Política Global de Seguridad del Sistema de Información

Grupo SGSI

Versión 2.6
Abril 2025
Público

BUREAU VERITAS

1. Introducción

La Política Global de Seguridad del Sistema de Información (ISSP Global) define el marco de referencia para la seguridad de la información de Bureau Veritas. Destaca los desafíos de seguridad, los objetivos, los principios de gobernanza y los requisitos de seguridad fundamentales que se aplican a toda la organización.
El ISSP Global tiene como objeto asegurar 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 seguridad de la información es un tema vital para Bureau Veritas, ya que la información en todas sus formas es un recurso estratégico del que depende el rendimiento, la sostenibilidad y la capacidad de la organización para desarrollar 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 su sistema de información mediante la implementación de medidas de seguridad adecuadas.
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 asegurar la protección eficaz de la información y la coherencia del Sistema de Gestión de Seguridad de la Información (SGSI).

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, 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 asegurar 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 la capitalización de las medidas de seguridad implementadas y las mejores prácticas en las diferentes entidades y filiales de la organización.

1.2.1. Perímetro organizativo

La 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 soportan la información de Bureau Veritas están incluidos en el Sistema de Gestión de Seguridad de la Información, así como todas los medios destinados a crear, adquirir, procesar, almacenar, distribuir o destruir esta información en o utilizando:

- Equipo de usuario (por ejemplo, computadoras de escritorio y portátiles, teléfonos inteligentes, 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 filiales. Su objetivo es asegurar la aplicabilidad independientemente del contexto técnico, sin dar detalles sobre las tecnologías que deben aplicarse, sino solo los requisitos funcionales y organizativos.

1.2.4. Enfoque

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

- Gestión de Riesgos de Información: las reglas establecidas en cada política deben construirse para gestionar y reducir los riesgos que tienen un impacto significativo en las operaciones del negocio y que amenazan la confidencialidad, integridad, disponibilidad y trazabilidad de la información.
- Cumplimiento: las reglas de seguridad deben imponer la evaluación de los requisitos de cumplimiento de la normativa, los términos contractuales y las normas del sector, así como la implementación de medidas adecuadas para su cumplimiento.
- Objetivos del 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 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:

- **La ISSP Global** (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:** definen las reglas de seguridad de la información por tema que se aplican a Bureau Veritas. Pueden concederse exenciones temporales a entidades o filiales si no puede asegurarse su cumplimiento. Las excepciones deben ser validadas por el CISO Global de Bureau Veritas.
- **Guías, reglas y procedimientos:** documentos operativos, actividades de apoyo, conforme con los requisitos definidos en las reglas de las Políticas Operativas. Estos documentos se pueden definir a nivel de grupo o localmente.

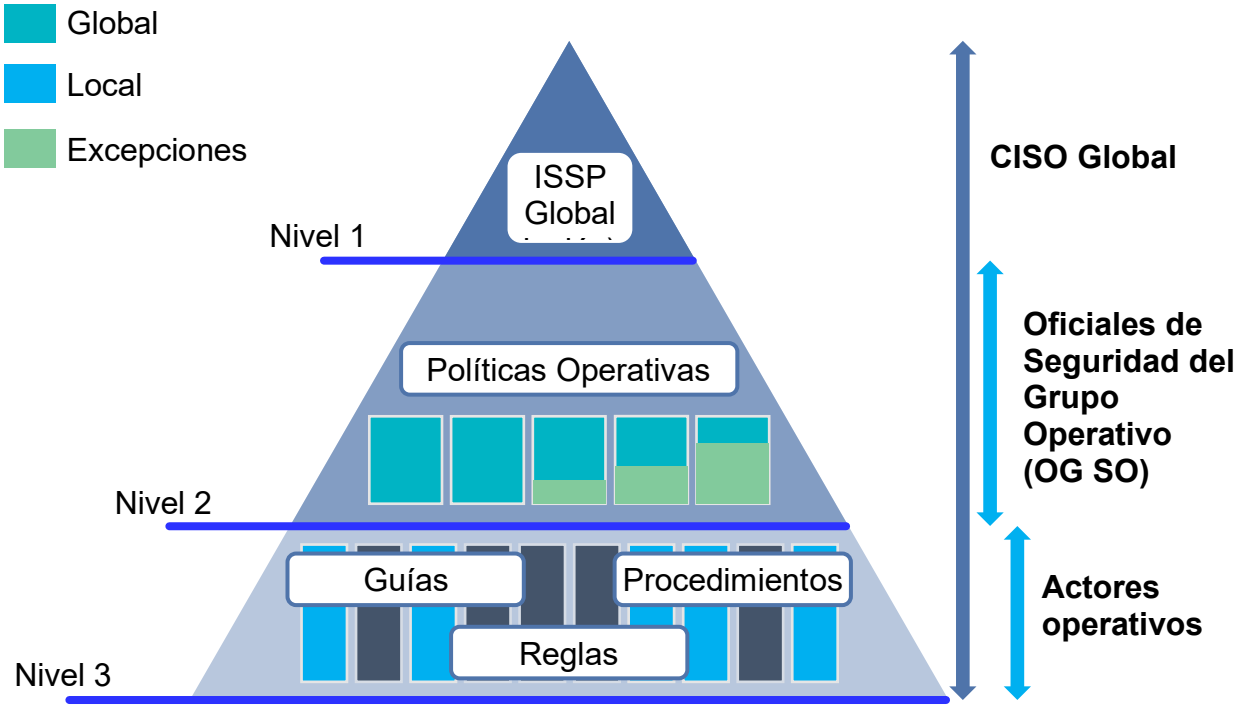

Figura 1- Repositorio documental y responsabilidades.

2.2. Aplicación de la política de seguridad

2.2.1. Ciclo de vida

Con el fin de asegurar la eficacia 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 su retroalimentación y validación.
- **Control y Seguimiento (Check):** esta fase permite identificar impactos en las actividades operativas. Se controla la aplicación de las políticas de ISS.

- **Mantenimiento y Mejora (Act):** Los oficiales de seguridad y otras partes interesadas (por ejemplo, corresponsales de seguridad) identifican las brechas e informan al CISO Global. Se analizan los comentarios para identificar las mejoras necesarias y alimentar la siguiente fase del Plan.

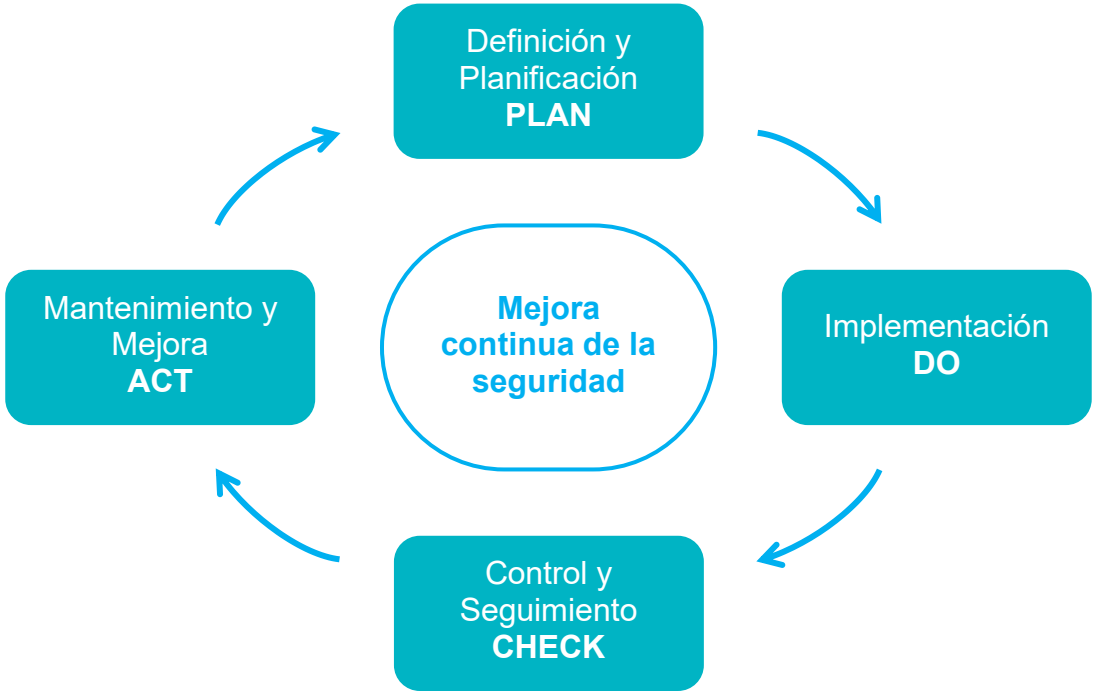

Figura 2- Ciclo de vida de la mejora continua.

La ISSP Global y las políticas operativas 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 ISS actualizadas se presentan para su validación a la Dirección Ejecutiva de Bureau Veritas.

El ciclo de vida completo de las Políticas ISS debe incluirse en el Sistema de Gestión de Seguridad de la Información (SGSI), asegurando su aplicación. Los distintos elementos del SGSI deben formalizarse y documentarse para asegurar la trazabilidad de sus operaciones.

2.2.2. Aplicabilidad

Las políticas de ISS deben aplicarse y hacerse cumplir.

Los incumplimientos de las Políticas de ISS deben estar sujetas a planes formales de acción correctiva con un calendario de finalización definido o excepcionadas.

2.2.3. Publicación

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

Por otra parte, las políticas operativas se publican internamente. Deben ser accesibles únicamente 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 el tratamiento de exenciones y excepciones

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

Las solicitudes de excepción deben ser revisadas y aprobadas por el CISO Global, el equipo de cumplimiento o el Oficial de Seguridad del Grupo Operativo (OG/SO) de la entidad solicitante.

3. Gobernanza de la seguridad del sistema de información

3.1. Visión general de la gobernanza

La gobernanza del sistema de seguridad de la información tiene como objeto 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, Grupo Operativo, Oficial de Seguridad de la Información, etc.).

A través de esta gobernanza, el objeto es estructurar la actividad de la gestión de seguridad del sistema de información de Bureau Veritas, definiendo los procesos pertinentes, promocionando la gestión y proporcionando el material necesario (Políticas de ISS, soportes de formación y concienciación, guías).

La gobernanza también incluye cualquier papel relevante para la promoción 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 Oficial de Seguridad de la Información Global (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 tal, está a cargo del Sistema de Gestión de Seguridad de la Información de Bureau Veritas.

El CISO Global desempeña sus funciones dentro de Bureau Veritas y junto a 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 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 de la gestión de seguridad del sistema de información de Bureau Veritas.
- Definir campañas de formación y sensibilización.
- Aprobar el nombramiento de Oficial de Seguridad del Grupo Operativo (OG/SO).
- Elaborar cuadros de mando globales de seguridad de la información, centralizar indicadores de los OG/SO y realizar análisis globales de la 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 filiales.
- Supervisar el cumplimiento de las políticas de ISS dentro del grupo Bureau Veritas.
- Gestionar las 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 acciones correctivas elaborado con las recomendaciones de las auditorías.
- Aprobar, asesorar y supervisar las auditorías locales de seguridad de la información con el OG/SO.
- Participar en los Comités Asesor de Cambios (CAB), en particular para los cambios con un impacto crítico o importantes en el sistema de información de Bureau Veritas.
- Supervisar la aplicación y el mantenimiento en condiciones operativas del proceso de gestión de incidentes de seguridad de Bureau Veritas y su comprobación periódica, en particular para asegurar la eficacia del plan de gestión de crisis y la unidad de crisis.
- Supervisar la aplicación y el mantenimiento en condiciones operativas del Plan de Continuidad de Negocio (BCP) de Bureau Veritas y su comprobación periódica.

3.3. Oficiales de Seguridad del Grupo Operativo (OG/SO)

3.3.1. Presentación de los OG/SO

Los OG/SO son los garantes de la seguridad y la continuidad del sistema de información de Bureau Veritas a nivel del Grupo Operativo. Son nombrados a nivel del Grupo Operativo 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 asegurar la implementación de iniciativas globales en su respectivo ámbito, especialmente la aplicación de políticas y marcos de cumplimiento.

3.3.2. Asignaciones de los OG/SO

Los OG/SO 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:

- Comunicar información importante al CISO Global.
- Velar por la aplicación de las políticas de ISS.
- Gestionar las excepciones a las políticas de ISS en su alcance.
- Asegurar el cumplimiento de las buenas prácticas de seguridad.
- Definir campañas específicas de formación y sensibilización.
- Elaborar cuadros de mando de seguridad locales, analizar los indicadores de seguridad y envíelos al CISO Global.
- Coordinar las acciones locales de seguridad.
- 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 reglas.
- Aprobar, asesorar y supervisar las auditorías locales de seguridad de la información con el CISO Global.
- Participar en los Comités Asesor 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 (BCP) en su alcance.

3.4. Corresponsales de seguridad locales

Además de los CISO Globales y los Oficiales de Seguridad del Grupo Operativo (OG/SO) descritos anteriormente, la organización de seguridad de la información involucra a Corresponsales de Seguridad locales.

Los Oficiales de Seguridad del Grupo Operativo identifican y supervisan a los Corresponsales de Seguridad locales dentro de las entidades, filiales, departamentos, empresas y donde sea necesario. Los Corresponsales de Seguridad locales asisten a los Oficiales de Seguridad del Grupo Operativo (OG/SO) 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 difícil.

4. Apéndices

4.1. Apéndice 1: Historial de revisiones

Versión	Autor	Descripción	Fecha
1.5	ISS Compliance	Nombramiento del CISO del Grupo	12/01/2017
2.0	ISS Compliance	Actualización de los contenidos para cumplir con la estrategia del grupo	27/03/2017
2.1	ISS Compliance	Actualización de los roles de seguridad. Actualización de la frecuencia de revisión de políticas Adición de una nueva política operativa al apéndice	19/12/2019
2.2	ISS Compliance	Adición de un enfoque de creación de políticas Adición de requisitos de publicación	19/03/2021
2.3	ISS Compliance	Revisión anual Adición de requisitos para la tramitación de las excepciones	07/04/2022
2.4	ISS Compliance	Revisión anual	20/04/2023
2.5	ISS Compliance	Revisión anual	30/04/2024
2.6	ISS Compliance	Revisión Anual Adopción de la norma ISO 27001:2022	09/04/2025
2.6	Fernando Hurtado	Traducción al español	08/08/2025

4.2. Apéndice 2: Aprobadores

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

4.3. Apéndice 3: Políticas Operativas

Título del documento	Nombre del documento
Política Global de Seguridad del Sistema de Información	BV_ISSP_Política Global de Seguridad del Sistema de Información

4.4. Apéndice 4: Políticas Operativas

Las Políticas Operativas que completan el ISSP Global sobre temas específicos 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 redes
- Seguridad en la nube
- Desarrollo y mantenimiento de aplicaciones
- Relación con proveedores
- Gestión de incidentes de seguridad
- Continuidad de la actividad