GLOBAL INFORMATION SYSTEM SECURITY POLICY

STATUS : VALIDATED

VERSION : 2.1

PUBLIC	INTERNAL	RESTRICTED	SECRET
X			

BUREAU VERITAS

Shaping a World of Trust

Aprobadores

Nombre	Cargo
Francois VILJOEN	Senior Vice President, Group CIO
Julien ANICOTTE	Group Chief Information Security Officer

Historia de Revisiones

Versión	Autor	Descripción	Fecha
1.5	ISS Compliance	Appointment of the Group CISO	12/01/2017
2.0	ISS Compliance	Update of the content to comply with group strategy	27/03/2017
2.1	ISS Compliance	Update of the security roles Update of the frequency of policy review Adding la new operational policy to the appendix	19/12/2019

Documentos de Referencia

Título del documento	Versión

Clasificación

Nível	Confidencialidad
C1	Público

INDICE

GLOSARIO

B

BCP: Business Continuity Plan (PCN: Plan de Continuidad de Negócios).

BL: Business Line. (Línea de Negocios)

C

CIO: Chief Information Officer

CISO: Chief Information Security Officer.

G

Global ISSP: Política Global de Seguridad de Sistemas de Información (Global ISSP). Este documento.

I

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

ISS Policies: Políticas ISS. Incluye la ISSP Global y Políticas Operacionales.

L

Local Security Correspondents (Recursos Locales de Seguridad): Se refiere a los recursos profesionales y equipos locales de Seguridad

O

OG: Grupo Operativo.

P

Personal del Proveedor: Se refiere al personal contratado por el Proveedor que actúa en la prestación de servicios para Bureau Veritas.

Políticas ISS: Políticas de Seguridad de la Información que incluyen la Política Global de Sistemas de Información y Políticas Operativas.

Proveedor: Ofertante seleccionado por Bureau Veritas para la ejecución de servicios en el ámbito de un contrato.

S

SGSI: Sistema de Gestión de Seguridad de la Información (Information Security Management System).

Servicios: Todos los servicios entregados por un proveedor para Bureau Veritas, que no se limitan a la asistencia técnica, servicios de mantenimiento y servicios Cloud del tipo SaaS, IaaS o PaaS que pueden ser suministrados en las instalaciones del cliente o de forma virtual.

SO: Security Officer.

1. INTRODUCCIÓN

La Política Global de la Seguridad de Sistemas de Información (PGSSI) define el marco de referencia de la Seguridad de la Información de Bureau Veritas mediante el destaque de objetivos y temas críticos de la Seguridad.

El objetivo de la PGSSI es el de asegurar la protección de la información mediante la aplicación de cuatro criterios de clasificación:

- Disponibilidad;
- Integridad;
- Confidencialidad;
- Trazabilidad.

1.1. EL TEMA VITAL DE LA SEGURIDAD DE LA INFORMACIÓN

La Información escrita y oral, procesada de forma manual o automática, es un recurso estratégico que viabiliza el desempeño, la sustentabilidad y la capacidad de realización de las actividades y negócios de Bureau Veritas.

Para hacer frente a las amenazas maliciosas y no intencionales que puedan afectar la Seguridad de la Información, Bureau Veritas debe proteger de forma eficiente sus sistemas de información mediante la implantación de medidas adecuadas de Seguridad, acorde con los desafíos que se puedan hacer presentes.

Estas medidas de Seguridad deben asegurar el cumplimiento de compromisos contractuales, el cumplimiento de disposiciones legales y regulatorias y la calidad y continuidad de los servicios entregados a los clientes por Bureau Veritas. El resultado práctico de la aplicación de estas medidas es el fortalecimiento de la imagen pública de Bureau Veritas.

1.2. OBJETIVOS EN COMUN PARA UNA PROTECCIÓN EFICAZ

El marco de referencia de la Política Global de la Seguridad de Sistemas de Información está definido por la Política Global de Sistemas de Información (Global ISSP) y sustentado mediante políticas operativas que establecen reglas y responsabilidades de la Gestión de Seguridad de información en lo que atañe a asuntos y temas específicos vinculados a la Seguridad.

Los principios de la gobernanza y las reglas comunes formalizadas en las Políticas de Seguridad de Sistemas de Información (ISS Policies) deben asegurar una protección eficaz de la información y la coherencia del Sistema de Gestión de Seguridad de la Información de

Bureau Veritas. Esos principios y reglas deben fundamentar y servir para perfeccionar las medidas de Seguridad y mejores prácticas implantadas en las diferentes entidades y subsidiarias de la organización.

1.2.1. PERIMETRO ORGANIZACIONAL

Las Políticas Globales de Seguridad de Sistemas de Información deben ser aplicadas a todas las entidades y filiales del grupo BV a nivel mundial.

Las políticas ISS también deben impactar a los proveedores. Estas políticas deben definir principios fundamentales de la Seguridad aplicables a todos los servicios contratados por Bureau Veritas.

Es factible que algunas subsidiarias puedan aplicar Políticas propias de Seguridad considerada la especificidad de las actividades realizadas, el país donde están ubicadas (i.e. restricciones legales locales) o de requisitos contractuales específicos de clientes o proveedores.

1.2.2. PERIMETRO FUNCIONAL

Todos los recursos que soportan la información de Bureau Veritas son parte del Sistema de Gestión de Seguridad de la Información así como todos los medios utilizados para crear, adquirir, procesar, almacenar, distribuir o desechar esa información que se logra mediante el uso de:

- Equipos de usuario (p. ej. computadores desktop y laptop, smartphones, tablets);
- Recursos operativos (p. ej. servidores, impresoras, dispositivos de telecomunicación);
- Software (p. ej. sistemas operacionales, aplicativos de software, bases de datos);
- Suportes físicos (papel);
- Recursos humanos y organizacionales.

1.2.3. PERIMETRO TÉCNICO

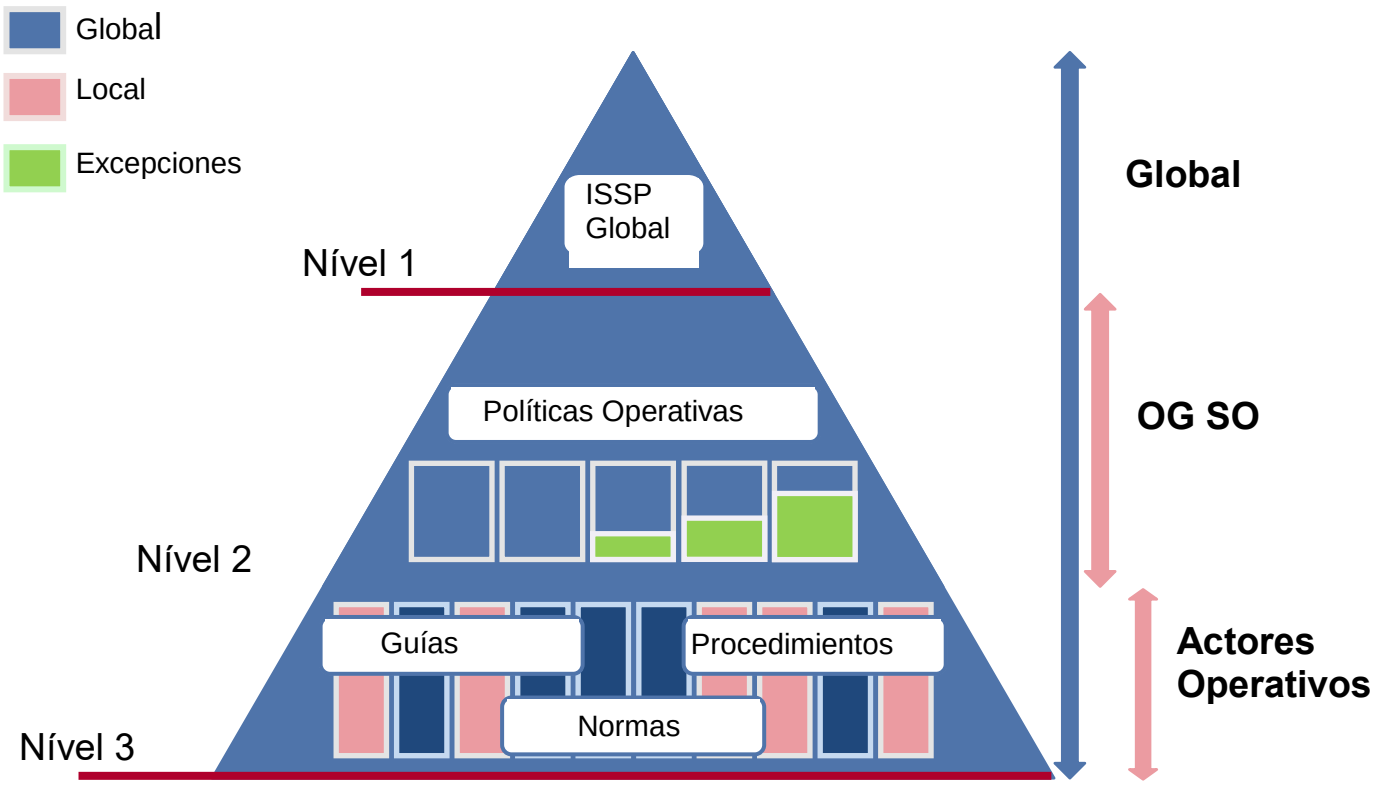
Las Políticas de Seguridad de Sistemas de Información son aplicables a todas las entidades y subsidiarias de Bureau Veritas. El principal objetivo es el de asegurar la aplicabilidad mediante la focalización de requisitos técnicos y organizacionales que son independientes de tecnologías.

2. DOCUMENTACION

2.1. ESTRUCTURA DOCUMENTAL DE LA SEGURIDAD DE LA INFORMACIÓN

La documentación de Seguridad de la información de Bureau Veritas está formalizada en un repositorio documental organizado en tres (3) niveles o capas:

- **Política Global de Sistemas de Información (Global ISSP):** documento de referencia que plantea desafíos, principios de gobernanza y principios fundamentales de la Seguridad de Información para todo el grupo Bureau Veritas de acuerdo a la norma ISO/IEC 27001;
- **Políticas Operativas:** definen reglas de Seguridad de Información conforme temas o asuntos que se aplican a Bureau Veritas. Excepciones temporales pueden ser autorizadas cuando el cumplimiento no pueda ser asegurado. Esas excepciones son validadas por el CISO Global de Bureau Veritas;
- **Guías, normas y procedimientos:** documentos operativos que soportan actividades en el marco de los requisitos establecidos en las reglas de las Políticas Operativas. Estos documentos pueden ser definidos a nivel de grupo o localmente.



2.2. IMPLANTACIÓN DE LA POLÍTICA DE SEGURIDAD

2.2.1. CICLO DE VIDA

Para asegurar la eficiencia y sustentabilidad a través del tiempo de las Políticas de Seguridad de Sistemas de Información (ISS Policies) y de la adecuación con los requisitos de Seguridad de Bureau Veritas, esas políticas deben ser objeto de la mejora continua.

El proceso de mejora continua debe ser cíclico, basado en los principios del PDCA (Plan-Do-Check-Act principle):

- **Definición y planificación (Plan)**: El CISO Global establece un plan de acción que contempla las políticas (ISS Policies) que deben ser revistas y actualizadas, las mejoras requeridas y la fase de comunicación;
- **Implantación (Do)**: El plan de acción establecido en la fase previa es implantado. Mejoras son aplicadas a las políticas (ISS Policies) correspondientes.
- **Control y monitoreo (Check)**: Las políticas revisadas son comunicadas a las personas relevantes para retroalimentación y validación. También, esta fase permite identificar impactos en las operaciones. Cuando necesario, ajustes pueden ser planificados para cumplir con las políticas (ISS Policies) actualizadas. El CISO Global es el responsable de validar las actualizaciones aplicadas.
- **Mantenimiento y mejora (Act)**: Nuevas versiones de las políticas (ISS Policies) son comunicadas con una definición del plazo de aplicación. La comunicación a todas las personas relevantes es asegurada (i.e. OG Security Officers, recursos locales de Seguridad).

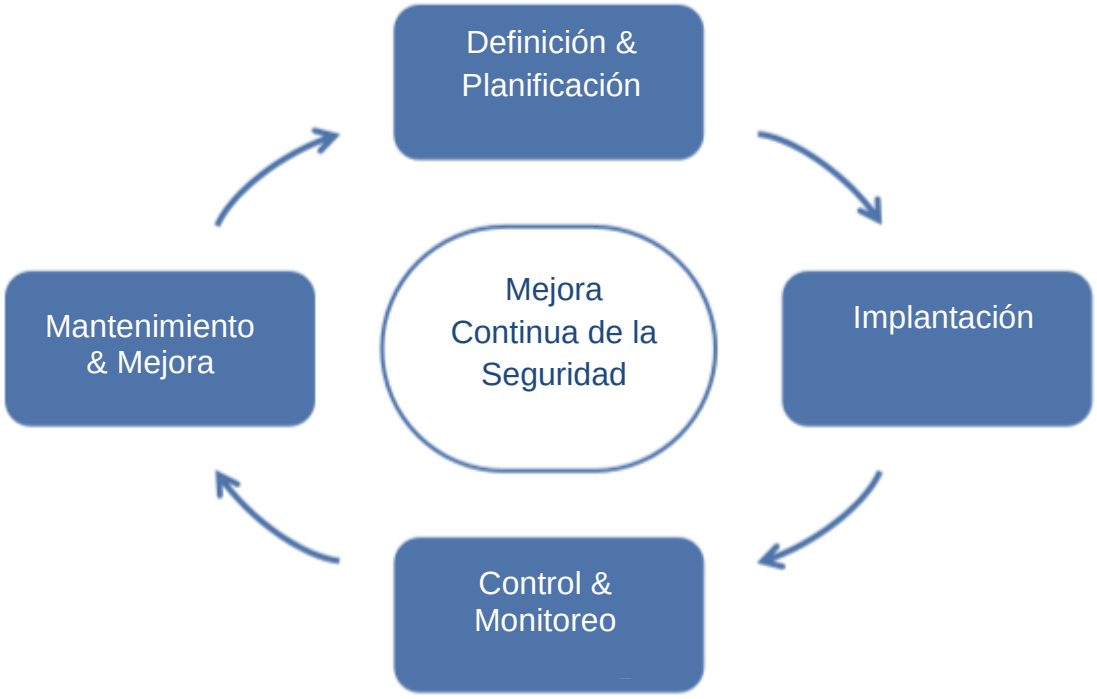


Figura 2 – Ciclo de vida de la Mejora Contínua

La Política Global de Sistemas de Información (Global ISSP) y las políticas operativas deben ser revisadas anualmente. La solicitud de actualizaciones, derivadas de necesidades internas o de factores externos, es administrada y validada por el CISO Global. Las políticas actualizadas son presentadas para validación al Comité Ejecutivo de Bureau Veritas.

El ciclo de vida de las políticas (ISS Policies) debe ser parte del Sistema de Gestión de Seguridad de la Información (SGSI) para asegurar una implantación eficaz. Los componentes del SGSI deben ser formalizados y documentados para asegurar la trazabilidad durante la operación.

2.2.2. APLICABILIDAD

Las políticas (ISS Policies) deben ser implantadas y aplicadas de forma sistemática. El no cumplimiento de las políticas (ISS Policies) debe ser objeto de planes de acción correctiva con plazos definidos para la realización o derogación.

3. GOBERNANZA DEL SISTEMA DE INFORMACIÓN

3.1. VISIÓN GENERAL DE LA GOBERNANZA

El principal objetivo de la gobernanza de la Seguridad del Sistema de Información es la definición de la estructura del flujo de Seguridad de la Información de Bureau Veritas y los roles y responsabilidades de todos actores relevantes que hacen parte de esa estructura (CISO Global, OG Security Officers, recursos profesionales y equipos de Seguridad de la Información, etc.)

A través de esta gobernanza, la meta es canalizar la actividad del flujo de la Seguridad del Sistema de Información mediante la definición de procesos relevantes, vitalizando el flujo y proveyendo el material necesario (Políticas ISS, capacitación y soporte a la concientización, guías).

La gobernanza también incluye cualquier rol relevante para la animación de la Seguridad del Sistema de Información dentro de las actividades de negocios, funciones de control, gestión de proyectos y Dirección.

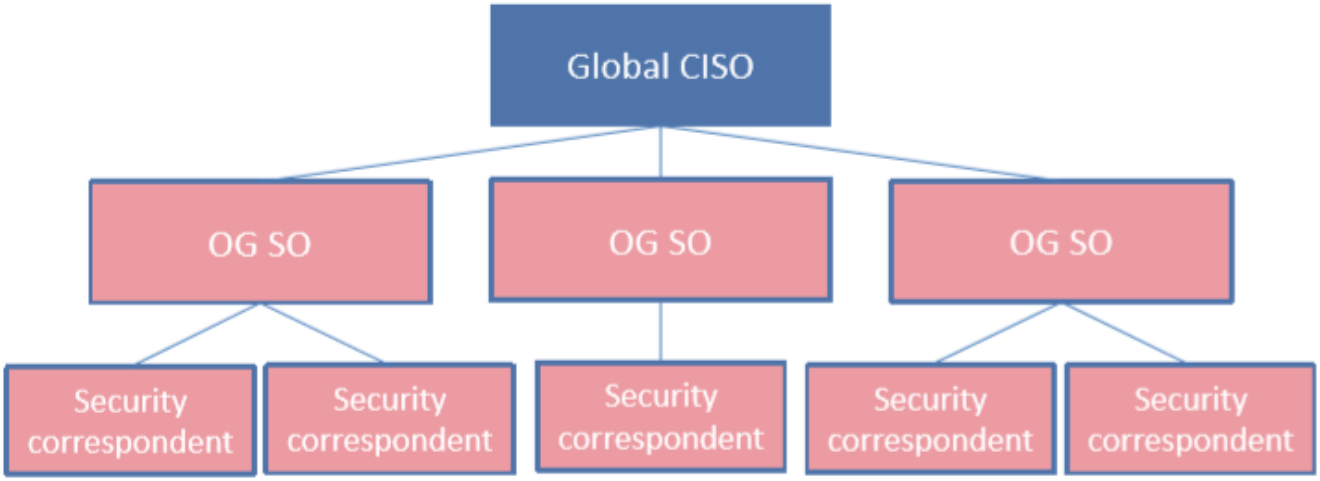


Figure 3 - Organización de la gobernanza de ISS de Bureau Veritas

3.2. EL CISO GLOBAL DE BUREAU VERITAS

3.2.1. PRESENTACIÓN DEL CISO GLOBAL

El CISO Global de Bureau Veritas es el responsable de asegurar y garantizar la Seguridad y Continuidad del Sistema de Información del grupo Bureau Veritas, sus entidades y filiales. En esa condición el CISO Global es el responsable del Sistema de Gestión de Seguridad de la Información de Bureau Veritas.

El CISO Global desarrolla sus actividades dentro de Bureau Veritas y actúa en conjunto con Proveedores, Clientes y terceros (i.e. organizaciones gubernamentales, organismos de certificación).

3.2.2. RESPONSABILIDADES DEL CISO GLOBAL

El CISO GLOBAL es el responsable de la Gestión y del mantenimiento del flujo operativo de la Seguridad de la Información. Las responsabilidades del cargo incluyen:

- Formalización, coordinación y mantenimiento en condiciones operativas la organización del flujo de Seguridad de sistemas de información de Bureau Veritas;
- Definición de campañas de capacitación y de concientización;
- Aprobación del nombramiento de OG Security Officers;
- Elaborar tableros de Gestión de Seguridad global, centralizar los indicadores elaborados por los OG Security Officers y realizar análisis global del rendimiento de la seguridad de los sistemas de información.
- Elaborar y actualizar Políticas (ISS Policies);
- Obtener la aprobación ejecutiva de Políticas (ISS Policies);
- Asegurar la aplicación y acompañar la implantación de Políticas (ISS Policies) en las entidades y subsidiarias del grupo Bureau Veritas;
- Monitorear el cumplimiento de Políticas (ISS Policies) en el grupo Bureau Veritas;
- Gestionar excepciones en lo que atañe al cumplimiento Políticas (ISS Policies) que posean impacto crítico u global;
- Planificar y evaluar la realización de auditorías del Sistema de Información en lo que atañe a la Seguridad y acompañar los planes de acción correctiva derivados de las recomendaciones de la auditoria;
- Aprobar, asesorar y acompañar la realización de auditorías locales de Seguridad de la Información con el OG Security Officer;
- Participar del Comité de Gestión de Cambios (CAB) para acompañar Cambios de impacto crítico o grandes al Sistema de Información Bureau Veritas;
- Monitorear la implantación y el mantenimiento (en condiciones operativas) y pruebas regulares del proceso de Gestión de Incidentes de Bureau Veritas para asegurar la eficiencia del plan de Gestión de Crisis y de la unidad operativa de crisis;

- Monitorear la implantación y el mantenimiento (en condiciones operativas) y pruebas regulares del proceso de Continuidad de Negócios de Bureau Veritas.

3.3. OG SECURITY OFFICERS (OG SO) DE BUREAU VERITAS

3.3.1. PRESENTACIÓN DEL OG SO

El OG Security Officers son responsables de garantizar la Seguridad y continuidad del sistema de información de Bureau Veritas al nivel de OG. Ellos son designados a nivel OG y serán socios confiables del equipo central.

Las principales responsabilidades del OG Security Officer son la realización y supervisión de actividades de Seguridad de la información de equipos técnicos y de negocio y asegurar la implantación de iniciativas globales en lo que atañe a la aplicación de políticas y marcos de referencia.

3.3.2. RESPONSABILIDADES DEL OG SO

Los OG Security Officer de Bureau Veritas son responsables de la implantación del Sistema de Gestión de Seguridad de la Información y del mantenimiento operativo del sistema en el ámbito del alcance establecido. Las responsabilidades de la función incluyen:

- Reportar informaciones importantes al Global CISO;
- Asegurar la implantación de Políticas (ISS Policies);
- Administrar excepciones en lo que atañe al cumplimiento de Políticas (ISS Policies) en sus áreas de alcance;
- Asegurar la aplicación de Buenas Prácticas de Seguridad;
- Definir campañas focalizadas de capacitación y de concientización;
- Generar tableros de control locales de seguridad, analizar indicadores de seguridad y enviarlos al CISO global.
- Coordinar acciones locales de Seguridad;
- Colaborar con áreas de negocio y de Tecnologia de la Información en la conversión de Políticas operativas en guías, normas y procedimientos técnicos (i.e. instalación, operación, gestión de eventos),
- Aprobar, asesorar y monitorear la realización de auditorías locales de Seguridad de la información con el CISO Global;
- Participar en el Comité de Gestión de Cambios (CAB) para cambios de los sistemas de información que impactan su alcance;
- Asegurar el mantenimiento de la operatividad del proceso de Gestión de Incidentes de seguridad que están dentro de su alcance de actuación;
- Asegurar el mantenimiento en condiciones operativas del plan de Continuidad de Negocios dentro de su alcance de actuación.

3.4. LOCAL SECURITY CORRESPONDENTS (RECURSOS LOCALES DE SEGURIDAD)

Más allá del CISO Global y de los OG Security Officers, la organización de Seguridad de la Información contempla la participación de recursos profesionales y equipos locales de Seguridad.

El OG Security Officer debe (donde necesario) identificar y supervisar esos recursos dentro de las entidades, filiales, departamentos y unidades de negocio de Bureau Veritas.

Esos recursos de Seguridad auxilian el OG Security Officer en la realización de su misión, implementan y mantienen la Seguridad de la Información dentro de su alcance o desarrollan proyectos focalizados en necesidades específicas de Seguridad.

4. APÉNDICE

4.1. APÉNDICE 1: POLÍTICAS OPERACIONALES

Las políticas operativas de la Política Global de Sistemas de Información (Global ISSP) que tratan de áreas temáticas son:

- Seguridad de Recursos Humanos (Human Resource Security).
- Clasificación de Recursos de Tecnologia de la Información (Classification of IT Resources).
- Control del Acceso Lógico (Logical Access Control).
- Seguridad Física (Physical Security).
- Seguridad de las Operaciones (Operations Security).
- Gestión de logs (Management of IT Traces).
- Manejo de Medios Digitales (Media Handling).
- Equipos de Usuarios (Users' Equipment).
- Seguridad de las Redes (Network Security).
- Seguridad en la nube (Cloud Security)
- Desarrollo y Mantenimiento de Aplicaciones (Development and Maintenance of Applications)
- Relación con proveedores (Suppliers Relationship).
- Gestión de Incidentes de Seguridad (Management of Security Incidents).
- Continuidad de las Actividades (Activity Continuity).