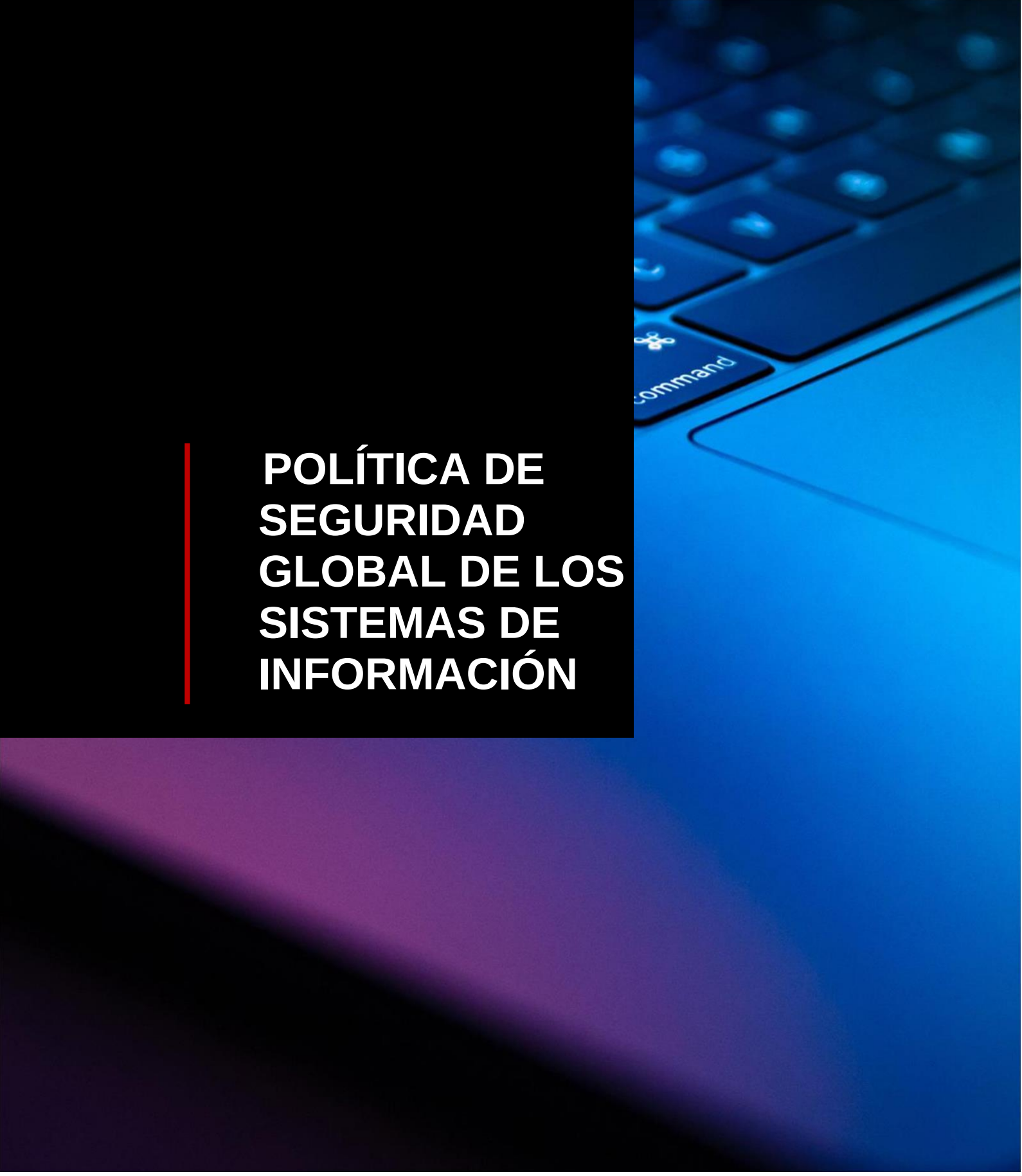

POLÍTICA DE SEGURIDAD GLOBAL DE LOS SISTEMAS DE INFORMACIÓN

ESTATUS : VALIDADO

VERSIÓN : 2,3

PÚBLICO INTERNO RESTRINGIDO SECRETO

X

BUREAU VERITAS

Shaping a World of Trust

Aprobadores

Nombre	Posición
Francois VILJOEN	Vicepresidente Senior, 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: Business Continuity Plan (Plan de continuidad de negocios).

BL: Business Line (Línea de Negocios).

C

CIO: Chief Information Officer (Director de Información).

CISO: Chief Information Security (Officer Director de Seguridad de la Información).

G

Global ISSP: Global Information System Security Policy. (Current Document) Política Global de Seguridad de los Sistemas de Información. Documento actual.

I

ISMS: Information Security Management System.
Sistema de Gestión de la Seguridad de la Información.

ISO 27001: (ISMS) Un Estándar de Gestión de la seguridad de la información. Proporciona los requisitos para un sistema de gestión de la seguridad de la información (ISMS).

ISS Policies: Políticas de Seguridad de los Sistemas de Información. Incluye la ISSP Global y Políticas Operativas

O

OG: Operating Group: Grupo Operativo.

S

Services: Servicios: todo tipo de servicios realizados por un Proveedor para Bureau Veritas, incluidos, entre otros, asistencia técnica, servicios de mantenimiento, cualquier servicio basado en la nube, como SaaS, IaaS o PaaS...; pueden prestarse in situ o fuera de las instalaciones.

SO: Security Officer: (Delegado de Seguridad.)

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

Supplier's Personnel: personal del Proveedor asignado por éste para la prestación de los Servicios.

1. INTRODUCCCIÓN

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

La 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, UNA ASUNTO VITAL

La información en todas sus formas, ya sea escrita, oral, electrónica, procesada manual o automáticamente, es un recurso estratégico del que dependen el rendimiento, la sostenibilidad y la capacidad de la empresa para desarrollar sus actividades y resultados.
Para hacer frente a las amenazas accidentales y malintencionadas que podrían afectar a la seguridad de su sistema de información, Bureau Veritas debe proteger eficazmente su sistema de información mediante la aplicación de medidas de seguridad adecuadas, en consonancia con los retos de seguridad.
Estas medidas de seguridad deben permitir a Bureau Veritas respetar sus compromisos contractuales, las obligaciones legales y reglamentarias y además de 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. OBJETIVOS COMUNES PARA UNA PROTECCIÓN EFICAZ

El marco de la Seguridad del Sistema de Información de Bureau Veritas está definido por el ISSP Global, apoyado por Políticas Operativas que detallan las normas y responsabilidades relativas a la gestión de la seguridad de la información sobre temas específicos.
Los principios de gobernanza y las normas comunes formalizadas en las Políticas ISS deben garantizar la protección eficaz 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 filiales de la organización.

1.2.1. PERÍMETRO ORGANIZATIVO

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

Las Políticas ISS también deben tener un impacto en los Proveedores. Estas políticas deben definir los principios fundamentales de seguridad que se aplican 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 debido a su actividad, al país en el que están ubicadas (por ejemplo, restricciones legales locales), a los requisitos contractuales del Cliente o de los 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, PCs y laptops, smartphones, tablets);
- Recursos operativos (por ejemplo, servidores, impresoras, dispositivos de telecomunicaciones);
- Software (por ejemplo, software operativo, bases de datos);
- Respaldo en papel;
- Recursos Humanos y Organizativos.

1.2.3. PERÍMETRO TÉCNICO

Las Políticas de SSI deben ser aplicadas por el grupo Bureau Veritas y todas sus entidades y filiales. Su objetivo es garantizar la aplicabilidad independientemente del contexto técnico, no dando detalles sobre las tecnologías a implementar, sino sólo los requisitos funcionales y organizativos.

1.2.4. ENFOQUE

Además de las mejores prácticas del sector, las políticas del SSI deben tener en cuenta lo siguiente:

- Gestión de riesgos de la información: las normas establecidas en cada política deben construirse para gestionar y reducir los riesgos que tienen un impacto significativo en las operaciones de negocio y que amenazan la confidencialidad, integridad, disponibilidad y trazabilidad de la información.;
- Compliance: the security rules must enforce assessing compliance

requisitos con regulación, términos contractuales, estándares de la industria, así como la implementación de medidas adecuadas para cumplir;

- Objetivos comerciales: Las políticas de ISS, así como la gobernanza de apoyo 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 ISS

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

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

- **El ISSP Global** (documento actual): documento de referencia, que establece los retos, los principios de gobernanza y los principios fundamentales de la seguridad de la información para todo el grupo Bureau Veritas, en línea con el estándar ISO 27001.;
- **Políticas Operativas**: definir las normas de seguridad de la información por temática solicitándolo a Bureau Veritas. Se pueden conceder excepciones temporales a entidades o filiales si no se puede garantizar el cumplimiento. Siendo estas validadas por el CISO Global de Bureau Veritas;
- **Guías, estándares y procedimientos:** documentos operativos, apoyo de actividades, conformes con los requisitos definidos en las normativas de las Políticas Operativas. Estos documentos pueden definirse a nivel de grupo o localmente.

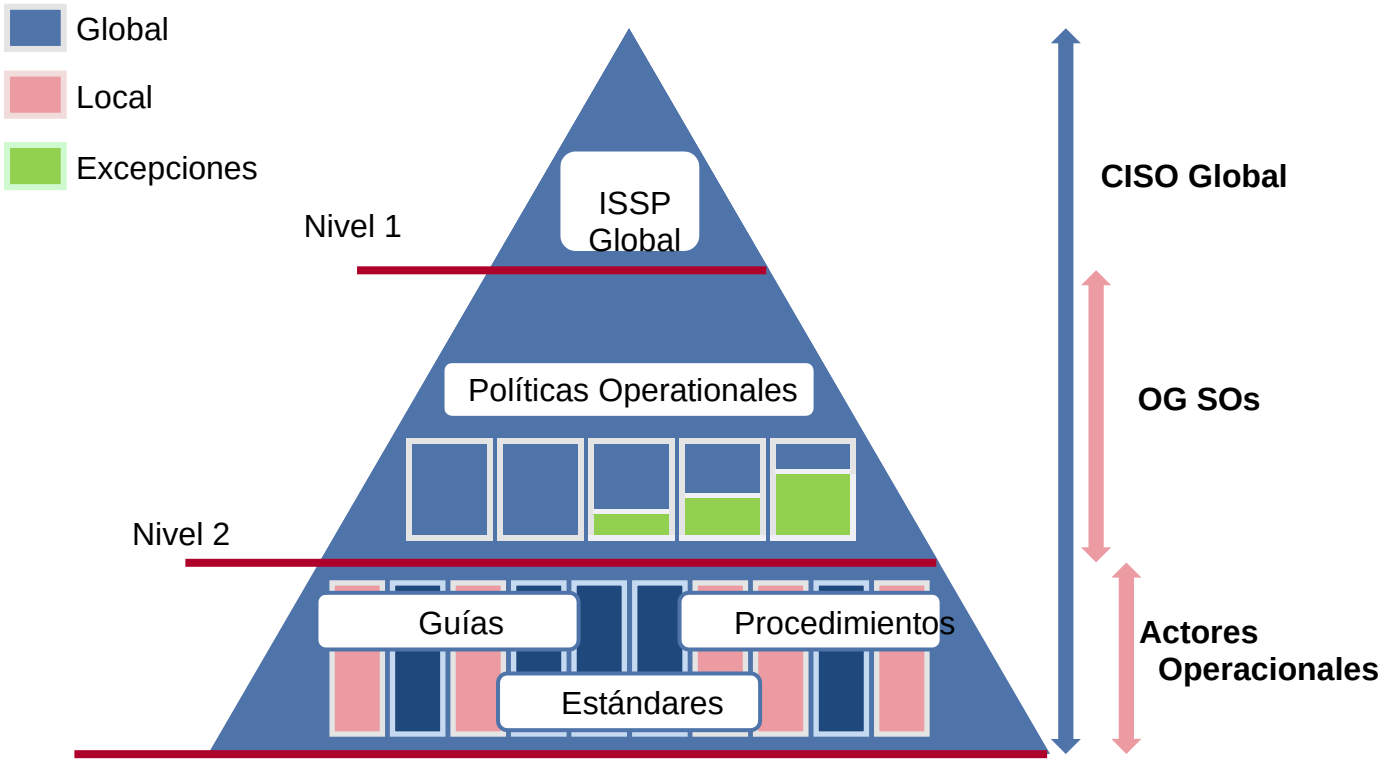

Figura 1 - Depósito documental y responsabilidades

2.2. IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD

2.2.1. CICLO DE VIDA

Con el fin de garantizar la eficacia y la sostenibilidad de las Políticas de SSI a lo largo del tiempo y su adecuación a los requisitos de seguridad de Bureau Veritas, las Políticas de SSI deben ser objeto de una mejora continua.

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

- **Definición y planificación (Planificar):** el CISO Global establece un plan de acción que incluye: Políticas ISS a actualizar, las mejoras necesarias y la fase de comunicación;
- **Implementación (Hacer)**: se aplica el plan de acción definido en la fase anterior. Las mejoras se aplican a las correspondientes políticas de la SSI; las políticas actualizadas se comunican a los delegados pertinentes para su retroalimentación y validación.
- **Control y monitoreo (Verificar)**: esta fase permite identificar las repercusiones en las actividades operativas. Se controla la aplicación de las políticas del SSI.
- **Mantenimiento y mejora (Actuar):** Los delegados de seguridad y otras partes interesadas (por ejemplo, los colaboradores de seguridad) identifican las deficiencias e informan al CISO global. Los comentarios se analizan para identificar las mejoras necesarias y alimentar la siguiente Fase de planificación.

Fase de Planificación.

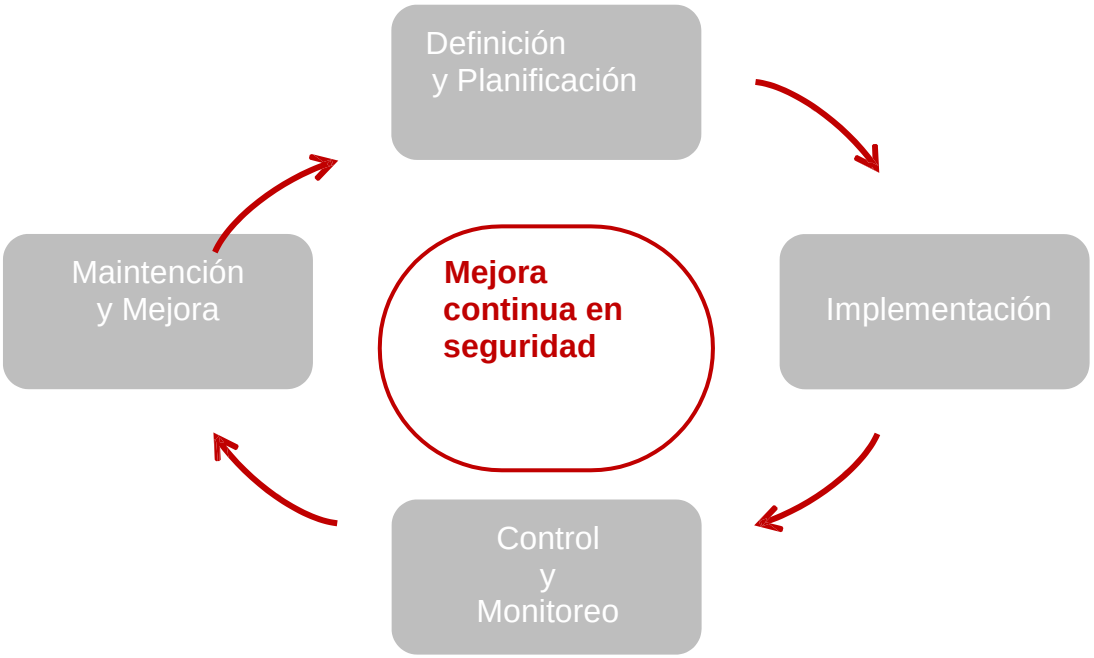

Figura 2 - Ciclo de vida de mejora continua.

Las políticas Globales y Operacionales de ISSP deben revisarse al menos una vez al año. Las solicitudes de actualizaciones, que surgen de necesidades internas o factores externos, son 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 (ISMS), asegurando su implementación. Los diversos elementos del ISMS deben formalizarse y documentarse para garantizar la trazabilidad de sus operaciones.

2.2.2. APLICABILIDAD

Las Políticas de ISS deben implementarse y hacerse cumplir.
Los incumplimientos de las Políticas de ISS deben estar sujetos a planes formales de acción correctiva con un cronograma de finalización definido o excepcione.

2.2.3. PUBLICACIÓN

La Política de seguridad del sistema de información global debe publicarse en el sitio web de la empresa para mostrar claramente el compromiso de Bureau Veritas de proteger su información y la información de los clientes.
Las políticas operativas, por otro lado, se publican internamente. Deben ser accesibles solo para todos los empleados 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 EL TRATAMIENTO 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 puede lograrse por diversas razones. El procedimiento derogatorio para la gestión, documentación y seguimiento de estas exenciones y excepciones deberá formalizarse e implementarse.

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 LA SEGURIDAD DEL SISTEMA DE INFORMACIÓN

3.1. DESCRIPCIÓN GENERAL DE LA GOBERNANZA

La gobernanza de la seguridad del sistema de información tiene como objetivo definir la estructura de la corriente 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 SOs, Equipo de Seguridad de la Información, etc.).

A través de esta gobernanza, el objetivo es enmarcar la actividad de la línea de seguridad de los sistemas de información de Bureau Veritas, definiendo los procesos relevantes, dinamizando la línea y proporcionando el material necesario (Políticas de SSI, soportes de capacitación y sensibilización, guías).

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

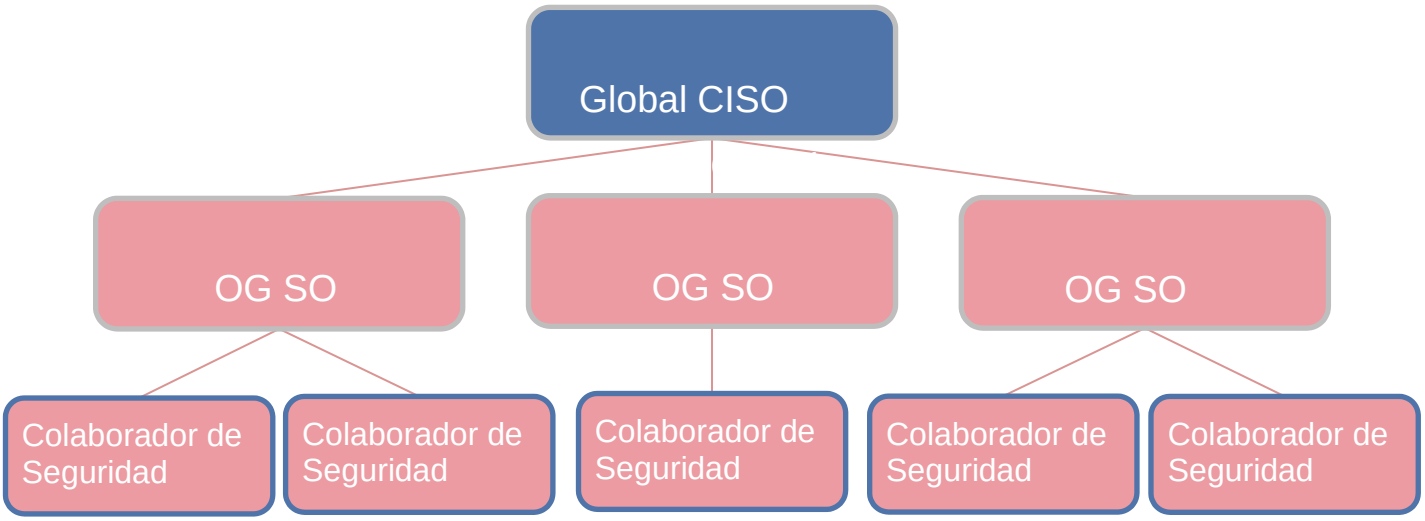

Figura 3 - Organización de la gobernanza del Sistema de SSI de Bureau Veritas

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 subsidiarias. Como tal, está a cargo del Sistema de Gestión de Seguridad de la Información de Bureau Veritas.
El CISO global lleva a cabo sus funciones dentro de Bureau Veritas y junto con proveedores, clientes y terceros externos (por ejemplo, entidades gubernamentales, organismos de certificación).

3.2.2. ASIGNACIONES DEL CISO GLOBAL

El CISO Global de Bureau Veritas está a cargo del Sistema de Gestión de Seguridad de la Información de la organización y su mantenimiento en condiciones operativas. Como parte de estas obligaciones, 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 capacitación y sensibilización;
- Aprobar el nombramiento del OG SO;
- Producir tableros de seguridad global, centralizar indicadores de OG SO y realizar análisis global del desempeño de 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 ISS dentro del grupo Bureau Veritas;
- Manejar excepciones 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 acción correctivo construido con las recomendaciones de las auditorías;
- Aprobar, asesorar y monitorear auditorías locales de seguridad de la información con el OG SO;
- Participar en los Consejos Asesores de Cambio (CAB), en particular para cambios con un impacto crítico o a gran escala 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 la unidad de crisis;
- Supervisar la implementación y el mantenimiento de las condiciones operativas del Plan de Continuidad de Negocios de Bureau Veritas y sus pruebas periódicas.

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

3.3.1. PRESENTACIÓN DEL OG SO

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

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

3.3.2. FUNCIONES DEL OG SO

Los Oficiales de Seguridad de OG de Bureau Veritas están a cargo de la implementación del Sistema de Gestión de Seguridad de la Información y su mantenimiento en condiciones operativas dentro de su respectivo ámbito. Como parte de su deber, sus misiones son:

- Reportar información importante al CISO Global;
- Hacer cumplir la implementación de las Políticas de ISS;
- Manejar las derogaciones a las Políticas de ISS en su alcance;
- Garantizar que se sigan las buenas prácticas de seguridad;
- Definir campañas específicas de capacitación y concienciación;
- Producir paneles de seguridad locales, analizar indicadores de seguridad y enviarlos al CISO Global;
- Coordinar las acciones de seguridad local;
- Contribuir, con los negocios 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 monitorear auditorías locales de seguridad de la información con el Director Global
  de seguridad de la información;
- Participar en Change Advisory Boards (CAB) para cambios en el sistema de información que impacten 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 alcance del Plan de Continuidad de Negocios.

3.4. COLABORADORES LOCALES DE SEGURIDAD

Además del CISO Global y los OG SOs descritos anteriormente, la organización de la seguridad de la información implica a delegados locales de la seguridad.

Los Colaboradores de la Seguridad OG identifican y supervisan a los delegados locales de la seguridad dentro de las entidades, filiales, departamentos, empresas y donde sea necesario. Los colaboradores locales de seguridad ayudan a los OG SOs en sus misiones, implementan la seguridad de la información en su ámbito o desarrollan proyectos basados en necesidades específicas de seguridad.

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 del contenido para ajustarlo a la estrategia del grupo	27/03/2017
2.1	Cumplimiento de ISS	Actualización de las funciones de seguridad Actualización de la frecuencia de revisión de las políticas	19/12/2019
		Agregar una nueva política operativa al apéndice	19/03/2021
2.2	Cumplimiento de ISS	Enfoque de creación de Políticas adicionales Agregar Requerimientos Publicitarios	
2.3	Cumplimiento de ISS	Revisión Anual Añadir el requisito de tramitar las excepciones	07/04/2022

4.2. APÉNDICE 2: POLÍTICAS OPERATIVAS

Las Políticas Operativas que completan el ISSP Global sobre sujetos de temáticas 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 las trazas informáticas
- Manejo de Medios de Comunicación
- Equipos de los Usuarios
- Seguridad de las Redes
- Seguridad en la Nube
- Desarrollo y Mantenimiento de Aplicaciones
- Relación con los Proveedores
- Gestión de incidentes de Seguridad
- Continuidad de la Actividad