SI	SI	
4.1.2	**4.1.2 CONTEXTO INTERNO**			
	El Contexto interno incluye: a) Los objetivos, estrategias y misión de negocios de la organización. b) Las políticas, planes y lineamiento para cumplir los objetivos. c) El liderazgo, roles y responsabilidades. d) La estrategia general para la gestión del riesgo. e) Partes interesadas internas. f) Los valores, la ética y la cultura. g) El flujo de información y los procesos de toma de decisiones. h) Las capacidades, los recursos y los bienes. i) Los procedimientos, los procesos y las prácticas. j) Las actividades, funciones, servicios y productos. k) La marca y la reputación.	SI	SI	
4.1.3	**4.1.3 CONTEXTO EXTERNO**			
	El Contexto externo, incluye: a) El contexto político y cultural. b) El ambiente legal, regulatorio, tecnológico, económico, natural y competitivo. c) Los acuerdos contractuales, incluyendo otras organizaciones dentro del alcance del contrato. d) Las dependencias de infraestructura y las interdependencias operacionales. e) Los acuerdos y relaciones con los contratistas y la cadena de suministro. f) Las cuestiones clave y las tendencias que puedan impactar los procesos y/u objetivos de la organización. g) La percepción, los valores, necesidades e intereses de las partes interesadas externas (incluyendo las comunidades locales en las áreas de operación). h) Las fuerzas operacionales y líneas de autoridad. La Organización debe asegurar que sus objetivos y preocupaciones de las partes interesadas externas sean consideradas cuando se desarrollen los criterios de la gestión de las operaciones de seguridad.	SI	SI	
4.1.4	**4.1.4 MAPEO Y ANÁLISIS DE LA CADENA DE SUMINISTRO Y LOS SUBCONTRATISTAS**			
	La organización **debe** identificar y documentar sus aguas arriba y sus aguas abajo en la cadena de suministro, particularmente en el uso de subcontratistas que puedan tener un impacto o riesgo, así como el potencial de causar eventos indeseables o disruptivos. **El manejo de los riesgos en la cadena de suministro debe incluirse en el programa general de gestión de las operaciones de seguridad en aquellos lugares en los que se han identificado posibles eventos disruptivos o indeseables.** La organización debe definir y documentar el nivel en su cadena de suministro	SI	SI	

	y sus subcontratistas para ser incluidos en su programa de gestión de operaciones de seguridad			
4.1.5	**4.1.5 DEFINICIÓN DE LOS CRITERIOS DEL RIESGO**			
	La organización **debe** definir y documentar criterios para evaluar la importancia del riesgo. Los criterios del riesgo deben reflejar los valores de la organización, sus objetivos y recursos. A la hora de definir los criterios, la organización **debe** considerar: a) Las actividades críticas, las funciones, servicios, productos y relaciones con las partes interesadas. b) El entorno y la incertidumbre operacionales en entornos con gobiernos debilitados o con ejercicios débiles de la ley. c) El impacto potencial relacionado con un evento disruptivo o indeseable. d) Los requisitos legales y regulatorios, así como otros requisitos (por ejemplo, obligaciones contractuales y compromisos con los derechos humanos) a los que la organización se suscribe. e) La política general de manejo del riesgo de la compañía. f) La naturaleza y tipos de las amenazas y sus consecuencias, que puedan ocurrir a sus bienes, negocios u operaciones y revisados apropiadamente. g) Cómo la probabilidad, sus consecuencias, así como el nivel del riesgo serán definidos. h) Las necesidades y el impacto en las partes interesadas – particularmente la vida, la seguridad y los derechos humanos. i) Riesgo reputacional y requerido. j) Tolerancia al nivel de riesgo o la aversión al riesgo de los clientes y la organización. k) Cómo la combinación y secuencia de múltiples riesgos pueden ser tomados en cuenta. Mientras los criterios del riesgo son establecidos, el principio del proceso de evaluación del riesgo es dinámicos y deben ser continuamente monitoreados y revisados apropiadamente.	SI	SI	
4.2	**4.2 COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES ASOCIADAS**			
	La organización **debe** determinar las cuestiones internas y externas que sean relevantes para su propósito y que afecten su habilidad para lograr los resultados esperados de sus Sistemas de Gestión de Operaciones en Seguridad (SGOS (SOMS en inglés)). El diseño e implementación de un marco para los sistemas de gestión está basado en el entendimiento de una organización de su contexto operacional interno y externo. Así, pues, una organización debe definir y documentar su contexto interno y externo, incluyendo su cadena de suministro y subcontratistas. Estos factores deben ser tomados en cuenta cuando se establezca, implemente y mantenga el SGOS de la organización y se asignen sus prioridades. La organización debe evaluar los factores internos y externos que puedan influenciar la manera en la que la organización gestiona el riesgo.	SI	SI	
4.3	**4.3 DETERMINACIÓN DEL ALCANCE DEL SISTEMA DE GESTIÓN DE LAS OPERACIONES DE SEGURIDAD**			

	La organización **debe** determinar los límites y la aplicabilidad del SGOS para establecer su alcance (por ejemplo, la organización completa, o una o más de sus partes o funciones constitutivas). La organización debe definir el alcance del SGOS en términos de la idoneidad frente a su tamaño, naturaleza y complejidad desde una perspectiva del mejoramiento continuo. A la hora de determinar este alcance, la organización debe considerar: – Los objetivos de la organización, las cuestiones externas e internas referidas en 4.1.2. – Los requisitos referidos en 4.1.3. – Los factores de riesgos que puedan afectar adversamente las operaciones y actividades de la organización dentro del contexto de las probabilidades y sus consecuencias. El alcance debe ser accesible como información documentada. Las organizaciones deben identificar todos los elementos de sus operaciones donde los SGOS apliquen, así como las exclusiones, si aplica. La organización debe definir el alcance de manera consistente con el respeto a las obligaciones aplicables y a las leyes internacionales, nacionales, locales y de derechos humanos, mientras protege y preserva la integridad de la organización, incluyendo su relación con las partes interesadas. Una Declaración de Aplicación deben definir las cláusulas relevantes del Anexo A que apliquen al alcance de la organización, las obligaciones legales y contractuales junto con el ambiente de operaciones basado en la evaluación del riesgo y el análisis de impacto a los derechos humanos. (véase 6.1). Donde el análisis del riesgo y el análisis de los derechos humanos identifiquen cláusulas específicas del Anexo A como relevantes y aplicables al alcance de la organización, a las obligaciones legales y contractuales y al ambiente operacional, estás deben ser dirigidas e implementadas por la organización. Las exclusiones específicas y sus justificaciones deben ser documentadas.	SI	SI	
4.4	**4.4 SISTEMA DE GESTIÓN DE OPERACIONES DE SEGURIDAD**			
	La organización **debe** establecer, implementar, mantener y mejorar continuamente un SGOS, incluyendo los procesos necesarios y sus interacciones, en concordancia con los requisitos de esta Norma Internacional. La organización **debe** establecer resultados deseados documentados para su sistema de gestión y mejorar continuamente su efectividad en concordancia con los requisitos propuestos en esta Norma Internacional. El SGOS deben implementar los principios y compromisos de la ICoC. Cuando la organización contrate, subcontrate o tercerice algún proceso o actividad que caiga dentro del alcance de la aplicación de esta Norma Internacional, la organización **debe** asegurar que el control de dicha subcontratación o proceso de tercerización será identificado y gestionado dentro del SGOS.	SI	SI	NO se terceriza a ningun servicio de vigilancia.
5. LIDERAZGO				
5.1	**5.1 LIDERAZGO Y COMPROMISO**			
5.1.1	**5.1.1 GENERAL**			
	La alta dirección debe demostrar liderazgo y compromiso al respecto del desarrollo y la implementación del SGOS y debe, también, continuamente mejorar su efectividad al: ● Asegurar que las políticas y los objetivos de las operaciones de seguridad están establecidas y son compatibles con las decisiones estratégicas de la organización. ● Asegurar la integración del SGOS a los requisitos de los propósitos de negocio de la Organización. ● Asegurar que los recursos precisados por el SGOS estén disponibles para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGOS. ● Comunicar la importancia de un sistema de gestión en operaciones de seguridad efectivo y en conformidad con el SGOS y sus requisitos y responsabilidades legales. ● Asegurar que el SGOS logre su resultado(s) esperado(s). ● Direccionando y apoyando a personas que contribuyan a la efectividad del SGOS. ● Apoyando otros roles administrativos para que demuestren su liderazgo mientras que lo aplican a sus áreas de responsabilidad. ● Conducir a intervalos planificados; revisiones gerenciales del SGOS. NOTA: Las referencias al 'negocio' en esta Norma Internacional pueden interpretarse de manera amplia como aquellas actividades que son	SI	SI	

	centrales para los propósitos de la organización y su existencia. La alta dirección debe proveer evidencia de un liderazgo activo para el SGOS al supervisar su establecimiento y su implementación, así como al motivar a los individuos para integrar operaciones de seguridad consistentes con el respeto por los derechos humanos como parte integral de la misión de la organización y su cultura.			
5.1.2	**5.1.2 SISTEMA DE GESTIÓN DE OPERACIONES DE SEGURIDAD**			
	La alta gerencia debe desarrollar, documentar y publicar una **Declaración de Conformidad que indique el compromiso de la organización,** así como su conformidad, con su responsabilidad inherente hacia los derechos humanos tal y como se refleja en la provisión de su SGOS y los siguientes documentos: ● Código Internacional de Conducta para Proveedores de Servicios de Seguridad Privada (ICoC). ● Documento de Montreux Sobre las obligaciones jurídicas internacionales pertinentes y las buenas prácticas de los Estados en lo que respecta a las operaciones de las empresas militares y de seguridad privadas durante los conflictos armados. ● Principios Rectores sobre las empresas y los derechos humanos; Marco de Implementación “Proteger, respetar y remediar” de las Naciones Unidas 2011. ● Cualquier otro compromiso internacional que reconozca los derechos humanos (por ejemplo, Principios voluntarios en seguridad y derechos humanos). La Declaración de Conformidad también estipula a las expectativas de sus partes interesadas en derechos humanos de la organización como directamente ligada a sus operaciones. La Declaración de Conformidad debe estar: a) Documentada, implementada y mantenida. b) Públicamente disponible y comunicada interna y externamente a todas las partes interesadas. c) Visiblemente respaldada por la alta dirección.	SI	SI	
5.2	**5.2 POLÍTICA**			
	La alta dirección debe establecer una política de operaciones en seguridad que: ● Sea apropiada para los propósitos de la organización. ● Provea de un marco para la estipulación de objetivos operativos. ● Incluya un compromiso para satisfacer las leyes aplicables y otro tipo de requisitos, incluyendo los compromisos voluntarios a los que la organización se suscriba. ● Incluya un compromiso con la mejora continua del SGOS. ● Provea un compromiso con los derechos humanos. ● Provea un compromiso para evitar, prevenir y reducir la probabilidad de ocurrencia de eventos disruptivos o indeseables. La política de operaciones de seguridad debe: ● Estar disponible como información documentada. ● Ser comunicada dentro de la organización. ● Ser comunicada apropiadamente a todas las personas que trabajan para el bien de la organización. ● Estar disponible a las partes interesadas de manera apropiada. ● Ser visiblemente respaldada por la alta dirección. ● Ser revisada en intervalos planificados y cada vez que ocurran cambios significativos.	SI	SI	
5.3	**5.3 ROLES, RESPONSABILIDAD Y AUTORIDADES**			

	La alta dirección debe asegurar que las responsabilidades y la autoridad para roles relevantes sean asignadas y comunicadas dentro de la organización. La alta dirección debe asignar a uno más individuos de la organización quien -fuera de otras responsabilidades- deben tener competencias definidas, así como roles, responsabilidades y autoridad definida para: a) Asegurar que el SGOS se ajuste a los requisitos de esta Norma Internacional. b) Reportar el desempeño del SGOS a la alta dirección. c) Asegurar que el SGOS esté establecido, bien comunicado, implementado, y mantenido en concordancia con los requisitos de esta Norma Internacional. d) Identificar, monitorear y gestionar las necesidades y expectativas de las partes interesadas delineadas en 4.2. e) Asegurar que los recursos necesarios estén disponibles. f) Promover la toma de conciencia sobre los requisitos del SGOS en la organización. g) Reportar el desempeño del SGOS a la alta dirección para su evaluación y la constitución de la base para el mejoramiento continuo. La alta dirección debe asegurar que aquellos responsables de la implementación y el mantenimiento de este SGOS tengan la autoridad necesaria, así como la competencia, para hacerlo idóneamente y ser responsables por la operación.	SI	SI	
6. PLANIFICACIÓN				
6.1	**6.1 ACCIONES PARA EVALUAR EL RIESGO Y LAS OPORTUNIDADES**			
6.1.1	**6.1.1 GENERAL**			
	A la hora de planear un SGOS, la organización debe considerar las cuestiones referidas en 4.1.2 y los requisitos referidos en 4.1.3 y determinar el riesgo y las oportunidades que deben ser atendidos para: ● Asegurar que el SGOS puede lograr los resultados esperados. ● Prevenir o reducir los efectos indeseables. ● Lograr el mejoramiento continuo. La organización debe establecer, implementar y mantener un proceso de atención al riesgo formal y documentado para sus operaciones en seguridad, incluyendo sus socios en la cadena de suministro y sus actividades de subcontratación. El proceso de atención al riesgo debe incluir: ● Identificación del riesgo- identificar y evaluar las amenazas, vulnerabilidades, consecuencias y riesgos contra los derechos humanos para identificar riesgos estratégicos, tácticos y operacionales debido a eventos, intencionales, no-intencionales o naturales que tengan consecuencias potenciales, directas o indirectas, para las actividades, bienes, operaciones, funciones y partes interesadas de la organización, así como su habilidad para acatar los derechos humanos; ● Análisis del riesgo - sistemáticamente analizar el riesgo (probabilidades y análisis de consecuencias, incluyendo el análisis de riesgo en derechos humanos) para determinar aquellos riesgos que tienen un impacto significativo en actividades, funciones, servicios, productos, cadenas de suministro, subcontratistas, relaciones con partes interesadas, poblaciones locales y el medio-ambiente. ● Evaluación del riesgo - sistemáticamente evaluar y priorizar controles del riesgo, así como amenazas y sus costos relacionados para determinar cómo llevar el riesgo a un nivel aceptable y consistente con los criterios del riesgo. La organización debe: a) Documentar y mantener esta información actualizada y segura. b) Revisar periódicamente si el alcance, la política, el riesgo, los criterios y la atención del riesgo de las operaciones de seguridad aún son apropiadas desde el punto de vista del contexto interno y externo de la organización. c) Re-evaluar el riesgo desde el contexto de cambios internos de la organización o cambios hechos al medio ambiente, los procedimientos, funciones, servicios, sociedades y cadenas de suministro en los que se desarrolla la organización. d) Evaluar los beneficios y costos directos e indirectos de las opciones para	SI	SI	

	gestionar el riesgo y mejorar la confiabilidad y la resiliencia. e) Evaluar la eficacia de las opciones de tratamiento del riesgo vigentes tras incidentes y después de ejercicios. f) Asegurar que los riesgos priorizados y sus impactos sean tomados en cuenta a la hora de establecer, implementar y operar un SGOS. g) Monitorear y evaluar la eficacia de los controles y tratamientos para el riesgo. La atención del riesgo debe identificar actividades, operaciones y procesos que precisen ser gestionados, los resultados deben incluir: a) Un registro priorizado del riesgo que identifique tratamientos para gestionar el riesgo. b) Justificaciones para la aceptación del riesgo. c) Identificación de puntos de control críticos (CCP en inglés). d) requisitos para el control de subcontratistas y terceros. De manera consistente con sus operaciones de seguridad, la organización debe establecer un proceso para monitorear, valorar, evaluar y responder al cambio en el entorno de los riesgos. La organización debe planear: a) Acciones para evaluar el riesgo y sus oportunidades. b) Cómo: ○ integrar e implementar las acciones dentro de sus procesos de SGOS; ○ evaluar la efectividad de estas acciones.			
6.1.2	**6.1.2 REQUISITOS LEGALES Y DE OTRA ÍNDOLE**			
	La organización debe asegurar que los requisitos legales aplicables y relevantes sean considerados e incorporados a la hora de establecer, implementar y mantener su SGOS. La organización debe: a) Identificar los requisitos legales, regulatorios, contractuales, de licencias y los compromisos relacionados con el negocio y las operaciones de seguridad; b) Identificar las responsabilidades en derechos humanos relevantes para el negocio y sus operaciones de seguridad y aquellos requeridos por la ley; c) Determinar cómo aplican estos requisitos a sus operaciones y a las de aquellos subcontratistas o socios dentro del alcance de esta Norma Internacional. La organización debe documentar esta información y mantenerla actualizada. Deberá comunicar información legal relevante y otros requisitos a aquellas personas que trabajan para ella, incluidos terceros que sean de relevancia y subcontratistas. Las organizaciones y sus clientes tienen una responsabilidad ética y legal para con estas obligaciones.	SI	SI	
6.1.3	**6.1.3 CONSULTORÍA Y COMUNICACIÓN DEL RIESGO INTERNO Y EXTERNO**			
	La organización debe establecer, implementar y mantener un proceso de comunicación y consultoría formal y documentado con las partes interesadas internas y externas en el proceso de atención al riesgo para asegurar que: a) Los objetivos operacionales y los intereses del cliente (incluidas las personas, organizaciones, comunidades y/o actividades protegidas) sean entendidos. b) Los riesgos sean adecuadamente identificados y comunicados. c) Los intereses de las partes interesadas internas y externas sean entendidos. d) Los riesgos y sus tratamientos sean comunicados a las partes interesadas. e) Que las dependencias y enlaces con subcontratistas y dentro de la cadena de suministro sean entendidos. f) Los procesos de atención al riesgo en las operaciones de seguridad se comuniquen con otras instancias de la administración. g) La atención del riesgo sea conducida apropiadamente dentro del contexto interno y externo y a partir de parámetros relevantes para la organización, sus subcontratistas y la cadena de suministro.	SI	SI	

6.2	**6.2 OBJETIVOS DE LAS OPERACIONES DE SEGURIDAD Y PLANEACIÓN PARA LOGRARLOS**			
6.2.1	**6.2.1 GENERAL**			
	La organización debe establecer objetivos para las operaciones de seguridad en niveles y con funcionarios relevantes. Los objetivos de las operaciones de seguridad deben: a) Ser consistentes con las políticas de operaciones de seguridad.b) Ser medibles (si es posible). c) Tener en cuenta requisitos aplicables. d) Ser monitoreados.e) Ser comunicados.f) Ser actualizados apropiadamente. A la hora de planear cómo lograr sus objetivos en seguridad, la organización debe determinar: ● Qué será hecho.● Qué recursos se necesitarán.● Quién será responsable. ● Cuándo será completado. ● Cómo serán evaluados los resultados. La organización debe establecer, implementar y mantener objetivos y metas documentados para gestionar el riesgo con el fin de anticipar, evitar, prevenir, disuadir, mitigar, responder y recuperarse de eventos indeseables o disruptivos. Los objetivos y metas documentados deben establecer expectativas internas y externas para la organización, sus subcontratistas y partes de la cadena de suministro que son críticas para el cumplimiento de la misión, entrega de los servicios y productos y operaciones funcionales. Los objetivos deben derivarse desde, y de manera consistente con, la política de operaciones de seguridad y la atención al riesgo, incluyendo los compromisos con: a) La reducción de riesgos a probabilidades y consecuencias mínimas. b) El respeto a las leyes internacionales, nacionales, locales y de derechos humanos; c) Requisitos financieros y operacionales de la organización (incluyendo los subcontratistas y los compromisos en la cadena de suministro). d) El mejoramiento continuo. A la hora de establecer y revisar los objetivos y metas, una organización debe considerar sus requisitos financieros, operacionales y de negocio, los requisitos legales, regulatorios y de otra índole, su impacto sobre los derechos humanos, sus riesgos significativos, sus opciones tecnológicas y los puntos de vista de sus partes interesadas. Las metas asociadas con los indicadores clave de desempeño deben ser medidos de manera cuantitativa o cualitativa. Las metas deben derivarse de manera consistente de los objetivos de las operaciones de seguridad y deben ser: a) Detalladas de manera apropiada. b) Conmensuradas con la gestión del riesgo. c) Específicas, medibles, logrables, relevantes y planificadas (si es posible). d) Comunicadas a todos los empleados y terceros pertinentes, incluyendo a los subcontratistas y a la cadena de suministro con el fin de que estas personas tomen conciencia de sus obligaciones individuales. e) Revisadas periódicamente para asegurar que mantengan su relevancia y que sean consistentes con los objetivos de las operaciones de seguridad y que sean modificadas de acuerdo a ellos.	SI	SI	
6.2.2	**6.2.2 LOGRAR LAS OPERACIONES DE SEGURIDAD Y OBJ. DEL TRAT. DE RIESGO**			

	La organización debe establecer, implementar y mantener programas para lograr sus objetivos para las operaciones de seguridad y el tratamiento del riesgo. Los programas deben estar optimizados y priorizados con el fin de controlar y tratar los riesgos asociados con sus operaciones, subcontratistas y su cadena de suministro. La organización debe establecer, implementar y mantener de manera formal y documentada el proceso de tratamiento del riesgo, que considera: a) Remover la fuente del riesgo, donde sea posible. b) Remover o reducir la probabilidad de un evento y sus consecuencias. c) Remover, reducir o mitigar las consecuencias dañinas. d) Compartir el riesgo con otras partes, incluyendo los seguros contra el riesgo. e) Expandir el riesgo entre bienes y funciones. f) Aceptar el riesgo o perseguir oportunidades de manera informada. g) Evitar o paralizar temporalmente las actividades que originan el riesgo. La alta dirección debe: a) evaluar los costos y beneficios de remover, reducir o mantener el riesgo. b) evaluar los programas de operaciones de seguridad para determinar si dichas medidas han introducido nuevos riesgos. c) revisar periódicamente el tratamiento del riesgo para reflejar el ambiente externo, incluyendo los requisitos legales, las regulaciones y requisitos de otra índole, así como las políticas de la organización, las instalaciones los sistemas de manejo de la información, las actividades, las funciones, los productos, los servicios y la cadena de suministro.	SI	SI	
7. SOPORTE				
7.1	**7.1 RECURSOS**			
7.1.1	**7.1.1 GENERAL**			
	La organización debe determinar y proveer los recursos necesarios para establecer, implementar, mantener y mejorar continuamente el SGOS. La organización debe considerar: a) Los recursos internos existentes, posiblemente adicionales, capacidades y limitaciones. b) Qué bienes y servicios deben provenir de fuentes externas. Los recursos disponibles incluyen toda la información relevante, las herramientas de gestión y administración, los recursos humanos (incluyendo a aquellas personas con experiencia relevante y conocimientos y habilidades de equipo técnico, especializado y de soporte logístico, ya sea interno o contratado externamente).	SI	SI	
7.1.2	**7.1.2 REQUISITOS ESTRUCTURALES**			
7.1.2.1	**7.1.2.1 General**			
	La organización debe ser una entidad legal o parte de una entidad definida legalmente. Deberá tener una estructura administrativa claramente definida que muestre control y responsabilidad en cada nivel de la organización (incluyendo a los subsidiarios dentro del alcance).	SI	SI	
7.1.2.2	**7.1.2.2 Estructura organizacional**			
	Una estructura administrativa claramente definida debe tener roles, responsabilidades, y autoridad para sus operaciones y servicios. La organización debe: a) Documentar su estructura organizacional, mostrando los deberes, responsabilidades y autoridad de la administración. b) Definir y documentar si la organización es definida como parte de una organización legal y la relación con otras partes de la misma entidad legal. c) Definir cualquier sociedad o acuerdos de sociedad dentro del alcance del SGOS.	SI	SI	
7.1.2.3	**7.1.2.3 Seguro**			
	La organización debe demostrar que tiene seguros para cubrir el riesgo y las deudas asociadas que surjan de las operaciones y las acciones consistentes con su atención del riesgo. Cuando se tercerice o se subcontraten servicios, operaciones o funciones, la organización debe asegurar el cubrimiento de seguros para los servicios subcontratados de manera apropiada.	SI	SI	
7.1.2.4	**7.1.2.4 Tercerización y subcontratación**			

	La organización debe tener un proceso claro y definido para la subcontratación y los procesos, funciones y actividades de tercerización. La organización debe establecer, documentar, comunicar y monitorear el cumplimiento con los términos de referencia específicos y los códigos de conducta para sus subcontratistas y terceros aliados con respecto a las operaciones de seguridad y el respeto por los derechos humanos. La organización debe tener un acuerdo documentado en donde recoja los compromisos con subcontratados y tercerizados, incluyendo: a) Compromiso por parte de los subcontratistas para atender las mismas obligaciones y compromisos legales, éticos y de derechos humanos que la compañía y de la manera descrita en esta Norma Internacional. b) Procesos para el reporte de riesgos, así como como la ocurrencia y las respuestas a eventos disruptivos o indeseables. c) Acuerdos de confiabilidad y ante conflictos de interés. d) Definición clara y documentada de los servicios a proveer. e) Dirigir y controlar los alcances y límites. f) Definición de la relación de apoyo entre el contratista y el subcontratista. g) Conformidad con las provisiones aplicables de esta Norma Internacional.	SI	SI	
7.1.2.5	**7.1.2.5 Procedimientos financieros y administrativos**			
	La organización debe desarrollar procedimientos y controles administrativos y financieros para apoyar la provisión de gestiones de la seguridad y el riesgo en todas las operaciones planificadas en anticipación y en respuesta cualquier evento disruptivo o indeseable. Los procedimientos deben ser: a) Establecidos para asegurar que las decisiones fiscales puedan ser ágiles. b) En concordancia con los niveles de autoridad y las funciones establecidos, así como los principios contables. c) Establecidos en común acuerdo y coordinación con el cliente.	SI	SI	
7.2	**7.2 COMPETENCIA**			
7.2.1	**7.2.1 GENERAL**			
	La organización debe: ● Determinar la competencia necesaria de una persona que realice trabajos bajo su supervisión en cuestiones que afecten el desarrollo de las operaciones de seguridad. ● Asegurar que estas personas son competentes desde el punto de vista de una adecuada educación, entrenamiento o experiencia. ● Donde aplique, tomar acciones para adquirir la competencia necesaria y evaluar la efectividad de las acciones tomadas.● Mantener la información documentada pertinente como evidencia de la competencia.	SI	SI	
7.2.2	**7.2.2 IDENTIFICACIÓN DE LA COMPETENCIA**			
	La organización debe identificar competencias, el nivel de competencia y las necesidades de entrenamiento asociadas con sus operaciones de seguridad, particularmente el desempeño de las funciones de cada individuo de manera consistente con las obligaciones legales y contractuales, así como con el respeto a los derechos humanos. La organización debe establecer, implementar y mantener procedimientos para asegurar que las personas que desempeñan labores para su beneficio demuestren un nivel apropiado de competencia en cada una de las áreas siguientes: a) Desempeño de sus funciones en seguridad. b) Gestión del riesgo. c) Gestión de los riesgos identificados en la evaluación del riesgo y potenciales impactos sobre los derechos humanos en el desempeño de su trabajo. d) Las leyes nacionales e internacionales aplicables, incluyendo las criminales y humanitarias que incluyen, pero no se limitan, a: o Prohibición de la tortura u otro tipo de comportamientos violentos degradantes, crueles e inhumanos. o Prohibición y concienciación sobre la explotación sexual, abuso o violencia motivada o Por el género. o Reconocimiento y prevención de la esclavitud y el tráfico humano. o Medidas contra el soborno, la corrupción y crímenes similares. e) La cultura, incluyendo las costumbres y religión del entorno de operaciones. f) Procedimientos para reducir la probabilidad y/o las consecuencias de eventos disruptivos o indeseables. incluyendo los procesos de respuesta y mitigación para reportar y responder ante estos eventos. g) Procedimientos de reporte y documentación de incidentes. h) Procedimientos de salubridad, seguridad y primeros auxilios. i) Cualificación	SI	SI	

	y aptitud para las operaciones mecánicas, el manejo de armas y contra incendios, todo con las armas apropiadas y especificadas por la organización para partes específicas de sus labores relacionadas con la seguridad. j) Limitaciones al uso de la fuerza relacionado con sus operaciones de seguridad. k) Protocolos, medios y procedimientos de comunicación. l) Procedimientos para quejas internas y de partes interesadas.			
7.2.3	**7.2.3 ENTRENAMIENTO Y EVALUACIÓN DE COMPETENCIAS**			
	La organización debe proveer entrenamiento basado en competencias y establecer los medios para medir el grado de eficiencia o los niveles de competencia. Las personas que trabajen para la organización debe estar entrenadas para demostrar el nivel de competencia y eficiencia requerido. La organización debe: a) Establecer mediciones basadas en competencias para sus programas de entrenamiento.b) Proveer entrenamientos para inculcar y comprender que el respeto hacia los derechos humanos es parte esencial de los valores centrales de la organización. c) Proveer espacios de educación y evaluación constantes para entrenamientos físicos, mecánicos y contra incendios para todo el personal autorizado para portar armas letales, no letales o de letalidad reducida en el ejercicio de sus funciones. d) Proveer de entrenamiento constante para el uso de armas y de la fuerza según lo requiera la ley o los requisitos contractuales, e incluso con mayor frecuencia para mantener el nivel de competencia identificado por la organización. e) Identificar otras competencias que requieran de entrenamientos periódicos para mantener el nivel de desempeño requerido o para incorporar nuevos requisitos. f) Proveer entrenamientos sobre la importancia del cumplimiento de las políticas y procedimientos de SGOS, así como de las consecuencias de distanciarse de los SGOS y las operaciones de seguridad.	SI	SI	
7.2.4	**7.2.4 DOCUMENTACIÓN**			
	La organización debe mantener registros de: a) Métricas y medidas de las competencias identificadas. b) Programas de entrenamiento. c) Registros asociados con los procesos de evaluación y entrenamiento de personas que trabajan para la organización.	SI	SI	
7.3	**7.3 CONCIENCIA**			
	La organización debe mantener registros de: a) Métricas y medidas de las competencias identificadas. b) Programas de entrenamiento. c) Registros asociados con los procesos de evaluación y entrenamiento de personas que trabajan para la organización.	SI	SI	
7.4	**7.4 COMUNICACIÓN**			
7.4.1	**7.4.1 GENERAL**			
	La organización debe determinar la necesidad de comunicaciones internas y externas relevantes para el SGOS, incluyendo: ● Qué comunicará; ● Cuándo comunicará; ● Con quién se comunicará; ● Cómo comunicar. La organización debe establecer, implementar y mantener procedimientos para: a) Comunicarse con las partes interesadas internas y externas. b) Recibir, documentar y responder a las comunicaciones de las partes interesadas internas y externas. c) Definir y asegurar la disponibilidad de los medios de comunicación durante situaciones atípicas o disruptivas. d) Probar regularmente los sistemas de comunicación para condiciones normales y anormales. Los procedimientos de comunicación deben considerar la naturaleza operacional y las restricciones legales a la hora de compartir información.	SI	SI	
7.4.2	**7.4.2 COMUNICACIONES OPERACIONALES**			

	La organización debe desarrollar procedimientos de comunicación para compartir información sobre las actividades del equipo de seguridad, su ubicación, estado operacional y logístico, información relevante sobre amenazas y reporte de incidentes para la dirección de la compañía, los clientes, otros equipos de seguridad privada y autoridades civiles y militares pertinentes. Esto debe incluir procedimientos para solicitar asistencia inmediata de autoridades civiles y militares, otros equipos de seguridad y apoyo médico y de emergencias. La organización debe asegurar que las comunicaciones verbales y escritas pueden ser recibidas y comprendidas por todos los niveles y operadores y que todos los niveles puedan responder en un lenguaje, o por medios, que puedan ser comprendidos por las partes interesadas internas y externas apropiadas. Los equipos de seguridad deben tener los medios para comunicar la información relacionada con la seguridad a la parte a la que protegen de una manera que la parte protegida pueda comprender.	SI	SI	
7.4.3	**7.4.3 COMUNICACIÓN DEL RIESGO**			
	La organización debe decidir, basado en la protección de la vida como la prioridad principal y en concierto con las partes interesadas, si comunicar externamente los riesgos significativos, su impacto y tratamiento a las partes interesadas y documentar esta decisión. Si se decide comunicar, la organización debe establecer e implementar métodos para esta comunicación, alerta o advertencia externa (incluyendo comunicaciones con los medios de comunicación masiva).	SI	SI	
7.4.4	**7.4.4 COMUNICACIÓN DE QUEJAS Y RECLAMOS**			
	Las quejas y los procedimientos de denuncias deben ser comunicados a las partes interesadas internas y externas. Los procedimientos deben estar públicamente disponibles en un sitio web para evitar los obstáculos causados por la lengua, el nivel educativo o el miedo a represalias, asimismo, deben contemplar la necesidad de la confidencialidad y la privacidad.	SI	SI	
7.4.5	**7.4.5 POLÍTICA DE COMUNICACIÓN DE DENUNCIAS**			
	La organización debe comunicar a las personas que trabajan para ella y que tengan razones para creer que una no conformidad con esta Norma Internacional ha ocurrido que tienen derecho a reportar esta no conformidad de manera anónima tanto internamente, a la organización, como externamente, a las autoridades competentes.	SI	SI	
7.5	**7.5 INFORMACIÓN DOCUMENTADA**			
7.5.1	**7.5.1 GENERAL**			
	El SGOS de la organización debe incluir: ● Información documentada, incluyendo registros, requeridos por esta Norma Internacional. ● Documentación de la política de operaciones de seguridad, una Declaración de Conformidad, objetivos y metas. ● Una descripción del alcance de este SGOS. ● Una Declaración de Aplicación. ● Una descripción de los elementos clave del SGOS y su interacción y referencia a documentos relacionados. ● Información documentada requerida para una efectiva implementación y operación del SGOS. ● Información documentada determinada por la organización como necesaria para la efectividad del SGOS.NOTA: El grado de información documentada para un SGOS puede diferir de una organización a otra debido a: ● El tamaño de la organización y el tipo de actividades, procesos, productos o servicios. ● La complejidad de sus procesos y sus interacciones. ● La competencia del personal.	SI	SI	
7.5.2	**7.5.2 CREACIÓN Y ACTUALIZACIÓN**			
7.5.2.1	**7.5.2.1 General**			

	A la hora de crear y actualizar la información documentada, la organización debe asegurar: ● Apropiada identificación y descripción (por ejemplo, de títulos, autores, fechas o número de referencia). ● Apropiados formatos (por ejemplo, idiomas, versiones de programas, gráficos) y medios (por ejemplo, papel o electrónico). ● Apropiadas revisiones y aprobaciones para la adecuación e idoneidad.	SI	SI	
7.5.2.2	**7.5.2.2 Registros**			
	La organización debe establecer y mantener registros para demostrar la conformidad con los requisitos de este SGOS. Los registros deben incluir, entre otros: a) Los registros requeridos por esta Norma Internacional. b) Licencias y permisos de operación. c) Examen de personal. d) Registros de entrenamiento. e) Registros de monitoreo de procesos. f) Registros de inspección, mantenimiento y calibración. g) Registros pertinente de subcontratación y proveedores. h) de reporte de incidentes. i) Registros de reportes de investigación de incidentes y sus disposiciones. j) Resultados de auditoría. k) Resultados de revisiones por la dirección. l) Decisiones sobre comunicaciones externas. m) Registro de los requisitos legales aplicables. n) Registro de riesgos significativos y sus impactos. o) De inventario de armas y recibos de adjudicación de armas. p) Registros de reuniones sobre sistemas de gestión. q) Información la seguridad, sobre el desempeño de las operaciones de seguridad y sobre derechos humanos. r) Comunicación con las partes interesadas.	SI	SI	
7.5.3	**7.5.3 CONTROL DE LA INFORMACIÓN DOCUMENTADA**			
	La información documentada requerida por el SGOS y esta Norma Internacional debe ser controlada para asegurar: a) Que esté disponible y en condiciones óptimas para su uso, cuando y donde sea necesitada) Que esté adecuadamente protegida (por ejemplo, de pérdida de confiabilidad, uso inapropiado o pérdida de su integridad).c) Para el control de la información documentada, la organización debe atender las siguientes actividades, cuando apliquen: • Distribución, acceso, recuperación y uso.• Almacenamiento y preservación, incluyendo la preservación de la legibilidad;• Control de cambios (o control de versiones). • Retención y disposición. La organización debe establecer, implementar y mantener procedimientos para: a) Aprobar documentos para adecuación antes de su emisión. b) Proteger la confidencialidad y sensibilidad de la información. c) Revisar, actualizar como sea necesario y re-aprobar documentos. d) Registrar las modificaciones a los documentos. e) Hacer que los documentos actualizados y aprobados estén disponibles para su consulta. f) Asegurar que los documentos permanecen legibles e identificables de manera inmediata. g) Asegurar que los documentos de origen externo se encuentren debidamente identificados y que su distribución sea controlada. h) Prevenir el uso no intencionado de documentación obsoleta. i) Asegurar la destrucción legal, apropiada y transparente de documentos obsoletos. La información documentada de origen externo que sea determinada por la organización como necesaria para la planeación y operación del SGOS debe ser identificada y controlada de manera apropiada. La organización debe establecer, implementar y mantener procedimientos para proteger la sensibilidad, confidencialidad e integridad de los registros, incluyendo el acceso a identificación, almacenamiento, recuperación, retención y eliminación de registros. Los registros deben ser mantenidos según como lo requiera el contrato y las leyes vigentes. Los registros de empleo y servicio deben ser mantenidos por mínimamente siete años o como lo requiera la ley vigente. Las organizaciones deben asegurar la integridad de los documentos al proveerles un respaldo seguro, accesible sólo para el personal autorizado y protegido de accesos, modificaciones sin autorización, eliminaciones, daños, deterioros o pérdidas.	SI	SI	Anexo 12. Procedimiento Control de Documentos y Registros V2
8. OPERACIÓN				

8.1	**8.1 PLANEACIÓN Y CONTROL DE OPERACIONES**			
8.1.1	**8.1.1 GENERAL**			
	La Organización como necesaria para la planeación y operación del SGOS debe ser identificada y controlada de manera apropiada.La organización debe establecer, implementar y mantener procedimientos para proteger la sensibilidad, confidencialidad e integridad de los registros, incluyendo el acceso a identificación, almacenamiento, recuperación, retención y eliminación de registros. Los registros deben ser mantenidos según como lo requiera el contrato y las leyes vigentes. Los registros de empleo y servicio deben ser mantenidos por mínimamente siete años o como lo requiera la ley vigente. Las organizaciones deben asegurar la integridad de los documentos al proveerles un respaldo seguro, accesible sólo para el personal autorizado y protegido de accesos, modificaciones sin autorización, eliminaciones, daños, deterioros o pérdidas. La organización debe planear, implementar y controlar los procesos necesarios para cumplir con los requisitos y para implementar las acciones descritas en 6.1 al:● Establecer criterios para los procesos. ● Implementar controles para los procesos en concordancia con los criterios. ● Mantener información documentada al grado de tener confianza en que los procesos se han llevado a cabo tal y como fueron planeados. La organización debe identificar las actividades que están asociadas con los riesgos significativos que fueron identificados y debe hacerlo de manera consistente con su política de gestión de operaciones de seguridad, su evaluación del riesgo, sus objetivos y metas; todo esto con el fin de asegurar que sean llevadas a cabo bajo condiciones específicas que le posibilitará: a) Cumplir los requisitos legales, incluyendo los permisos y licencias de operación. b) Cumplir la misión mientras se protege la reputación del cliente. e) Respetar los derechos de las comunidades locales. f) Implementar controles de gestión del riesgo para minimizar la probabilidad y las consecuencias de un evento disruptivo o indeseable. g) Lograr los objetivos y metas de las operaciones de seguridad. La organización debe establecer, implementar y mantener procedimientos documentados para controlar situaciones en las que su ausencia podría derivar en una desviación de la política del SGOS y sus objetivos y metas. La organización debe controlar la planificación de los cambios y evaluar las consecuencias de los cambios involuntarios, emprendiendo acciones para mitigar cualquier efecto adverso de la manera necesaria. La organización debe asegurarse que los procesos tercerizados estén controlados.	SI	SI	
8.1.2	**8.1.2 DESEMPEÑO DE LAS FUNCIONES RELACIONADAS CON LA SEGURIDAD**			
	La organización debe establecer, implementar y mantener procedimientos para apoyar la protección de las personas, los bienes tangibles e intangibles, y otras funciones relacionadas con la seguridad, incluyendo, pero no estando limitadas a: a) El manejo de riesgos identificados en la evaluación del riesgo. b) Funciones específicas requeridas por el cliente o por las autoridades competentes. c) Otras tareas específicas del contexto y las funciones.	SI	SI	
8.1.3	**8.1.3 RESPETO POR LOS DERECHOS HUMANOS**			
	La organización debe establecer, implementar y mantener procedimientos para tratar a todas las personas con dignidad y respeto hacia sus derechos humanos y para reportar cualquier tipo de no-conformidad. La organización debe desarrollar y comunicar a todas las personas trabajando para ella procedimientos para una conducta consistente con los principios del respeto a los derechos humanos; así como cualquier regulación contractual que aplique a las operaciones de seguridad de la organización.	SI	SI	
8.1.4	**8.1.4 PREVENCIÓN Y GESTIÓN DE EVENTOS INDESEABLES O DISRUPTIVOS**			

	La organización prevendrá, mitigará y responderá ante eventos indeseables o disruptivos teniendo en consideración la siguiente: a) El desempeño de las funciones de seguridad. b) La salvaguarda de la vida y lo promoción de la seguridad del personal y de las partes interesadas internas y externas. c) Respeto por la vida humana y su dignidad. d) Anticipación y prevención de la escalación de eventos disruptivos. e) Minimización del desorden ocasionados a las operaciones y los servicios. f) Minimización del potencial de cualquier impacto adverso sobre la comunidad local. g) Notificación a las autoridades pertinentes. h) Lecciones aprendidas y acciones preventivas y correctivas.	SI	SI	
8.2	**8.2 ESTABLECIMIENTO DE NORMAS**			
	La organización debe establecer, implementar y mantener un Código Ético con normas de comportamiento para todas las personas que trabajen para la organización, incluyendo a los empleados, subcontratistas y terceros asociados. El Código Ético debe estar documentado y debe establecer la importancia de la conducta profesional en las operaciones de seguridad y debe comunicar claramente el respeto por los derechos humanos y la dignidad de los seres humanos. El Código Ético deberá asegurar que todas las personas que trabajen en beneficio de la organización comprendan su responsabilidad para prevenir y reportar cualquier abuso sobre los derechos humanos. La organización debe comunicar y documentar su Código Ético a todas las personas que trabajen para ella, así como a sus clientes.	SI	SI	
8.3	**8.3 USO DE LA FUERZA**			
8.3.1	**8.3.1 GENERAL**			
	La organización debe establecer y documentar procedimientos para el uso de la fuerza para las personas que trabajen para ella. Donde sea posible, estos procedimientos deben ser gobernados por las leyes para el uso de la fuerza (RUF en inglés) publicadas por una autoridad legal competente para ser usadas en operaciones de seguridad consistentes con los requisitos de esta Norma Internacional. La organización debe establecer procedimientos para el uso de la fuerza para ser empleado por el personal de las operaciones de seguridad a manera de defensa personal, incluyendo la defensa de personas bajo la protección de la organización. Estos procedimientos pueden incluir: a) Autorización para el uso y el porte de armas para el personal. b) El uso de un espectro de la fuerza. c) El uso de fuerza no letal y de letalidad reducida. d) El uso de la fuerza letal. e) El uso de la fuerza en apoyo a las autoridades competentes (si aplica). f) Entrenamiento. La organización debe establecer y documentar procedimientos específicos al alcance de sus operaciones y a las condiciones del trabajo hecho en cada locación. Los procedimientos de uso de la fuerza de la organización deben ser consistentes con los requisitos y leyes contractuales y legales y deben ser concertados con cualquier otra entidad a la que el servicio de operaciones de seguridad privada le sea provisto.	SI	SI	
8.3.2	**8.3.2 AUTORIZACIÓN DE ARMAS**			

	La organización debe establecer y documentar procedimientos para autorizar a sus personas para estar armados en el desarrollo de las operaciones de seguridad. Las autorizaciones deben: a) Ser garantizadas únicamente a aquél personal que sea determinado como idóneo para la tarea a llevar a cabo y que han sido evaluados como apropiados para llevar las tareas a cabo a partir de sus antecedentes. b) Ser específicas para un tipo y modelo de armas y solo será adjudicada cuando el individuo ha sido cualificado en ese tipo y modelo en el marco de una norma que especifique procedimientos que sean apropiados para esa arma y para las labores esperadas. Todas las autorizaciones de armas deben estar por escrito y firmadas (ya sea digitalmente o con tinta) por oficiales que las autoricen antes de ser adjudicadas a un individuo. La organización debe mantener documentados los resultados de la cualificación individual por todo el tiempo que el individuo esté autorizado para estar armado.	SI	SI	
8.3.3	**8.3.3 ESPECTRO DEL USO DE LA FUERZA**			
	La organización **debe** establecer y documentar procedimientos que describan el espectro del uso de la fuerza, es decir, la aplicación de una cantidad de fuerza apropiada, razonable y necesaria para las operaciones de seguridad. Los elementos de este espectro deben contener: a) El uso de la ferza debe ser razonable en intensidad, duración y magnitud, basado en las circunstancias aplicables en el momento. b) Alertar a las personas y proveer oportunidad para abandonar o cesar las acciones amenazantes cuando la situación o las circunstancias lo permitan. c) La reducción (desescalada) de la fuerza aplicada si la situación y las circunstancias lo permiten. d) Controles de supervisión a la hora de iniciar, aumentar o reducir el uso de la fuerza y la mitación de esa autoridad. Los procedimientos para un espectro de la fuerza deben ser consistentes con el derecho legítimo de la defensa personal.	SI	SI	
8.3.4	**8.3.4 LETALIDAD REDUCIDA**			
	Los procedimientos de uso de la fuerza de la organización deben evaluar el uso de la letalidad reducida, es decir, aquel grado de fuerza cuya probabilidad de causar la muerte o heridas físicas serias es menor, así como los tipos de letalidad reducida autorizados y disponibles para la persona que conduce las operaciones de seguridad. La organización debe documentar los procedimientos para el uso de la letalidad reducida en concordancia con las leyes vigentes para la defensa personal, incluyendo, pero no limitado, a las siguientes circunstancias: a) Contra personas que asalten a otras personas o a uno mismo para prevenir heridas o cuando el asalto continúa tras el uso de las alternativas al uso de la fuerza. b) Contra personas que se resisten a una captura legal y cuando el uso de las alternativas al uso de la fuerza no ha sido suficiente. c) Para prevenir la pérdida o destrucción de propiedad bajo la protección de la organización.	SI	SI	
8.3.5	**8.3.5 FUERZA LETAL**			

	La fuerza letal sólo está justificada bajo condiciones de necesidad y puede ser usada solamente cuando los medios menores no pueden ser razonablemente puestos en práctica o han fallado. El procedimiento para el uso de la fuerza de la organización debe identificar las leyes vigentes de la defensa personal para cada una de sus operaciones de seguridad y debe atender al uso de la letalidad en relación con lo siguiente: a) El derecho inherente a la defensa personal. b) La defensa de otros. c) Defensa de la propiedad, incluyendo la propiedad inherentemente peligrosa o la infraestructura crítica que, de perderse o destruirse, crearía una amenaza inminente de muerte o de herida grave. La fuerza letal está justificada únicamente bajo condiciones de necesidad cuando hay una creencia razonable de que: a) Una persona o personas presentan una amenaza inminente de muerte o de herida grave para el individuo u otras personas cercanas a él. b) Es necesario prevenir un acto de robo o sabotaje de propiedad inherentemente peligrosa. c) Hay que prevenir el sabotaje o destrucción de infraestructura crítica, el daño a lo que la autoridad competente considere como una amenaza inminente de muerte o de herida grave.	SI	SI	
8.3.6	**8.3.6 USO DE LA FUERZA EN APOYO A LAS AUTORIDADES COMPETENTES**			
	Cuando se esté autorizado por un estado para apoyar las operaciones de las autoridades competentes, las organizaciones deben solicitar los Reglamentos para el Uso de la Fuerza (RUF en inglés) de la autoridades civiles o militares relevantes para la función. Cuando no haya RUF disponibles, los procedimientos para el uso de la fuerza deben regirse, adicionalmente, por estos elementos derivados de los Principios Básicos sobre el Empleo de la Fuerza y de Armas de Fuego por los Funcionarios Encargados de Hacer Cumplir la Ley de las Naciones Unidas: ● El uso intencional de las armas de fuego sólo será efectuado cuando sea estrictamente inevitable para la protección de la vida. ● El espectro del uso de la fuerza debe incluir identificación aural o visual del personal de la organización como autoridad competente, así como la clara advertencia de la posibilidad del uso de armas de fuego .	NA	NA	
8.3.7	**8.3.7 ENTRENAMIENTO PARA EL USO DE LA FUERZA**			
	Los procedimientos para el uso de la fuerza de la organización deben describir los requisitos iniciales y recurrentes para el entrenamiento. El personal de operaciones de seguridad autorizado para portar armas debe completar satisfactoriamente el entrenamiento que incluye familiarización con las armas (aula académica), cualificación con munición real y entrenamiento sobre el uso de la fuerza. Tal entrenamiento debe ser completado cada 12 meses o más frecuentemente dependiendo de los requisitos legales y contractuales o según como lo indique la evaluación del riesgo de la organización. Los registros de entrenamiento y de certificación de la competencia deben ser mantenidos por todo el tiempo que los individuos estén asociados a la organización, los siguientes elementos deben incluirse en la organización del entrenamiento para el uso de la fuerza: a) Leyes vigentes para la defensa personal en situaciones de seguridad particulares. b) Una revisión a las autorizaciones de la organización para usa armas y sus políticas de almacenamiento y porte. c) Una revisión de las diferencias entre el uso apropiado de la fuerza en operaciones de seguridad y las reglas para entablar combate de las fuerzas militares. d) Un examen de los compromisos que pueden resultar del uso de la fuerza y de las armas de fuego que resulte en la muerte y perjuicio por herida grave a una persona. e) Obediencia a las órdenes superiores debido a que la defensa no está permitida en circunstancias en las que no puede ser razonablemente determinado, que las instrucciones para el uso de la fuerza fueron manifiestamente ilegales. f) Aplicación del espectro del uso de la fuerza.	SI	SI	
8.4	**8.4 CAPTURA Y REQUISA**			

8.4.1	**8.4.1 CAPTURA DE PERSONAS**			
	Los procedimientos operacionales de la organización deben contemplar la aprehensión de personas presuntamente relacionadas con haber cometido un ataque contra personas o bienes relacionadas con la operación de seguridad. Los procedimientos deben describir el contexto legal bajo el que las personas pueden ser retenidas contra su voluntad, las limitaciones sobre el uso de la fuerza en esas capturas y los procedimientos de cuándo y a quién transferirá la organización la custodia de la persona o personas retenidas.	SI	SI	
8.4.2	**8.4.2 REQUISA**			
	Los procedimientos operacionales de la organización deben contemplar las circunstancias bajo las que un tercero puede ser requisado en busca de armas u otro tipo de contrabando. La requisa de personas en puntos claves de acceso debe describir los requisitos para tratar a estas personas en concordancia con la dignidad personal, las consideraciones culturales y los derechos humanos fundamentales.	SI	SI	
8.5	**8.5 OPERACIONES EN APOYO A LAS AUTORIDADES COMPETENTES**			
8.5.1	**8.5.1 APOYO A LAS AUTORIDADES COMPETENTES**			
	La organización debe desarrollar esas operaciones únicamente como lo dispongan las autoridades competentes o las autoridades militares a cargo según las leyes vigentes y relevantes. La organización debe desarrollar procedimientos adicionales para apoyar las operaciones de seguridad en apoyo a las autoridades competentes que incluyan: a) Uniformes y fachadas de vehículos según lo dispongan las autoridades competentes o las autoridades militares a cargo. b) Procedimientos documentados para el aseguramiento o disposición de la asistencia de ayuda médica a cualquier persona herida o afectada. c) Reporte oportuno de incidentes que causen heridas o la muerte por el uso de la fuerza y de armas de fuego en actividades del ejercicio de la ley ante las autoridades competentes, así como al personal supervisor de la organización. d) De saberse, la notificación a las autoridades competentes que se apoyan los nombres de las personas heridas o de cualquier manera afectadas por las actividades de ejercicio de la ley de la organización.	NA	NA	
8.5.2	**8.5.2 OPERACIONES DE DETENCIÓN**			
	Vigilar, transportar o interrogar personas privadas de su libertad, detenidas o encarceladas por las autoridades competentes está fuera del alcance de esta Norma Internacional.	NA	NA	
8.6	**8.6 RECURSOS, ROLES, RESPONSABILIDADES Y AUTORIDAD**			
8.6.1	**8.6.1 GENERAL**			
	La organización debe mantener personal suficiente (empleados, contratistas o subcontratistas) con el nivel apropiado de competencia para cumplir con sus obligaciones contractuales. El personal debe ser provisto de una paga adecuada y de acuerdos de remuneración, incluido el aseguramiento, de manera apropiada con sus responsabilidades y su contexto. La organización debe proteger la confidencialidad de esta información de manera apropiada y proveerá el personal de documentación en su lengua y comprensible para todas las partes. La organización debe mantener información documentada para todo el personal: a) Según lo requerido por las obligaciones legales y contractuales. b) Para mantener contacto son los individuos y su familia inmediata. c) Para asistir la recuperación del personal en caso de un incidente. d) Necesaria para notificar a la familia del individuo en caso de herida o muerte.	SI	SI	
8.6.2	**8.6.2 PERSONAL**			
8.6.2.2	**8.6.2.2 Selección, examen de antecedentes y elección de personal**			

	La organización debe establecer, documentar, implementar y mantener procedimientos para examen de antecedentes e investigación de todas las personas que trabajan para ella en todas las posiciones, con el fin de asegurar que sean aptos para las tareas que conducirán (por ejemplo, subcontratistas, terceros aliados y subsidiarios). Donde sea posible y de manera consistente con las leyes de protección de datos, el examen debe incluir:a) Consistencia con los requisitos legales y contractuales. b) Verificaciones de identidad, mayoría de edad e historia personal. c) Examen del historial académico y profesional. d) Revisión del estado militar, policial y del servicio de seguridad. e) Revisión de posibles antecedentes criminales. f) Revisar reportes de violaciones contra los derechos humanos. g) Examen de abuso de sustancias. h) Examen físico y mental para verificar la idoneidad ante las actividades asignadas i) Evaluación de la idoneidad para portar armas como parte de sus responsabilidades. Los requisitos de mayoría de edad pueden ser impuestos por las leyes locales, por las leyes aplicables al domicilio legal de la organización o pueden ser propuestos por el cliente. En ningún caso ninguna persona menor de 18 años de edad será empleado en tareas que requieran el porte y uso de armas de fuego o cualquier otra arma. La investigación debe incluir un juramento por parte del personal de que nada en su conducta pasada o actual contradirá el Código Ético de la organización, la Declaración de Conformidad o la adherencia a las cláusulas de esta Norma Internacional. El personal debe notificar a la organización cualquier cambio en las circunstancias que puedan llevar a un cambio en el estado de su examen. El examen de antecedentes involucra la revelación de información de alta sensibilidad; por ello, la organización debe desarrollar procedimientos para asegurar de manera discreta, estricta y apropiada la confidencialidad de la información, tanto interna como externamente. Los registros deben ser mantenidos de manera consistente por estatutos con limitaciones relevantes. La selección del personal cualificado debe basarse en competencias definidas, incluyendo el conocimiento, las habilidades, las idoneidades y atributos. El examen y las medidas para la selección deben ser consistentes con los requisitos aplicables y leyes vigentes, así como de referencias normativas consistentes como esta Norma Internacional.	SI	SI	
8.6.2.3	**8.6.2.3 Selección, examen de antecedentes e investigación de subcontratistas**			
	La organización debe establecer procesos definidos para la selección, examen de antecedentes y evaluación de subcontratistas. La organización es responsable por el trabajo de los subcontratistas y es responsable, según lo disponga la ley, por la conducta de los subcontratistas. La organización debe: a) Asegurar acuerdos contractuales escritos apropiados con los subcontratistas. b) Asesorar al cliente sobre el compromiso por escrito y, cuando sea apropiado, obtener aprobación del cliente. c) Mantener un registro de todos los subcontratistas que usa. d) Comunicar las responsabilidades de esta Norma Internacional a sus subcontratistas. e) Mantener un registro de evidencia de conformidad o desviaciones de esta Norma Internacional para el trabajo subcontratado.	SI	SI	
8.6.3	**8.6.3 OBTENCIÓN Y GESTIÓN DE ARMAS, MATERIALES PELIGROSOS Y MUNICIONES**			
	La organización que use armas, materiales peligrosos, explosivos y municiones debe establecer procedimientos debidamente documentados y registros para la obtención, el manejo, la responsabilidad y la trazabilidad de las armas, incluyendo: a) Cumplimiento de las leyes nacionales e internacional vigentes (por ejemplo, las sanciones de las Naciones Unidas). b) Cumplimiento con los controles de importación y exportación, registros, certificaciones, permisos y requisitos de transporte. c) Adquisición. d) Almacenamiento seguro. e) Controles sobre su identificación, disposición, uso, mantenimiento, devolución y pérdida. f) Registros con respecto a cuán y a quién fueron asignadas las armas. g) Identificación y conteo de todas las armas y municiones. h) Eliminación apropiada y verificación de la misma.	SI	SI	
8.6.4	**8.6.4 UNIFORMES E INSIGNIAS**			

	En consistencia con la seguridad de sus clientes, otros civiles y los requisitos establecidos por la ley, la organización debe usar uniformes e insignias para identificar su personal y sus medios de transporte como pertenecientes a la organización cuando estén llevando a cabo actividades según lo estipulado en su contrato. Esta identificación debe ser visible a distancia y distinguible de aquellas usadas por las fuerzas policiales y militares. La organización debe establecer y documentar procedimientos para el uso de los uniformes e insignias, así como procedimientos para identificar y documentar cuándo esas identificaciones son inconsistentes con los requisitos de esta cláusula.	SI	SI	
8.7	**8.7 RECURSOS, ROLES, RESPONSABILIDADES Y AUTORIDAD**			
	La organización debe establecer, implementar y mantener procedimientos para promover un ambiente de trabajo seguro y saludable, incluyendo precauciones razonables para proteger a las personas que trabajan para la organización en operaciones de alto riesgo o amenaza, de manera consistente con las obligaciones contractuales y las regulaciones y leyes vigentes. Estos procedimientos deben incluir: a) Evaluar la salud ocupacional y los riesgos de seguridad para las personas trabajando para la organización, así como los riesgos a terceros. b) Entrenamiento ante ambientes hostiles. c) Provisión de equipos personales para la protección, armas apropiadas y munición. d) Concienciación, atención y apoyo en salud médica y psicológica. e) Lineamientos para identificar y atender la violencia en el puesto de trabajo, faltas de conducta apropiada, abuso de alcohol o drogas, acoso sexual y comportamiento indebidos.	SI	SI	
8.8	**8.8 MANEJO DE INCIDENTES**			
8.8.1	**8.8.1 GENERAL**			
	La organización debe establecer, implementar y mantener procedimientos para identificar eventos indeseables y disruptivos que puedan impactar la organización, sus actividades, servicios, partes interesadas, derechos humanos y el medioambiente. Los procedimientos deben documentar cómo la organización prevendrá, mitigará y responderá proactivamente a eventualidades. A la hora de establecer, implementar y mantener procedimientos para ágilmente prepararse para mitigar y responder ante un evento disruptivo, la organización debe considerar cada una de las siguientes acciones: a) Salvaguardar la vida y asegurar la seguridad de las partes interesadas internas y externas; b) Respetar los derechos humanos y la dignidad humana; c) Prevenir el aumento y la escalada de un evento disruptivo; d) Minimizar la disrupción a las operaciones; e) Notificar a las autoridades apropiadas; f) Proteger la imagen y la reputación (tanto de la organización como del cliente); g) Acciones correctivas y preventivas.	SI	SI	
8.8.2	**8.8.2 MONITOREO, REPORTE E INVESTIGACIÓN DE INCIDENTES**			
	La organización debe establecer, implementar y mantener procedimientos para el monitoreo de incidentes, investigaciones arreglos y enmiendas disciplinarias. Los incidentes que involucren el uso de la fuerza armada, cualquier baja, herida física, acusación de abuso, pérdida de información valiosa o equipos delicados, abuso de sustancias o cualquier inconformidad con el Documento de Montreux y el ICoC, así como las leyes vigentes y aplicables, deben ser reportados e investigados siguiendo los siguientes pasos: a) Documentación del incidente.b) Notificación a las autoridades competentes. c) Pasos para investigar el incidente. d) Identificación de las causas primordiales. e) Acciones correctivas y preventivas tomadas. f) Cualquier compensación y defensa suministrados a las partes afectadas. La organización debe asegurar que todas las personas trabajando para ella son	SI	SI	

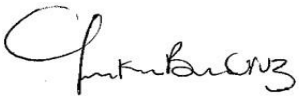
	concientes de sus responsabilidades y de los mecanismos para monitorear y reportar no-conformidades. Los registros de las no-conformidades y los incidentes deben ser mantenidos por un mínimo de siete años o como lo especifiquen las normas y regulaciones legales.			
8.8.3 PROCEDIMIENTOS INTERNOS Y EXTERNOS ANTE QUEJAS Y RECLAMOS				
	La organización debe establecer procedimientos para documentar y atender las quejas de reclamos recibidas de las partes interesadas internas (incluyendo al cliente y otras partes afectadas). Los criterios eficaces para los procesos de quejas, deben estar establecidos y documentados. Los procedimientos serán comunicados a las partes interesadas internas y externas para facilitar el reporte, por parte de los individuos, de no-conformidades potenciales y efectivas frente a esta Norma Internacional, o violaciones a las leyes nacionales, internacionales y de derechos humanos. La organización debe investigar las acusaciones de manera ágil e imparcial, con las debidas consideraciones de confidencialidad impuestas por la ley local vigente. Las organizaciones deben establecer y documentar procesos para: a) Recibir y atender quejas y reclamos; b) Establecer pasos jerárquicos para la resolución de los procesos; c) Investigación de los reclamos, incluyendo procedimientos para: i) Cooperar con los mecanismos de investigación externos; ii) Prevenir la intimidación de testigos o el entorpecimiento de recolección de evidencia; iii) Proteger de la retaliación a los individuos que denuncien agravios o comuniquen quejas con buena intención d) Identificar las causas primordiales; e) Acciones correctivas y preventivas emprendidas, incluyendo las acciones disciplinarias adecuadas para cualquier infracción; f) Comunicaciones con las autoridades competentes; Las quejas sobre actos criminales, violaciones de los derechos humanos o peligro inminentes para los individuos serán tratadas inmediatamente por la organización y las demás autoridades de manera apropiada.	SI	SI	
8.8.4	**8.8.4 POLÍTICA DE PROTECCIÓN PARA DENUNCIANTES**			
	La organización debe establecer una política de protección de denunciantes para aquellas personas que trabajan para ella y que tengan razones para creer que una no-conformidad con esta Norma Internacional ha sido cometida, y deben respetar su derecho a reportar anónimamente e internamente dicha anomalía, así como externamente a las autoridades competentes. La organización no debe tomar ninguna acción adversa contra un individuo por el acto de reportar una acción de buena fe. La organización debe informar al cliente de todas las violaciones de la ley o de derechos humanos informadas.	SI	SI	
9. EVALUACIÓN DE DESEMPEÑO				
9.1	**9.1 MONITOREO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN**			
9.1.1	**9.1.1 GENERAL**			

	La organización debe evaluar los planes de gestión, los procedimientos y capacidades de las operaciones de seguridad con evaluaciones periódicas, examen, reportes post-incidentes, lecciones aprendidas, evaluaciones de desempeño y ejercicios. Los cambios significativos en estos factores deben reflejarse inmediatamente en los procedimientos. La organización debe mantener registros de los resultados de las evaluaciones periódicas. La organización debe determinar: ● Qué necesita ser monitoreado y medido. ● Los métodos para el monitoreo, la medición, el análisis y la evaluación, de ser posible, para asegurar resultados válidos. ● Cuándo deben ser efectuados el monitoreo y la medición. ● Cuándo deben ser evaluados y analizados los resultados del monitoreo y la medición. La organización debe mantener la información documentada apropiada como evidencia de los resultados. la organización debe evaluar el desempeño de las operaciones de seguridad y la efectividad del SGOS. La organización debe establecer, implementar y mantener métricas de desempeño y procedimientos para monitorear y medir, de manera periódica y regular, aquellas características de la operación que tengan un impacto material en su desempeño (incluyendo sociedades, subcontratos y relaciones en la cadena de suministro). Los procedimientos deben incluir la documentación de información para monitorear el desempeño, los controles operacionales aplicables y la conformidad con los objetivos y metas de la gestión de las operaciones de seguridad. La organización debe evaluar y documentar el desempeño de los sistemas que protegen sus bienes (humanos y físicos), así como sus sistemas de comunicaciones y de información.	SI	SI	
9.1.2	**9.1.2 EVALUACIÓN DE CONFORMIDAD**			
	De manera consistente con su compromiso con la conformidad, la organización debe establecer, implementar y mantener procedimientos para evaluar periódicamente la conformidad con los requisitos legales y de derechos humanos. La organización debe mantener un registro con los resultados de todas sus evaluaciones periódicas.	SI	SI	
9.1.3	**9.1.3 EJERCICIOS Y PRUEBAS**			
	La organización debe usar ejercicios y otros medios para probar la idoneidad y eficacia de los planes del SGOS, los procesos y procedimientos, incluyendo las relaciones con las partes interesadas y las interdependencias con subcontratistas. Los ejercicios en escenarios operacionales para el manejo de incidentes deben atender los puntos identificados en la evaluación del riesgo, así como pruebas de estrés para identificar posibles problemas y debilidades en los procedimientos de gestión del riesgo. Los ejercicios serán diseñados y conducidos de manera que se limite el riesgo y la disrupción a las operaciones, mientras expone las personas, los bienes y la información a la cantidad mínima de riesgo. Los ejercicios deben ser conducidos de manera regular (al menos anualmente), o siguiendo los cambios relevantes a la misión y/o estructura de la organización, o siguiendo los cambios relevantes del ambiente exterior. Un reporte formal debe ser redactado después de cada ejercicio. El reporte debe evaluar la idoneidad y la eficacia de los planes del SGOS de la organización, procesos y procedimientos, incluyendo no-conformidades y debe proponer acciones preventivas y correctivas. Los reportes generados tras cada ejercicio deben hacer parte de la evaluación hecha por la alta dirección.	SI	SI	
9.2	**9.2 AUDITORÍA INTERNA**			
	La organización debe establecer, implementar y mantener un programa de auditoría para la gestión de las operaciones de seguridad y conducir auditorías internas en intervalos planeados para proveer información sobre si: a) Se ajustan a: - Los requisitos propios de la compañía para su SGOS. - Las obligaciones legales, regulatorias y de derechos humanos vigentes, así como las obligaciones contractuales. - Los requisitos de esta Norma Internacional. b) Son implementadas y mantenidas de manera efectiva. c) Se desarrollan según lo esperado. d) Han sido efectivas para lograr la política, la meta y los objetivos del SGOS de la organización.	SI	SI	

9.2.2	**9.2.2**			
	La organización debe: a) Planear, establecer, implementar y mantener programas de auditoría que incluyan la frecuencia, los métodos, las responsabilidades, los requisitos de planeación y reportes que tomarán en consideración el estado y la importancia de los procesos y las áreas encargadas, así como los resultados de auditorías previas. b) Definir los criterios de auditoría, la frecuencia del alcance, los métodos, las responsabilidades, los requisitos de planeación y el reporte de cada auditoría. c) Seleccionar auditores y conducir auditorías para asegurar un proceso de auditorías objetivo e imparcial (por ejemplo, los auditores no deben auditar su propio trabajo). d) Asegurar que los resultados de las auditorías sean reportados al área administrativa Responsable por el área auditada. e) Mantener información documentada como evidencia de la implementación de un programa de auditoría y los resultados de las auditorías. El área administrativa responsable del área auditada debe asegurar que las acciones son tomadas sin ningún tipo de retraso injustificado para eliminar las no-conformidades detectadas y sus causas. Las actividades de seguimiento deben incluir la verificación de las acciones tomadas y el reporte y la verificación de los resultados.	SI	SI	
9.3	**9.3 EVALUACIÓN GERENCIAL**			
	La alta dirección debe revisar el SGOS de la organización en intervalos planeados con el fin de asegurar su continuidad, idoneidad, adecuación y efectividad. Esta evaluación debe incluir la identificación de oportunidades de mejora y las necesidades de cambio para el SGOS, incluyendo la política de SGOS y sus objetivos. Los resultados de estas evaluaciones deben ser documentados claramente y los registros deben ser mantenidos. La evaluación de la dirección debe incluir consideraciones sobre: a) El estado de las acciones provenientes de revisiones por la dirección anteriores. b) Cambios en cuestiones internas o externas relevante para el SGOS. c) Información sobre el desempeño de las operaciones de seguridad, incluyendo puntos sobre: i) No-conformidades y acciones correctivas; ii) Resultados del monitoreo y la medición; iii) Resultados de la auditoría; d) Impactos a las operaciones de seguridad. e) Criterios y controles de la gestión del riesgo) Oportunidades para el mejoramiento continuo. Los resultados de la evaluación directiva deben incluir decisiones relacionadas con las oportunidades para el mejoramiento continuo y cualquier necesidad de cambio al SGOS. La organización debe mantener información documentada como evidencia de los resultados de las revisiones por la dirección.	SI	SI	
9.3.2	**9.3.2 INSUMOS PARA LA EVALUACIÓN**			
	Los insumos para la revisión por la dirección deben incluir: a) Resultados de evaluaciones y auditorías del SGOS. b) Retroalimentación de las partes interesadas. c) Técnicas, productos o procedimientos que podrían usarse en la organización para mejorar la eficacia y el desempeño del SGOS. d) El estado de las acciones correctivas y preventivas. E) El resultado de las pruebas y los ejercicios. f) Riesgos atendidos inadecuadamente en evaluaciones del riesgo anteriores. g) Reportes de incidentes. h) Resultados de mediciones de la efectividad. i) Acciones continuas de revisiones por la dirección anteriores. j) Cualquier cambio que pudiera afectar el SGOS. k) Adecuación de los objetivos y las políticas. l) Recomendaciones para el mejoramiento.	SI	SI	
9.3.3	**9.3.3 RESULTADOS DE LA EVALUACIÓN**			
	Los resultados de las evaluaciones de la alta dirección deben incluir decisiones y acciones relacionadas con posibles cambios a la política, los objetivos y metas y otros elementos del SGOS, con miras a promover el mejoramiento continuo, incluyendo: a) Mejoramiento de la efectividad del SGOS. b) Actualización de los planes de evaluación y gestión del riesgo. c) Modificación de los procedimientos y controles que afectan el riesgo, como sea necesario, para responder a eventos internos y externos que puedan	SI	SI	

	afectar el SGOS. d) Recursos necesarios. e) Mejoramiento de cómo está siendo medida la eficacia de los controles.			
10. MEJORA				
10.1	**10.1 NO-CONFORMIDAD Y ACCIÓN CORRECTIVA**			
	La organización debe establecer, implementar y mantener procedimientos para lidiar con las no-conformidades y tomar acciones correctivas y preventivas. Los procedimientos deben definir los requisitos para identificar y corregir no-conformidades y tomar acciones para mitigar sus consecuencias. Cuando ocurra una no-conformidad, la organización debe: a) Reaccionar a la no-conformidad y, según aplique: - Efectuar acciones para controlarla y corregirla. - Lidiar con las consecuencias. b) Evaluar la necesidad de acciones para prevenir no-conformidades y eliminar las causas de no-conformidad, con el fin de que no recurran u ocurran en otra parte: - Revisando y evaluando la no-conformidad. - Determinando las causas que originaron la no-conformidad. - Determinando si existen no-conformidades similares o podrían existir potencialmente. c) Investigar las no-conformidades, determinando sus causas y efectuando acciones que eviten su recurrencia. d) Implementar cualquier acción apropiada y necesaria que esté diseñada para evitar la recurrencia. e) Revisar la eficacia de cualquier acción preventiva efectuada. f) Registrar los resultados de las acciones correctivas y preventivas efectuadas. g) Hacer cambios al SGOS de ser necesario. Las acciones correctivas deben ser apropiadas a los efectos de las no-conformidades encontradas. La organización debe asegurar que los cambios propuestos sean hechos a la documentación del SGOS y que se mantendrá información documentada como evidencia de: - La naturaleza de las no-conformidades y cualquier acción subsecuente efectuada. - Los resultados de cualquier acción correctiva.	SI	SI	
10.2	**10.2 MEJORA CONTINUA**			
10.2.1	**10.2.1 GENERAL**			
	La organización debe mejorar continuamente la idoneidad, adecuación y eficacia del SGOS a través del uso de la política, objetivos, resultados de auditoría, análisis de eventos monitoreados, acciones preventivas y correctivas y revisiones por la dirección de las operaciones de seguridad.	SI	SI	
10.2.2	**10.2.2 GESTIÓN DEL CAMBIO**			
	La organización debe establecer y un programa de gestión del cambio para las operaciones de seguridad definido y documentado para asegurar que cualquier cambio interno o externo que impacte la organización sea evaluado en relación con el SGOS. Deberá identificar cualquier actividad crítica novedosa que deba ser incluida en el programa de gestión del cambio del SGOS.	SI	SI	
10.2.3	**10.2.3 OPORTUNIDADES PARA EL MEJORAMIENTO**			
	La organización debe monitorear, evaluar y aprovechar oportunidades para el mejoramiento del desempeño del SGOS y eliminar cualquier causa potencial de problemas, incluyendo: a) Monitoreo continuo del horizonte operacional para identificar potenciales problemas y oportunidades para el mejoramiento. b) Determinando e implementando las acciones necesarias para mejorar el desempeño de las operaciones de seguridad. c) Revisando la eficacia de las acciones tomadas para el mejoramiento del desempeño. Las acciones emprendidas deben ser apropiadas al impacto, los riesgos potenciales, las realidades recursivas y las obligaciones de la organización. La alta dirección debe asegurar que las acciones son emprendidas sin ningún retraso innecesario para aprovechar las oportunidades para el mejoramiento. Cuando los acuerdos existentes sean revisados y los nuevos acuerdos que puedan impactar la calidad de la gestión de las operaciones y las actividades sean introducidos, la organización debe considerar el riesgo asociado antes de implementarlos. Los resultados de las evaluaciones y las acciones	SI	SI	

	emprendidas deben estar claramente documentadas y los registros deben ser mantenidos. Las actividades de seguimiento deben incluir la verificación de las acciones emprendidas y el reporte de los resultados de la verificación.			



YENNY KARINA BONILLA CRUZ
Representante Legal - Fecha actualización: 04/05/2024