

Política Global de Segurança do Sistema de Informação SGSI do Grupo

Versão 2.6
Abril de 2025
Público



**BUREAU
VERITAS**

1. Introdução

A Política Global de Segurança do Sistema de Informação (Global ISSP) define a estrutura de referência para a segurança da informação do Bureau Veritas. Ele destaca os desafios de segurança, objetivos, princípios de governança e requisitos fundamentais de segurança que se aplicam a toda a organização. O ISSP Global tem como objetivo garantir a proteção da informação através dos quatro critérios de classificação: Disponibilidade, Integridade, Confidencialidade e Rastreabilidade.

1.1. Segurança da informação, uma questão vital

A segurança da informação é uma questão vital para o Bureau Veritas, pois a informação em todas as suas formas é um recurso estratégico do qual dependem o desempenho, a sustentabilidade e a capacidade de desenvolver atividades e resultados da organização. Para lidar com ameaças acidentais e maliciosas que possam afetar a segurança de seu sistema de informação, o Bureau Veritas deve proteger seu sistema de informação implementando medidas de segurança adequadas.

A estrutura do Sistema de Segurança da Informação do Bureau Veritas é definida pelo ISSP Global, apoiado por Políticas Operacionais que detalham regras e responsabilidades relativas à gestão da segurança da informação em temas específicos. Os princípios de governança e regras comuns formalizados nas Políticas de SGI devem garantir a proteção efetiva das informações e a coerência do Sistema de Gestão de Segurança da Informação (SGSI).

1.2. Objetivos comuns para uma proteção eficaz

A estrutura do Sistema de Segurança da Informação do Bureau Veritas é definida pelo ISSP Global, apoiado por Políticas Operacionais que detalham regras e responsabilidades relativas à gestão da segurança da informação em temas específicos.

Os princípios de governança e regras comuns formalizados nas Políticas de ISS devem garantir a proteção efetiva das informações no âmbito do Bureau Veritas e a coerência do sistema de gestão da segurança da informação. Além disso, devem permitir capitalizar as medidas de segurança implementadas e as melhores práticas nas diferentes entidades e subsidiárias da organização.

1.2.1. Perímetro organizacional

O ISSP Global deve ser aplicado a todas as entidades e subsidiárias do grupo Bureau Veritas em todo o mundo. As Políticas da ISS também devem ter impacto sobre os Fornecedores. Essas políticas devem definir princípios fundamentais de segurança aplicáveis aos serviços contratados pelo Bureau Veritas com Fornecedores. Algumas subsidiárias ou entidades do Bureau Veritas podem estar sujeitas a políticas de segurança dedicadas e específicas devido à sua atividade, ao país em que estão localizadas (por exemplo, restrições legais locais), aos requisitos contratuais do Cliente ou dos Fornecedores.

1.2.2. Perímetro funcional

Todos os recursos que dão suporte às informações do Bureau Veritas estão incluídos no Sistema de Gerenciamento de Segurança da Informação, bem como todas as formas destinadas a criar, adquirir, processar, armazenar, distribuir ou destruir essas informações ou usando:

- . Equipamento do usuário (por exemplo, computadores desktop e laptop, smartphones, tablets).
- . Recursos operacionais (por exemplo, servidores, impressoras, dispositivos de telecomunicações).
- . Software (por exemplo, software operacional, bancos de dados).
- . Suporte de papel.
- . Recursos humanos e organizacionais.

1.2.3. Perímetro técnico

As Políticas de ISS devem ser implementadas pelo grupo Bureau Veritas e todas as suas entidades e subsidiárias. Eles visam garantir a aplicabilidade independentemente do contexto técnico, não fornecendo detalhes sobre as tecnologias a serem implementadas, mas apenas os requisitos funcionais e organizacionais.

1.2.4. Aproximação

Além das melhores práticas do setor, as políticas de ISS devem considerar o seguinte:

- . Gerenciamento de riscos de informações: as regras estabelecidas em cada política devem ser construídas para gerenciar e reduzir riscos que tenham um impacto significativo nas operações de negócios e ameacem a confidencialidade, integridade, disponibilidade e rastreabilidade das informações.

- . Conformidade: as regras de segurança devem impor a avaliação dos requisitos de conformidade com regulamentos, termos contratuais, padrões do setor, bem como a implementação de medidas adequadas para cumprir.

- . Objetivos de negócios: As políticas de ISS, bem como o apoio à governança, devem cooperar e coordenar com as empresas para alinhar a estratégia de segurança com os objetivos e a estratégia do Bureau Veritas: resiliência e proteção de dados.

2. Documentação da ISS

2.1. Estrutura da documentação de segurança do sistema de informação

A documentação de segurança da informação do Bureau Veritas é formalizada como um repositório documental de três níveis:

- . **O ISSP Global** (documento atual): documento de referência, estabelecendo desafios, princípios de governança e princípios fundamentais de segurança da informação para todo o grupo Bureau Veritas, em consonância com a ISO 27001.

- . **Políticas Operacionais:** definir regras de segurança da informação por tema que se aplica ao Bureau Veritas. Podem ser concedidas derrogações temporárias a entidades ou filiais se o cumprimento não puder ser assegurado. Eles são validados pelo CISO Global do Bureau Veritas.

- . **Guias, normas e procedimentos:** documentos operacionais, atividades de suporte, em conformidade com os requisitos definidos nas regras das Políticas Operacionais. Esses documentos podem ser definidos no nível do grupo ou localmente.

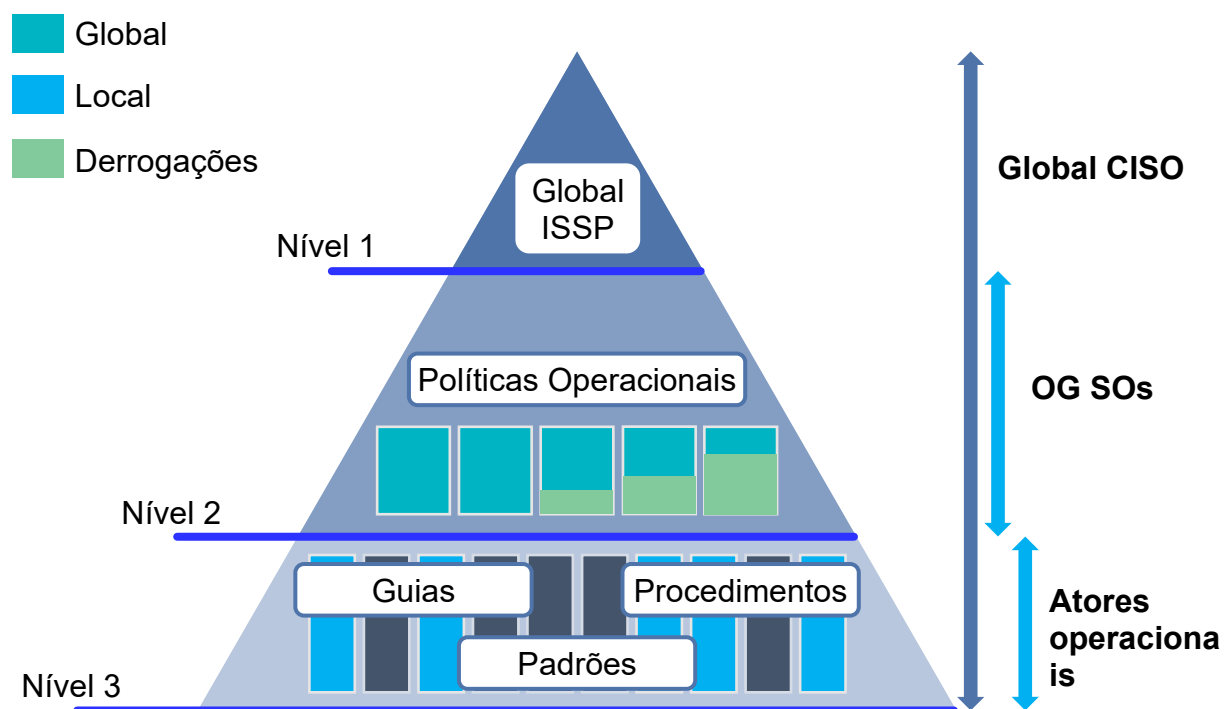


Figura 1- Repositório documental e responsabilidades.

2.2. Aplicação da política de segurança

2.2.1. Ciclo de vida

A fim de garantir a eficiência e sustentabilidade das Políticas da ISS ao longo do tempo e sua adequação aos requisitos de segurança do Bureau Veritas, as Políticas da ISS devem estar sujeitas a melhorias contínuas.

Esse processo de melhoria contínua deve ser cíclico, baseado no princípio Plan-Do-Check-Act (PDCA):

- . **Definição e Planejamento (Plan):** o CISO Global estabelece um plano de ação incluindo as Políticas de ISS para atualizar, as melhorias necessárias e a fase de comunicação.

- . **Implementação (Do):** o plano de ação definido na fase anterior é implementado. Melhorias são aplicadas às Políticas de ISS correspondentes; As políticas atualizadas são comunicadas às pessoas relevantes para feedback e validação.

. **Controle e Monitoramento (Check):** esta fase permite identificar impactos nas atividades operacionais. A aplicação das políticas da ISS é controlada.

. **Manutenção e aprimoramento (Act):** Os oficiais de segurança e outras partes interessadas (por exemplo, correspondentes de segurança) identificam os GAPs e informam o CISO global. O feedback é analisado para identificar as melhorias necessárias e alimentar a próxima fase do Plano.

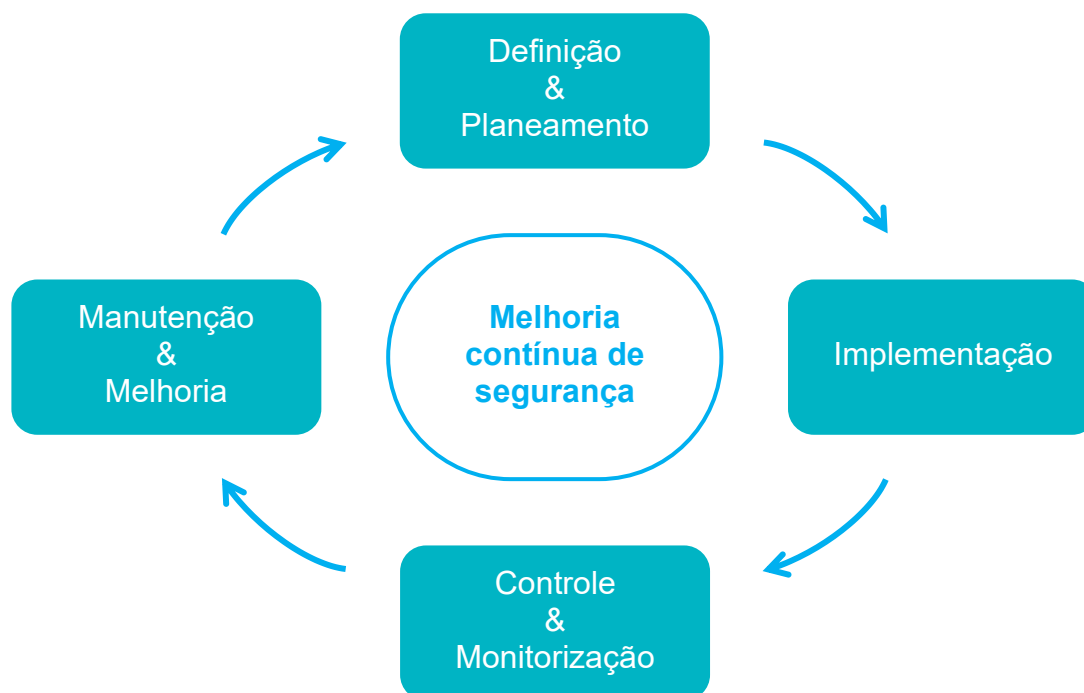


Figura 2- Ciclo de vida de melhoria contínua.

O ISSP Global e as políticas operacionais devem ser revisados pelo menos uma vez por ano. As solicitações de atualizações, decorrentes de necessidades internas ou fatores externos, são centralizadas e validadas pelo CISO Global. As Políticas de ISS atualizadas são submetidas para validação à Gerência Executiva do Bureau Veritas.

Todo o ciclo de vida das Políticas de ISS deve ser incluído no Sistema de Gestão de Segurança da Informação (SGSI), garantindo a sua implementação. Os vários elementos do SGSI devem ser formalizados e documentados para garantir a rastreabilidade de suas operações.

2.2.2. Aplicabilidade

As Políticas da ISS devem ser implementadas e aplicáveis.

As não conformidades com as Políticas ISS devem estar sujeitas a planos formais de ação corretiva com um cronograma de conclusão definido ou derrogações.

2.2.3. Publicação

A Política Global de Segurança do Sistema de Informação deve ser publicada publicamente no site da empresa, a fim de mostrar claramente o compromisso do Bureau Veritas em proteger suas informações, bem como as informações dos clientes.

As políticas operacionais, por outro lado, são publicadas internamente. Eles devem ser acessíveis apenas para todos os usuários do Bureau Veritas.

Cada atualização das políticas deve ser seguida de uma comunicação às partes interessadas relevantes para informá-las sobre as novas mudanças.

2.2.4. Procedimentos para o tratamento de isenções e exceções

Espera-se que todos os componentes do Sistema de Informação do Bureau Veritas estejam em conformidade com as políticas e padrões da ISS. No entanto, em vários casos, o cumprimento de algumas regras não pode ser alcançado por vários motivos. O procedimento de derrogação para gerenciar, documentar e monitorar essas isenções e exceções deve ser formalizado e implementado.

As solicitações de derrogação devem ser analisadas e aprovadas pelo CISO Global, equipe de conformidade ou OG/SO da entidade solicitante.

3. Governança da Segurança do Sistema de Informação

3.1. Visão geral da governança

A governança do sistema de segurança da informação visa definir a estrutura do fluxo de segurança da informação do Bureau Veritas, bem como as funções e responsabilidades de todas as pessoas relevantes que compõem essa estrutura (CISO Global, OG SOs, Equipe de Segurança da Informação etc.).

Por meio dessa governança, o objetivo é enquadrar a atividade do fluxo de segurança do sistema de informação do Bureau Veritas, definindo processos relevantes, animando o fluxo e fornecendo o material necessário (Políticas de ISS, suportes de treinamento e conscientização, guias).

A governança também inclui qualquer papel relevante para a animação da segurança do sistema de informação dentro das atividades de negócios, funções de controle, propriedade e gerenciamento de projetos.



Figura 3 - Organização da governança do ISS do Bureau Veritas.

3.2. O Diretor Global de Segurança da Informação (CISO Global) do Bureau Veritas

3.2.1. Apresentação do CISO Global

O CISO Global do Bureau Veritas é o garantidor da segurança e da continuidade do sistema de informação do grupo Bureau Veritas, suas entidades e suas subsidiárias. Como tal, eles são responsáveis pelo Sistema de Gestão de Segurança da Informação do Bureau Veritas.

O CISO Global cumpre suas funções dentro do Bureau Veritas e ao lado de fornecedores, clientes e terceiros externos (por exemplo, entidades governamentais, organismos de certificação).

3.2.2. Atribuições do CISO Global

O CISO Global do Bureau Veritas supervisiona o Sistema de Gestão de Segurança da Informação da organização e sua manutenção em condições operacionais. Como parte dessas funções, suas missões são:

- . Formalizar, coordenar e manter em condições operacionais a organização do fluxo de segurança do sistema de informação do Bureau Veritas.
- . Definir campanhas de treinamento e conscientização.
- . Aprovar a nomeação de OG/SO.
- . Produzir dashboards de segurança global, centralizar indicadores de OG/SO's e realizar análises globais de informações.
- . Desenvolver e atualizar as Políticas de ISS.
- . Obter a aprovação da Gerência Executiva para as Políticas da ISS.
- . Aplicar e acompanhar a implementação das Políticas da ISS dentro do grupo Bureau Veritas, suas entidades e subsidiárias.
- . Monitorar a conformidade com as Políticas da ISS dentro do grupo Bureau Veritas.
- . Lidar com derrogações às políticas de ISS com escopo global ou impacto crítico.
- . Planejar e supervisionar auditorias no sistema de informação para fins de segurança e seguir o plano de ação corretiva construído com as recomendações das auditorias.
- . Aprovar, aconselhar e monitorar auditorias locais de segurança da informação com o OG SO.
- . Participar de Conselhos Consultivos de Mudança (CAB), particularmente para mudanças com impacto crítico ou grande no sistema de informação do Bureau Veritas.
- . Monitorar a implementação e a manutenção em condições operacionais do processo de gerenciamento de incidentes de segurança do Bureau Veritas e seus testes regulares, particularmente para garantir a eficiência do plano de gerenciamento de crises e da unidade de crise.
- . Monitorar a implementação e a manutenção em condições operacionais do Plano de Continuidade de Negócios do Bureau Veritas e seus testes regulares.

3.3. Oficiais de Segurança do Grupo Operacional (OG/SO)

3.3.1. Apresentação do OG/SO

Os Oficiais de Segurança do OG são os garantidores da segurança e da continuidade do sistema de informação do Bureau Veritas no nível do OG. Eles são nomeados no nível OG e serão parceiros de confiança para a equipe central.

Suas principais atribuições são a execução e supervisão das atividades de segurança da informação em seu escopo dentro das empresas e equipes técnicas, mas também garantir a implementação de iniciativas globais em seu respectivo escopo, especialmente a aplicação de políticas e estruturas de compliance.

3.3.2. Atribuições do OG/SO

Os Oficiais de Segurança OG do Bureau Veritas supervisionam a implementação do Sistema de Gestão de Segurança da Informação e sua manutenção em condições operacionais dentro de seus respectivos escopos. Como parte dessas funções, suas missões são:

- . Relatar informações importantes ao CISO global.
- . Impor a implementação das políticas de ISS.
- . Lidar com derrogações às Políticas ISS em seu escopo.
- . Certificar-se de que as boas práticas de segurança sejam seguidas.
- . Definir campanhas dedicadas de treinamento e conscientização.
- . Produzir dashboards de segurança locais, analisar indicadores de segurança e envia-los ao CISO global.
- . Coordenar ações de segurança locais.
- . Contribuir, junto às empresas e Departamentos de TI/SI, para a transcrição das Políticas Operacionais em procedimentos técnicos (e.g. instalação, operação, tratamento de eventos), guias e normas.
- . Aprovar, aconselhar e monitorar auditorias locais de segurança da informação com o CISO global.
- . Participar dos Conselhos Consultivos de Mudança (CAB) para mudanças no sistema de informação que afetam seu escopo.
- . Garantir a manutenção em condições operacionais do processo de gerenciamento de incidentes de segurança em seu escopo.

. Garantir a manutenção em condições operacionais do Plano de Continuidade de Negócios em seu escopo.

3.4. Correspondentes de segurança locais

Além dos CISO globais e OG SOs descritos acima, a organização de segurança da informação envolve correspondentes de segurança locais.

Os Oficiais de Segurança da OG identificam e supervisionam os correspondentes de segurança locais dentro de entidades, subsidiárias, departamentos, empresas e sempre que necessário. Os correspondentes de Segurança Local auxiliam os OG SOs em suas missões, implementam a segurança da informação em seu escopo ou desenvolvem projetos com base em necessidades específicas de segurança.

3.5. Contato com autoridades e grupos de interesses especiais

Quando apropriado, o Bureau Veritas e suas subsidiárias estabelecem e mantêm contato com as autoridades competentes.

Além disso, quando relevante, o Bureau Veritas deve estabelecer e manter contato também com grupos de interesses especiais ou outros fóruns especializados em segurança e associações profissionais.

Ter estabelecido canais de contato com as partes mencionadas acima pode ser necessário para conformidade (por exemplo, notificar as autoridades relevantes sobre uma violação de dados). Além disso, grupos de interesse especial ou outros fóruns especializados em segurança e associações profissionais podem ajudar a empresa a antecipar o desenvolvimento do campo da segurança cibernética e se preparar para mudanças e evoluções. Essas conexões também podem ser úteis caso seja necessário suporte / aconselhamento quando confrontado com uma situação desafiadora.

4. Apêndices

4.1. Apêndice 1: Histórico de revisões

Versão	Autor	Descrição	Data
1.5	ISS Compliance	Nomeação do CISO do Grupo	12/01/2017
2.0	ISS Compliance	Atualização do conteúdo para atender à estratégia do grupo	27/03/2017
2.1	ISS Compliance	Atualização dos direitos de acesso Atualização da frequência de revisão de política Adicionando uma nova política operacional ao apêndice	19/12/2019
2.2	ISS Compliance	Adicionando abordagem de criação de políticas Adicionando requisitos de publicação	19/03/2021
2.3	ISS Compliance	Revisão anual Adicionando o requisito para o tratamento das derrogações	07/04/2022
2.4	ISS Compliance	Revisão anual	20/04/2023
2.5	ISS Compliance	Revisão anual	30/04/2024
2.6	ISS Compliance	Revisão Anual Adoção da ISO 27001:2022	09/04/2025

4.2. Apêndice 2: Aprovadores

Nome	Posição
François VILJOEN	Vice-presidente sênior, CIO do grupo
Julien ANICOTTE	Diretor de Segurança da Informação do Grupo (CISO)

4.3. Apêndice 3: Políticas Operacionais

Título do documento	Nome do documento
Política Global de Segurança do Sistema de Informação	BV_ISSP_Política Global de Segurança do Sistema de Informação

4.4. Apêndice 4: Políticas Operacionais

As Políticas Operacionais que completam o ISSP Global sobre assuntos temáticos para o Bureau Veritas são:

- . Segurança de Recursos Humanos
- . Classificação da Informação
- . Controle de acesso lógico
- . Segurança física
- . Segurança de operações
- . Gerenciamento de logs de TI

- . Manuseio de mídia
- . Equipamento dos Usuários
- . Segurança de rede
- . Segurança na nuvem
- . Desenvolvimento e Manutenção de Aplicações
- . Relacionamento com Fornecedores
- . Gestão de Incidentes de Segurança
- . Continuidade da atividade