GLOBAL INFORMATION SYSTEM SECURITY POLICY

STATUS : VALIDATED

VERSION : 2.1

PUBLIC	INTERNAL	RESTRICTED	SECRET
X			

BUREAU VERITAS

Shaping a World of Trust

Aprovação

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

Histórico da Revisão

Versão	Autor	Descrição	Data
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 a new operational policy to the appendix	19/12/2019

Documentos de Referencia

Título de documento	Versão

Classificação

Nível	Confidencialidade
C1	Público

SUMMARY

GLOSSÁRIO

B

BCP: Business Continuity Plan (PCN: Plano de Continuidade de Negócios).

BL: Business Line. (Linha de Negócios)

C

CIO: Chief Information Officer

CISO: Chief Information Security Officer.

F

Fornecedor: Ofertante selecionado por Bureau Veritas para a realização de serviços no âmbito de um contrato.

G

Global ISSP: Política Global de Sistemas de Informação (Global ISSP). Este documento.

O

OG: Grupo Operacional.

P

Pessoal do Fornecedor: Refere-se a pessoal contratado pelo Fornecedor que atua na prestação de serviços a Bureau Veritas.

Políticas ISS: Políticas de Segurança da Informação. Incluem Política Global de Sistemas de Informação e Políticas Operacionais.

S

SGSI: Sistema de Gestão de Segurança da Informação Information Security Management System.

Serviços: Todos os serviços fornecidos por Bureau Veritas, que não se limitam a assistência técnica, serviços de manutenção e serviços Cloud do tipo SaaS, IaaS or PaaS que podem ser fornecidos nas instalações do cliente ou de forma virtualizada.

SO: Security Officer.

Local Security Correspondents (Recursos Locais de Segurança): Refere-se recursos profissionais e equipes locais de segurança

1. INTRODUÇÃO

A Política Global da Segurança de Sistemas de Informação (PGSSI) estabelece o marco de referencia da Segurança da Informação de Bureau Veritas mediante o destaque a objetivos e questões críticas da segurança.

O objetivo da PGSSI é o de assegurar a proteção da informação mediante a aplicação de quatro critérios de classificação, a saber:

- Disponibilidade;
- Integridade;
- Confidencialidade;
- Rastreabilidade.

1.1. A QUESTÃO VITAL DE SEGURANÇA DA INFORMAÇÃO

A Informação escrita e oral, processada de forma manual ou automática, é um recurso estratégico que viabiliza o desempenho, a sustentabilidade e a capacidade de realização das atividades e resultados de negócio do Bureau Veritas.

Para lidar com ameaças maliciosas e não intencionais que possam afetar a Segurança da Informação, o Bureau Veritas deve proteger de forma eficiente seus ativos de informação mediante a implantação de medidas adequadas de segurança, acorde com os desafios que possam se apresentar.

Essas medidas de segurança devem assegurar o atendimento de compromissos contratuais, o atendimento de disposições legais e regulatórias bem como a qualidade e continuidade dos serviços entregues aos clientes por Bureau Veritas. O resultado prática da aplicação dessas medidas é o fortalecimento da imagem pública de Bureau Veritas.

1.2. OBJETIVOS EM COMUM PARA UMA PROTEÇÃO EFICAZ

O marco de referencia da Política Global da Segurança de Sistemas de Informação é definido pela Política Global de Sistemas de Informação (Global ISSP) e sustentado mediante políticas operacionais que estabelecem regras e reponsabilidades da gestão de segurança de informação de assuntos e questões específicas vinculadas à segurança.

Os princípios da governança e as regras comuns formalizadas nas Politicas de Segurança de Sistemas de Informação (ISS Policies) devem assegurar uma proteção eficaz da informação e a coerência do Sistema de Gestão de Segurança da Informação de Bureau Veritas. Esses

princípios e regras devem fundamentar e servir para aperfeiçoar as medidas de segurança e melhores práticas implantadas nas diferentes entidades e organizações.

1.2.1. PERIMETRO ORGANIZACIONAL

As Politicas de Segurança de Sistemas de Informação devem impactar todos os Fornecedores. Essas políticas devem definir princípios fundamentais de segurança aplicáveis a todos os serviços contratados por Bureau Veritas. É factível que algumas subsidiárias devam aplicar politicas de segurança especificas dada a atividade realizada e o país onde estão sediadas (i.e. restrições legais locais) ou devido a requisitos contratuais específicos do cliente ou de fornecedores.

1.2.2. PERIMETRO FUNCIONAL

Todos os recursos que suportam a informação de Bureau Veritas fazem parte do Sistema de Gestão de Segurança da Informação bem como todos os meios utilizados par criar, adquir, processar, armazenar, distribuir ou descartar essa informação mediante a utilização de:

- Equipamentos de usuário (i.e. computadores desktop laptop, smartphones, tablets);
- Recursos operacionais (i.e. servidores, impressoras, dispositivos de telecomunicação);
- Software (e.g. sistemas operacionais, aplicações, bases de dados);
- Suportes físicos (papel);
- Recursos humanos e organizacionais.

1.2.3. PERIMETRO TÉCNICO

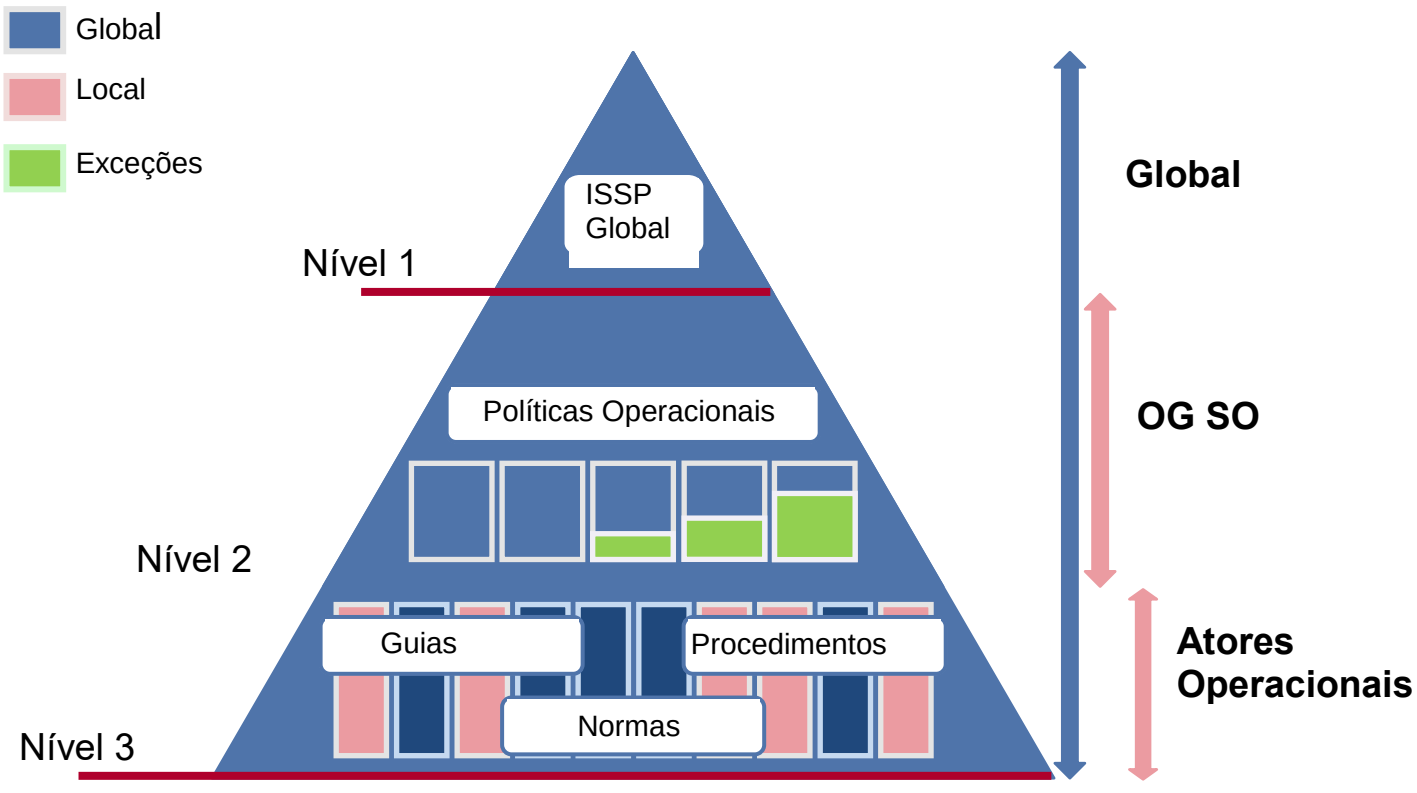
As Politicas de Segurança de Sistemas de Informação são aplicáveis a todas as entidades e subsidiárias de Bureau Veritas. O principal objetivo é o de assegurar a aplicabilidade mediante a focalização de requisitos técnicos e organizacionais que independem de tecnologias.

2. DOCUMENTAÇÃO

2.1. ESTRUTURA DOCUMENTAL DA SEGURANÇA DE INFORMAÇÃO

A documentação de segurança da informação de Bureau Veritas é formalizada em repositório documental organizado em três (3) níveis ou camadas:

- **Política Global de Sistemas de Informação (Global ISSP):** documento de referencia que estabelece desafios, princípios de governança e princípios fundamentais da segurança de informação para todo o grupo Bureau Veritas de acordo com a norma ISO/IEC 27001;
- **Politicas Operacionais:** pautam e definem regras de segurança de informação conforme temas ou assuntos que se aplicam a Bureau Veritas. Uma exceção temporária pode ser autorizada quando o atendimento não possa ser assegurado. Essas exceções são validadas pelo CISO Global de Bureau Veritas;
- **Guias, normas e procedimentos:** documentos operacionais que suportam atividades aderentes com os requisitos estabelecidos nas regras das Politicas Operacionais. Esses documentos podem ser definidos em nível grupal ou local.



2.2. IMPLEMENTAÇÃO DA POLÍTICA DE SEGURANÇA

2.2.1. CICLO DE VIDA

Para assegurar a eficiência e sustentabilidade das Politicas de Segurança de Sistemas de Informação (ISS Policies) e a adequação com os requisitos de segurança de Bureau Veritas, essas políticas devem ser objeto da melhoria contínua.

O processo de melhoria continua é cíclico e está baseado nos princípios do PDCA:

- **Definição e planejamento (Plan)**: O CISO Global define um plano de ação que contém as políticas (ISS Policies) que devem ser revistas e atualizadas, as melhorias requeridas, bem como o período de comunicação;
- **Implantação (Do)**: O plano de ação estabelecido é implantado. Melhorias são aplicadas a políticas (ISS Policies) identificadas.
- **Controle e monitoramento (Check)**: As políticas revisadas são comunicadas a pontos focais para feedback e validação. Esta etapa também viabiliza a identificação do impacto operacional. Quando necessário, ajustes podem ser aplicadas para assegurar o atendimento das políticas (ISS Policies) revisadas. O CISO Global é responsável de validar as atualizações.
- **Manutenção e melhoria (Act)**: Novas versões das políticas (ISS Policies) são comunicadas com uma definição do prazo de aplicação. A comunicação a todos os pontos focais relevantes é assegurada (i.e. OG Security Officers, contatos de segurança).

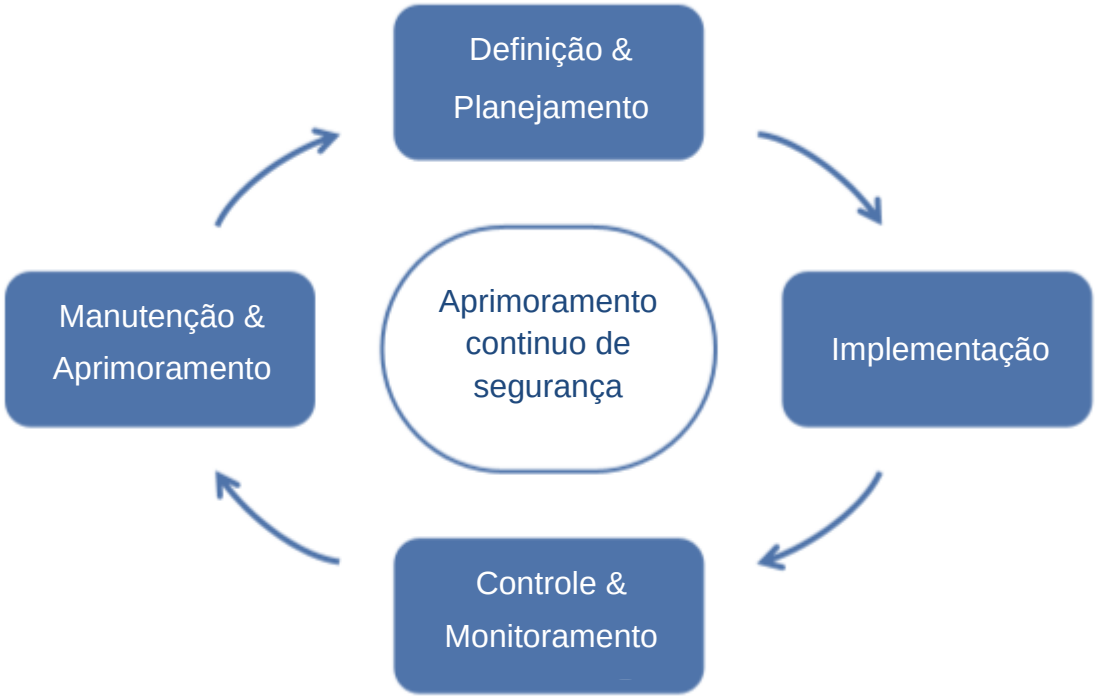


Figura 2 – Ciclo de vida do aprimoramento continuo

A Política Global de Sistemas de Informação (Global ISSP) e políticas operacionais devem ser revisadas anualmente. A solicitação de atualizações, derivadas de necessidades internas ou de fatores externos, é administrada e validada pelo CISO Global. As políticas revisadas são apresentadas para validação por parte do Comitê Executivo de Bureau Veritas.

O ciclo de vida das políticas (ISS Policies) deve fazer parte do Sistema de Gestão de Segurança da Informação (SGSI) para assegurar uma implantação eficaz. Os componentes do SGSI devem ser formalizados e documentados para assegurar a rastreabilidade durante a operação.

2.2.2. APLICABILIDADE

As políticas (ISS Policies) devem ser implantadas e sistematicamente aplicadas. O não atendimento das políticas (ISS Policies) deve ser objeto de planos de ação corretiva com prazos definidos para a realização com justificativa formal da não realização.

3. GOVERNANÇA DO SISTEMA DE INFORMAÇÃO

3.1. VISÃO GERAL DA GOVERNANÇA

O principal objetivo da governança da Segurança do Sistema de Informação é a definição da estrutura do fluxo de segurança da informação de Bureau Veritas, bem como os papeis e responsabilidades de todos os pontos focais relevantes que fazem parte dessa estrutura (CISO Global, OG Security Officers, recursos profissionais e equipes de Segurança da Informação, etc.)

O principal alvo dessa governança é a canalização o fluxo da Segurança do Sistema de Informação mediante a definição de processos relevantes, vitalização do fluxo e fornecimento de materiais necessários (Políticas ISS, treinamento e suportes da conscientização, guias).

A governança também inclui papeis relevantes da Segurança do Sistema de Informação dentro das atividades de negocio, funções de controle, gestão de projetos e Direção.

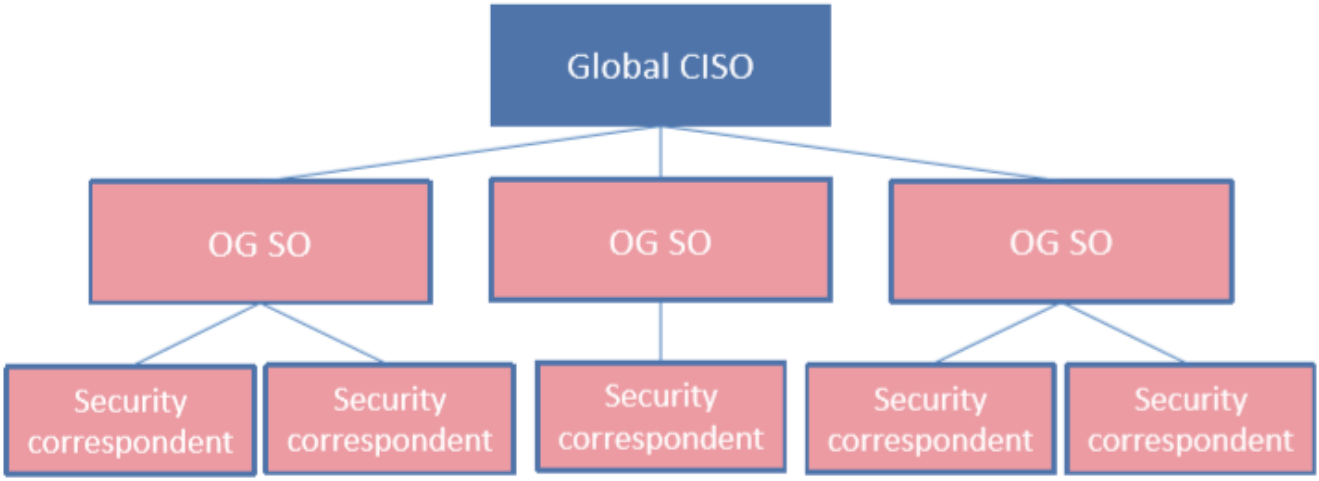


Figure 3 - Organização de governança do ISS do Bureau Veritas

3.2. O CISO GLOBAL DE BUREAU VERITAS

3.2.1. APRESENTAÇÃO DO CISO GLOBAL

O CISO Global de Bureau Veritas é responsável de assegurar e garantir a segurança e continuidade do sistema de informação das entidades, subsidiárias e do grupo Bureau Veritas. Nessa condição é responsável do Sistema de Gestão de Segurança de Informação de Bureau Veritas.

O CISO Global desenvolve suas atividades dentro de Bureau Veritas e atua em conjunto com Fornecedores, Clientes e terceiros (i.e. organizações governamentais, organismos de certificação).

3.2.2. RESPONSABILIDADES DO CISO GLOBAL

O CISO GLOBAL é o responsável da gestão e da manutenção do fluxo operacional da Segurança da Informação. As responsabilidades da função incluem:

- Formalização, coordenação e manutenção em condições operacionais do fluxo da segurança de sistemas de informação de Bureau Veritas;
- Definição de campanhas de treinamento e de conscientização;
- Aprovação da nomeação de OG Security Officers;
- Elaborar painéis de gestão de segurança global, centralizar os indicadores elaborados por OG Security Officers;
- Elaborar e revisar Políticas (ISS Policies);
- Obter aprovação executiva de Políticas (ISS Policies);
- Assegurar a aplicação e acompanhar a implantação de Políticas (ISS Policies) nas entidades e subsidiárias do grupo Bureau Veritas;
- Monitorar o cumprimento de Políticas (ISS Policies) no grupo Bureau Veritas;
- Gerir exceções quanto ao atendimento Políticas (ISS Policies) que possuam impacto crítico ou global;
- Planejar e avaliar a realização de auditorias do sistema de informação para efeitos de segurança e acompanhar o plano de ação corretiva derivado das recomendações da auditoria;
- Aprovar, assessorar e monitorar a realização de auditorias locais de segurança da informação com o OG Security Officer;
- Participar no Comitê de Gestão de Mudanças (CAB) para acompanhar mudanças com impacto crítico ou extensivo ao sistema de informação Bureau Veritas;
- Monitorar a implantação e a manutenção em condições operacionais e teste regular do processo de gestão de incidentes de Bureau Veritas para assegurar a eficiência do plano de gestão de crise e da unidade de crise;
- Monitorar a implantação e a manutenção em condições operacionais e teste regular do processo de Continuidade de Negócios de Bureau Veritas.

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

3.3.1. APRESENTAÇÃO DO OG SO

O OG Security Officer é responsável de assegurar a segurança e continuidade do sistema de informação de Bureau Veritas no nível de OG.

As principais responsabilidades do OG Security Officer exigem a realização e supervisão de atividades de segurança da informação de equipes técnicas e de negócio e assegurar a implantação de iniciativas globais quanto à aplicação de políticas e marcos de referência.

3.3.2. RESPONSABILIDADES DO OG SO

OG Security Officer de Bureau Veritas são responsáveis da implantação do Sistema de Gestão de Segurança da Informação e da manutenção operacional do sistema no âmbito de atuação estabelecido. As responsabilidades da função incluem:

- Relatar informações importantes ao Global CISO;
- Assegurar a implantação de Politicas (ISS Policies);
- Administrar exceções quanto o cumprimento de Politicas (ISS Policies) nas suas áreas de atuação;
- Assegurar a aplicação de boas prática de segurança;
- Definir campanhas focalizadas de treinamento e de conscientização;
- Relatar informação importante ao Global CISO;
- Assegurar a implantação de Politicas (ISS Policies);
- Administrar exceções quanto o cumprimento de Politicas (ISS Policies) nas suas áreas de atuação;
- Assegurar a aplicação de boas prática de segurança;
- Definir campanhas focalizadas de treinamento e de conscientização;
- Elaborar painéis de gestão de segurança locais, analisar indicadores e enviar esses indicadores ao CISO Global;
- Coordenar ações locais de segurança;
- Colaborar com áreas de negócio e de Tecnologia da Informação na conversão de politicas operacionais em guias, normas e procedimentos técnicos (i.e. instalação, operação, gestão de eventos),
- Aprovar, assessorar e monitorar a realização de auditorias locais de segurança da informação com o CISO Global;
- Participar no Comitê de Gestão de Mudanças (CAB) para acompanhar mudanças com impacto no escopo de atuação;

- Assegurar a manutenção em condições operacionais do processo de gestão de incidentes no escopo de atuação;
- Assegurar a manutenção em condições operacionais do processo de Continuidade de Negocios no escopo de atuação.

3.4. LOCAL SECURITY CORRESPONDENTS (RECURSOS LOCAIS DE SEGURANÇA)

Além do CISO Global e dos OG Security Officers, a organização de segurança de informação contempla a atuação de recursos profissionais e equipes locais de segurança.

O OG Security Officer deve identificar e supervisionar esses recursos (onde for necessário) dentro das entidades, subsidiárias, departamentos e unidades de negócio de Bureau Veritas.

Esses recursos de segurança auxiliam o OG Security Officer na realização de sua missão de implantar e manter a segurança da informação dentro do escopo de atuação ou quando da elaboração de projetos focalizados no atendimento de necessidades específicas de segurança.

4. APENDICE

4.1. APENDICE 1: POLÍTICAS OPERACIONAIS

As políticas operacionais da Política Global de Sistemas de Informação (Global ISSP) que tratam de áreas temáticas são:

- Segurança e Recursos Humanos (Human Resource Security).
- Classificação de Recursos de Tecnologia da Informação (Classification of IT Resources).
- Controle do Acesso Lógico (Logical Access Control).
- Segurança Física (Physical Security).
- Segurança das Operações (Operations Security).
- Gestão de logs (Management of IT Traces).
- Manuseio de Mídias (Media Handling).
- Equipamento de Usuários (Users' Equipment).
- Segurança da Rede (Network Security).
- Segurança Cloud (Cloud Security)
- Desenvolvimento e Manutenção de Aplicações (Development and Maintenance of Applications)
- Relacionamento com fornecedores (Suppliers Relationship).
- Gestão de Incidentes de Segurança (Management of Security Incidents).
- Continuidade das Atividades (Activity Continuity).