POLÍTICA GLOBAL DE SEGURIDAD DEL SISTEMA DE INFORMACIÓN

STATUS : VALIDATED

VERSION : 2,5

PÚBLICO INTERNO SECRETO RESTRINGIDO

X

BUREAU VERITAS

Shaping a World of Trust

Aprobadores

Nombre	Posición
François VILJOEN	Vicepresidente sénior, CIO del grupo
Julien ANICOTTE	Director de Seguridad de la Información del Grupo

Documentos de referencia

Título del documento	Nombre del documento

Clasificación

Nivel	Confidencialidad
C1	Público

RESUMEN

GLOSARIO

B

BCP: Plan de Continuidad de Negocio.

BL: Línea de Negocio.

C

CIO: Director de Información.

CISO: Director de Seguridad de la Información.

G

ISSP global: Política global de seguridad de los sistemas de información. Documento actual.

Yo

SGSI: Sistema de Gestión de Seguridad de la Información.

ISO 27001: Un estándar de gestión de la seguridad de la información. Proporciona los requisitos para un sistema de gestión de seguridad de la información (SGSI).

Políticas de ISS: Políticas de seguridad de los sistemas de información. Incluir el ISSP global y las políticas operativas.

O

Y: Grupo Operativo.

S

Servicios: todo tipo de servicios prestados por un Proveedor para Bureau Veritas, incluyendo pero no limitado a asistencia técnica, servicios de mantenimiento, cualquier servicio basado en la nube como SaaS, IaaS o PaaS. Los servicios se pueden proporcionar en el sitio o fuera del sitio.

SO: Oficial de Seguridad.

Proveedor: Licitador que ha sido seleccionado por Bureau Veritas para prestar los Servicios en virtud de un Contrato.

U

Usuario: cualquier persona, ya sea un empleado, contratista u otra parte interesada, que interactúe y utilice el Sistema de Información de Bureau Veritas para realizar tareas, acceder a información o realizar operaciones dentro de un contexto organizacional definido.

1. INTRODUCCIÓN

La Política Global de Seguridad del Sistema de Información define el marco de referencia para la seguridad de la información de Bureau Veritas destacando los problemas y objetivos de seguridad. También proporciona principios de gobernanza y requisitos de seguridad fundamentales que se aplican a Bureau Veritas.

El ISSP Global tiene como objetivo garantizar la protección de la información a través de los cuatro criterios de clasificación: Disponibilidad; Integridad; Confidencialidad y trazabilidad.

1.1. LA SEGURIDAD DE LA INFORMACIÓN, UN TEMA VITAL

La información en todas sus formas, ya sea escrita, oral, electrónica, procesada manual o automáticamente, es un recurso estratégico en el que se basa el rendimiento, la sostenibilidad y la capacidad de la empresa para desarrollar sus actividades y resultados.

Para hacer frente a las amenazas accidentales y maliciosas que puedan afectar a la seguridad de su sistema de información, Bureau Veritas debe proteger eficazmente su sistema de información mediante la implementación de medidas de seguridad adecuadas, de acuerdo con los retos de seguridad.

Estas medidas de seguridad deben permitir a Bureau Veritas respetar sus compromisos contractuales, las restricciones legales y reglamentarias y la continuidad de los servicios prestados a los clientes, así como su calidad. Además, esto contribuye a la protección y mejora de la imagen de Bureau Veritas.

1.2. COMÚN OBJETIVOS PARA UN PROTECCIÓN EFECTIVA

El marco de la seguridad del sistema de información de Bureau Veritas está definido por el ISSP global, respaldado por políticas operativas que detallan las reglas y responsabilidades con respecto a la gestión de la seguridad de la información en temas específicos.

Los principios de gobernanza y las reglas comunes formalizadas en las Políticas de ISS deben garantizar la protección efectiva de la información en el ámbito de Bureau Veritas y la coherencia del sistema de gestión de la seguridad de la información. Asimismo, deben permitir capitalizar las medidas de seguridad implementadas y las mejores prácticas en las diferentes entidades y subsidiarias de la organización.

1.2.1. PERÍMETRO ORGANIZACIONAL

El ISSP Global debe aplicarse a todas las entidades y filiales del grupo Bureau Veritas en todo el mundo.

Las políticas de ISS también deben tener un impacto en los proveedores. Estas políticas deben definir los principios fundamentales de seguridad aplicables a los servicios contratados por Bureau Veritas con los Proveedores.

Algunas filiales o entidades de Bureau Veritas pueden estar sujetas a políticas de seguridad específicas y específicas debido a su actividad, el país en el que se encuentran (por ejemplo, restricciones legales locales), los requisitos contractuales de los Clientes o Proveedores.

1.2.2. PERÍMETRO FUNCIONAL

Todos los recursos que respaldan la información de Bureau Veritas están incluidos en el Sistema de Gestión de Seguridad de la Información, así como todas las formas destinadas a crear, adquirir, procesar, almacenar, distribuir o destruir esta información en o utilizando:

- Equipos de los usuarios (por ejemplo, ordenadores de sobremesa y portátiles, smartphones, tabletas).
- Recursos operativos (por ejemplo, servidores, impresoras, dispositivos de telecomunicaciones).
- Software (por ejemplo, software operativo, bases de datos).
- Soporte en papel.
- Recursos humanos y organizacionales.

1.2.3. PERÍMETRO TÉCNICO

Las políticas de ISS deben ser implementadas por el grupo Bureau Veritas y todas sus entidades y subsidiarias. Su objetivo es garantizar la aplicabilidad independientemente del contexto técnico, no dando detalles sobre las tecnologías a implementar, sino solo los requisitos funcionales y organizativos.

1.2.4. ACERCARSE

Además de las mejores prácticas de la industria, las políticas de ISS deben tener en cuenta lo siguiente:

- Gestión de riesgos de la información: las reglas establecidas en cada política deben construirse para gestionar y reducir los riesgos que tienen un impacto significativo en las operaciones comerciales y amenazan la confidencialidad, integridad, disponibilidad y trazabilidad de la información.
- Cumplimiento: las reglas de seguridad deben hacer cumplir los requisitos de

evaluación de la regulación, los términos contractuales, los estándares de la industria, así como la implementación de medidas adecuadas para cumplir.

- Objetivos de negocio: Las políticas de ISS, además de apoyar la gobernanza, deben cooperar y coordinarse con el negocio para alinear la estrategia de seguridad con los objetivos y la estrategia de Bureau Veritas: resiliencia y protección de datos.

2. DOCUMENTACIÓN DE LA ISS

2.1. ESTRUCTURA DE LA DOCUMENTACIÓN DE SEGURIDAD DEL SISTEMA DE INFORMACIÓN

La documentación de seguridad de la información de Bureau Veritas se formaliza como un repositorio documental de tres niveles:

- **The Global ISSP** (documento actual): documento de referencia, que establece los desafíos, los principios de gobernanza y los principios fundamentales de la seguridad de la información para todo el grupo Bureau Veritas, en línea con la norma ISO 27001.
- **Políticas Operativas**: definir las reglas de seguridad de la información por tema aplicable a Bureau Veritas. Podrán concederse exenciones temporales a entidades o filiales si no puede garantizarse su cumplimiento. Están validados por el CISO Global de Bureau Veritas.
- **Guías, normas y procedimientos**: documentos operativos, actividades de apoyo, cumplimiento de los requisitos definidos en las normas de las Políticas Operativas. Estos documentos se pueden definir a nivel de grupo o localmente.

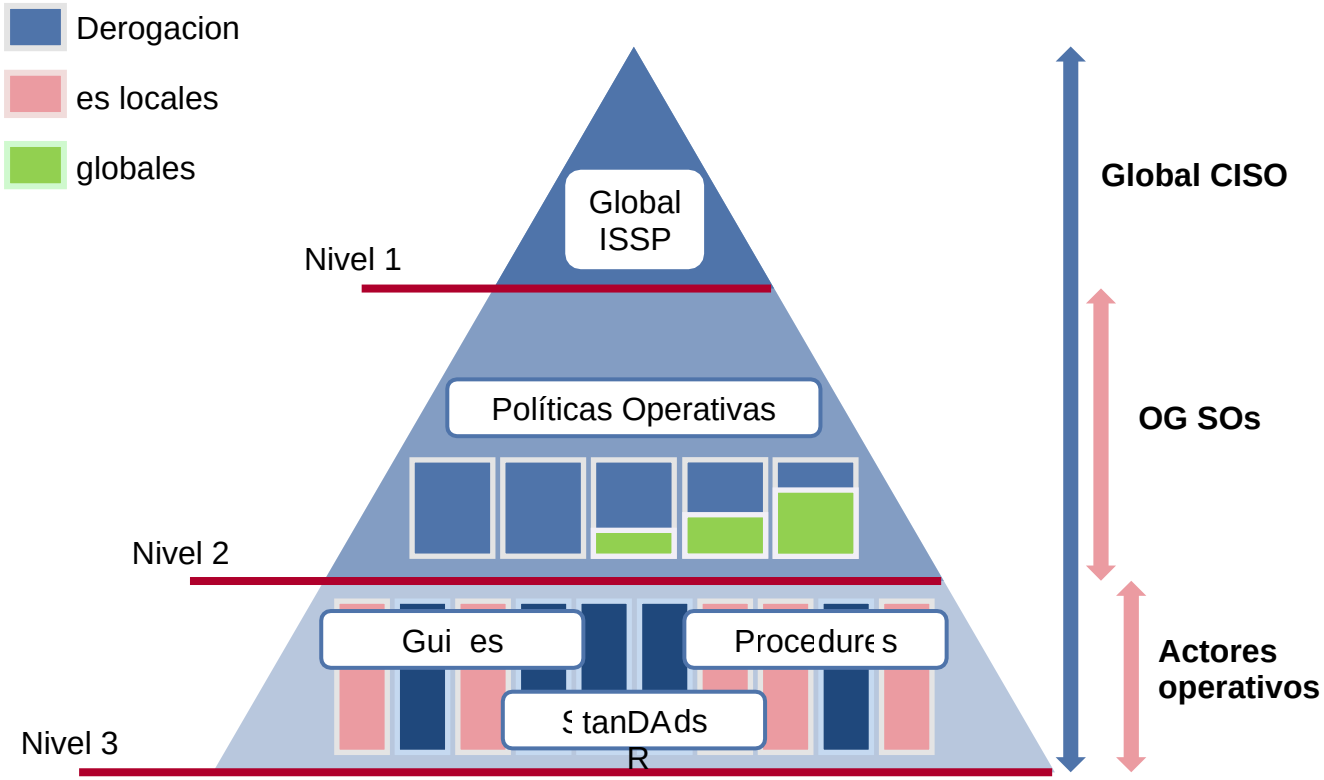

Figura 1 – Repositorio documental y responsabilidades.

2.2. IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD

2.2.1. CICLO DE VIDA

Con el fin de garantizar la eficiencia y sostenibilidad de las Políticas de ISS a lo largo del tiempo y su adecuación a los requisitos de seguridad de Bureau Veritas, las Políticas de ISS deben estar sujetas a una mejora continua.

Este proceso de mejora continua debe ser cíclico, basado en el principio Planificar-Hacer-Verificar-Actuar (PDCA):

- **Definición y planificación (Plan):** el CISO Global establece un plan de acción que incluye: las políticas de ISS a actualizar, las mejoras necesarias y la fase de comunicación.
- **Implementación (Do):** se implementa el plan de acción definido en la fase anterior. Las mejoras se aplican a las políticas de ISS correspondientes; Las políticas actualizadas se comunican a las personas pertinentes para que las revisen y validen.
- **Control y seguimiento (Check):** esta fase permite identificar impactos en las actividades operativas. La aplicación de las políticas de ISS está controlada.
- **Mantenimiento y mejora (Ley):** Los oficiales de seguridad y otras partes interesadas (por ejemplo, corresponsales de seguridad) identifican las BPA e informan al CISO global. Los comentarios se analizan para identificar las mejoras necesarias y alimentar la próxima fase del Plan.

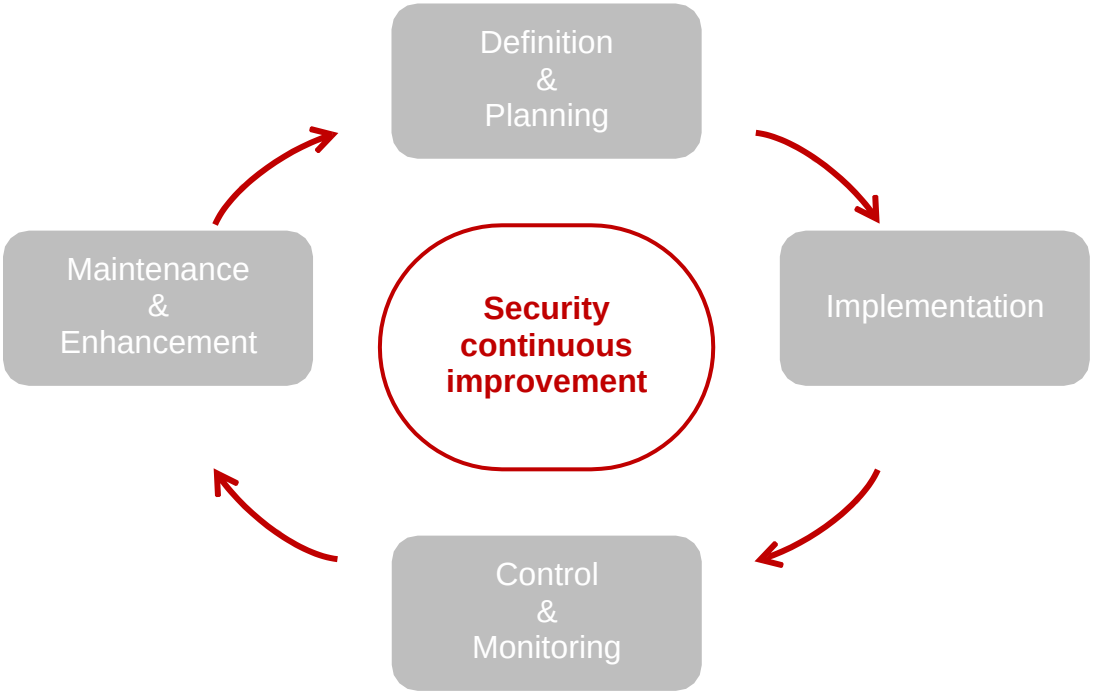

Figura 2 - Ciclo de vida de la mejora continua.

Las políticas operativas y del ISSP global deben revisarse al menos una vez al año. Las solicitudes de actualizaciones, que surgen de necesidades internas o factores externos, están centralizadas y validadas por el CISO Global. Las políticas de ISS actualizadas se envían para su validación a la Dirección Ejecutiva de Bureau Veritas.

Todo el ciclo de vida de las Políticas ISS debe estar incluido en el Sistema de Gestión de Seguridad de la Información (SGSI), asegurando su implementación. Los diversos elementos del SGSI deben formalizarse y documentarse para garantizar la trazabilidad de sus operaciones.

2.2.2. APLICABILIDAD

Las políticas de ISS deben ser implementadas y aplicables.

Los incumplimientos de las Políticas de ISS deben estar sujetos a planes formales de acción correctiva con un cronograma de finalización definido o derogaciones.

2.2.3. EDITORIAL

La Política Global de Seguridad del Sistema de Información debe publicarse públicamente en el sitio web de la empresa para mostrar claramente el compromiso de Bureau Veritas de proteger su información, así como la información de los clientes.

Las políticas operativas, por otro lado, se publican internamente. Deben ser accesibles solo para todos los usuarios de Bureau Veritas.

Cada actualización de las políticas debe ir seguida de una comunicación a las partes interesadas pertinentes para informarles de los nuevos cambios.

2.2.4. PROCEDIMIENTOS PARA LA TRAMITACIÓN DE EXENCIONES Y EXCEPCIONES

Se espera que todos los componentes del sistema de información de Bureau Veritas cumplan con las políticas y estándares de ISS. Sin embargo, en varios casos, el cumplimiento de algunas reglas no se puede lograr por diversas razones. Debe formalizarse e implementarse el procedimiento de derogación para gestionar, documentar y supervisar estas exenciones y excepciones.

Las solicitudes de derogación deben ser revisadas y aprobadas por el CISO Global, el equipo de cumplimiento o el OG/SO de la entidad solicitante.

3. GOBERNANZA DE EL SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

3.1. VISIÓN GENERAL DE LA GOBERNANZA

La gobernanza de la seguridad del sistema de información tiene como objetivo definir la estructura del flujo de seguridad de la información de Bureau Veritas, así como las funciones y responsabilidades de todas las personas relevantes que componen esta estructura (CISO global, OG, equipo de seguridad de la información, etc.).

A través de esta gobernanza, el objetivo es enmarcar la actividad de la corriente de seguridad del sistema de información de Bureau Veritas, definiendo los procesos relevantes, animando la corriente y proporcionando el material necesario (Políticas de ISS, soportes de formación y concienciación, guías).

La gobernanza también incluye cualquier papel relevante para la animación de la seguridad del sistema de información dentro de las actividades comerciales, las funciones de control, la propiedad y la gestión de proyectos.

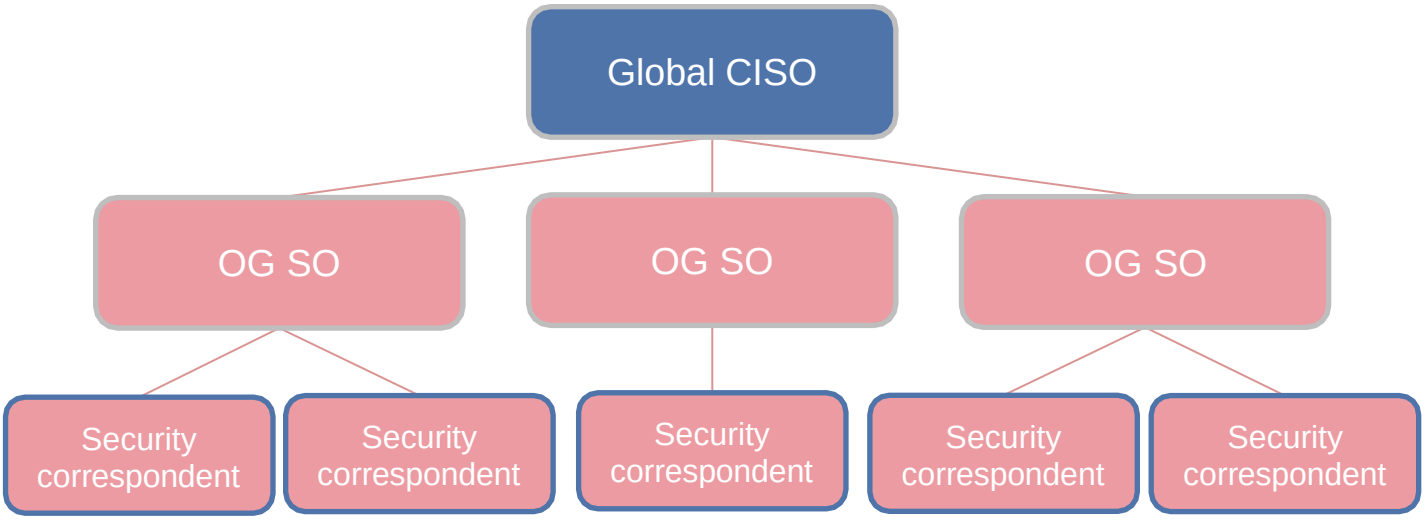

Figura 3 - Organización de la gobernanza ISS de Bureau Veritas.

3.2. EL DIRECTOR GLOBAL DE SEGURIDAD DE LA INFORMACIÓN (CISO GLOBAL) DE BUREAU VERITAS

3.2.1. PRESENTACIÓN DEL CISO GLOBAL

El CISO Global de Bureau Veritas es el garante de la seguridad y la continuidad del sistema de información del grupo Bureau Veritas, sus entidades y sus filiales. Como tales, están a cargo del Sistema de Gestión de Seguridad de la Información de Bureau Veritas.

El CISO Global cumple con sus obligaciones dentro de Bureau Veritas y junto a proveedores, clientes y terceros externos (por ejemplo, entidades gubernamentales, organismos de certificación).

3.2.2. ENCARGOS DEL CISO GLOBAL

El CISO Global de Bureau Veritas supervisa el Sistema de Gestión de Seguridad de la Información de la organización y su mantenimiento en condiciones operativas. Como parte de estas funciones, sus misiones son:

- Formalizar, coordinar y mantener en condiciones operativas la organización del flujo de seguridad del sistema de información de Bureau Veritas.
- Definir campañas de formación y sensibilización.
- Aprobar el nombramiento de los OG.
- Produzca paneles de seguridad globales, centralice los indicadores de los SO de OG y realice análisis globales del rendimiento de la seguridad del sistema de información.
- Desarrollar y actualizar las políticas de ISS.
- Obtener la aprobación de la Dirección Ejecutiva para las Políticas de ISS.
- Hacer cumplir y acompañar la implementación de las políticas de ISS dentro del grupo Bureau Veritas, sus entidades y subsidiarias.
- Supervisar el cumplimiento de las políticas de ISS dentro del grupo Bureau Veritas.
- Gestionar las derogaciones a las políticas de ISS con un alcance global o un impacto crítico.
- Planificar y supervisar las auditorías del sistema de información con fines de seguridad y seguir el plan de acciones correctivas elaborado con las recomendaciones de las auditorías.
- Apruebe, asesore y supervise las auditorías locales de seguridad de la información con el OG SO.
- Participar en los Consejos Asesores de Cambio (CAB), particularmente para cambios con un impacto crítico o grande en el sistema de información de Bureau Veritas.
- Supervisar la implementación y el mantenimiento en condiciones operativas del

proceso de gestión de incidentes de seguridad de Bureau Veritas y sus pruebas periódicas, en particular para garantizar la eficiencia del plan de gestión de crisis y de la unidad de crisis.

- Supervisar la implementación y el mantenimiento en condiciones operativas del Plan de Continuidad de Negocio de Bureau Veritas y sus pruebas periódicas.

3.3. GRUPO OPERATIVO DE OFICIALES DE SEGURIDAD (OG SO) DE BUREAU VERITAS

3.3.1. PRESENTACIÓN DEL OG SO

Los Oficiales de Seguridad OG son los garantes de la seguridad y la continuidad del sistema de información de Bureau Veritas a nivel OG. Son nombrados a nivel OG y serán socios de confianza para el equipo central.

Sus principales funciones son la ejecución y supervisión de las actividades de seguridad de la información en su ámbito dentro de las empresas y los equipos técnicos, pero también garantizar la implementación de iniciativas globales en su respectivo ámbito, especialmente la aplicación de políticas y marcos de cumplimiento.

3.3.2. CESIONES DE OG SO

Los oficiales de seguridad OG de Bureau Veritas supervisan la implementación del Sistema de Gestión de Seguridad de la Información y su mantenimiento en condiciones operativas dentro de su respectivo alcance. Como parte de estas funciones, sus misiones son:

- Reportar información importante al CISO Global.
- Hacer cumplir la implementación de las políticas de ISS.
- Gestionar las derogaciones a las políticas de ISS en su alcance.
- Asegúrese de que se sigan las buenas prácticas de seguridad.
- Definir campañas específicas de formación y sensibilización.
- Produzca paneles de seguridad locales, analice los indicadores de seguridad y envíelos al CISO global.
- Coordinar las acciones de seguridad local.
- Contribuir, con las empresas y los departamentos de TI/SI, a la transcripción de las políticas operativas en procedimientos técnicos (por ejemplo, instalación, operación, manejo de eventos), guías y estándares.
- Aprobar, asesorar y supervisar las auditorías locales de seguridad de la información con el CISO global.
- Participar en los Consejos Asesores de Cambios (CAB) para los cambios en el sistema de información que afecten su alcance.
- Asegurar el mantenimiento en condiciones operativas del proceso de gestión de incidentes de seguridad en su ámbito.
- Asegurar el mantenimiento en condiciones operativas del Plan de Continuidad de Negocio en su alcance.

3.4. CORRESPONSALES DE SEGURIDAD LOCALES

Además de los CISO globales y los SO OG descritos anteriormente, la organización de seguridad de la información involucra a corresponsales de seguridad locales.

Los oficiales de seguridad de OG identifican y supervisan a los corresponsales de seguridad locales dentro de entidades, subsidiarias, departamentos, negocios y donde sea necesario. Los corresponsales de seguridad locales asisten a los SO de OG en sus misiones, implementan la seguridad de la información en su ámbito o desarrollan proyectos basados en necesidades de seguridad específicas.

3.5. CONTACTO CON AUTORIDADES Y GRUPOS DE INTERÉS ESPECIAL

Cuando corresponda, Bureau Veritas y sus filiales establecen y mantienen contacto con las autoridades competentes.

Además, cuando proceda, Bureau Veritas debe establecer y mantener contacto también con grupos de interés especial u otros foros especializados en seguridad y asociaciones profesionales.

Tener canales de contacto establecidos con las partes mencionadas anteriormente puede ser necesario para el cumplimiento (por ejemplo, notificar a las autoridades pertinentes de una violación de datos). Además, los grupos de interés especial u otros foros especializados en seguridad y asociaciones profesionales pueden ayudar a la empresa a anticipar el desarrollo del campo de la ciberseguridad y prepararse para el cambio y la evolución. Estas conexiones también pueden ser útiles en caso de que se requiera apoyo / asesoramiento cuando se enfrenta a una situación desafiante.

4. APÉNDICES

4.1. APÉNDICE 1: HISTORIAL DE REVISIONES

Versión	Autor	Descripción	Fecha
1.5	Cumplimiento de ISS	Nombramiento del CISO del Grupo	12/01/2017
2.0	Cumplimiento de ISS	Actualización de los contenidos para cumplir con la estrategia del grupo	27/03/2017
2.1	Cumplimiento de ISS	Actualización de los roles de seguridad Actualización de la frecuencia de la revisión de las políticas Adición de una nueva política operativa al apéndice	19/12/2019
2.2	Cumplimiento de ISS	Adición de un enfoque de creación de directivas Adición de requisitos de publicación	19/03/2021
2.3	Cumplimiento de ISS	Revisión anual Adición de requisitos para la tramitación de las excepciones	07/04/2022
2.4	Cumplimiento de ISS	Revisión anual	20/04/2023
2.5	Cumplimiento de ISS	Revisión anual	30/04/2024

4.2. APÉNDICE 2: POLÍTICAS OPERATIVAS

Las Políticas Operativas que completan el ISSP Global sobre temas temáticos para Bureau Veritas son:

- Seguridad de los recursos humanos
- Clasificación de la información
- Control de acceso lógico
- Seguridad Física
- Seguridad de las operaciones
- Gestión de trazas de TI
- Manejo de medios
- Equipos de los usuarios
- Seguridad de la red
- Seguridad en la nube

- Desarrollo y mantenimiento de aplicaciones
- Relación con Proveedores
- Gestión de Incidentes de Seguridad
- Continuidad de la actividad