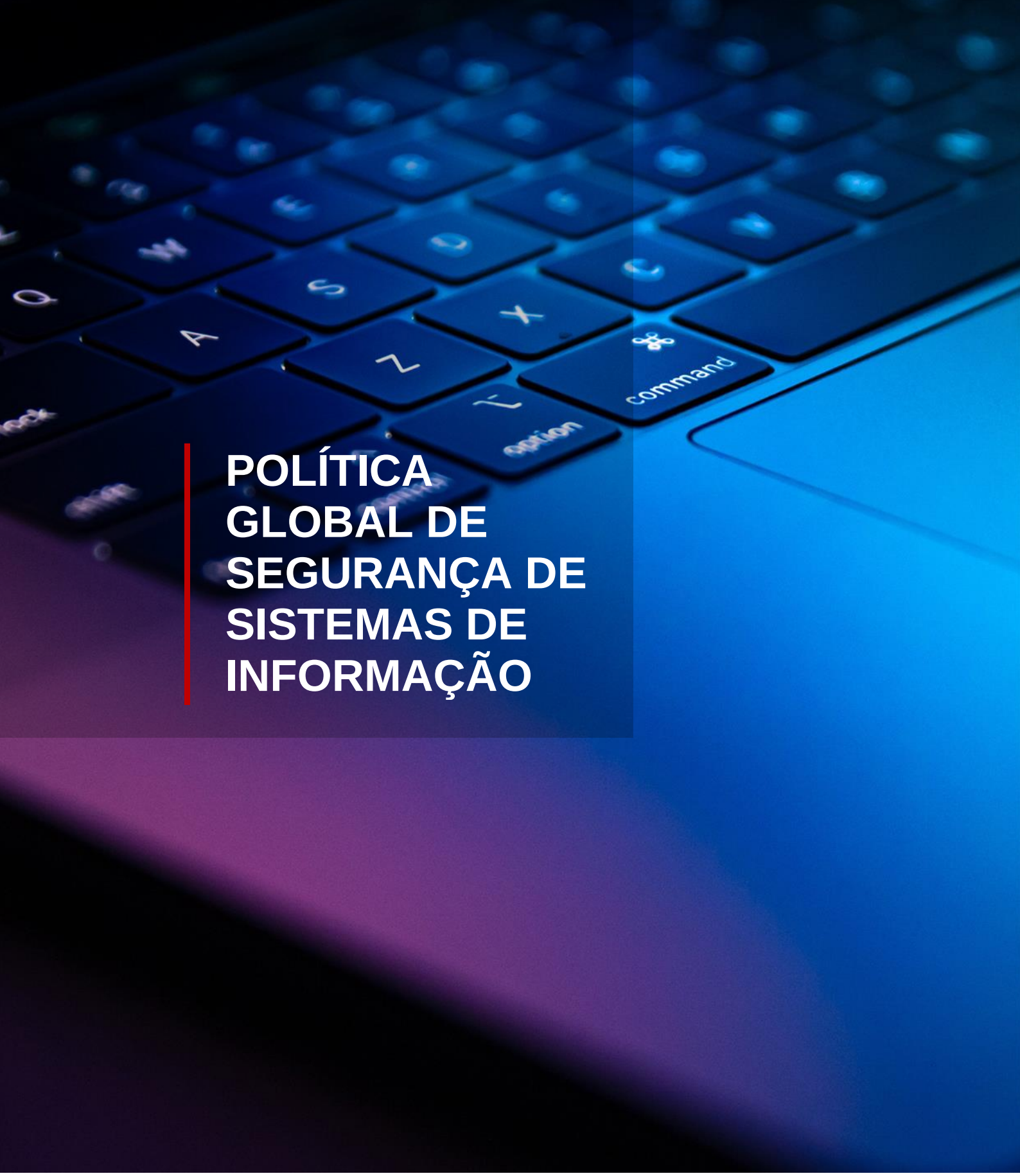

POLÍTICA GLOBAL DE SEGURANÇA DE SISTEMAS DE INFORMAÇÃO

STATUS : PUBLICADO

VERSION : 1.3

PUBLIC	INTERNAL	RESTRICTED	SECRET
X			

Shaping a World of Trust

Aprovadores

Nome	Posição
Francois VILJOEN	Senior Vice President, Group CIO
Julien ANICOTTE	Group Chief Information Security Officer
Ricardo VILLAGELIN	LAM CIO

Histórico de Revisão

Versão	Autor	Descrição	Data
1.0	Ricardo VILLAGELIN / Daniel RODRIGUEZ / John FRANKLIN ARCE	Versão Português Brasil: Política Global de Segurança de Sistemas de Informação	04/10/2021
1.1	Ricardo VILLAGELIN / Daniel RODRIGUEZ / John FRANKLIN ARCE	Versão Português Brasil: Revisão da redação e formato da Política Global de Segurança de Sistemas de Informação	21/11/2022
1.2	Ricardo VILLAGELIN / Daniel RODRIGUEZ / John FRANKLIN ARCE	Versão Português Brasil: Revisão das atribuições do Security Officer OG	08/12/2022
1.3	Daniel Dos Santos RODRIGUEZ / Leonardo Da Silva ARAUJO	Versão Português Brasil: Revisão Anual	14/11/2023

Documentos de referência

Versão	Autor	Título do Documento	Data
2.4	ISS Compliance	GLOBAL INFORMATION SYSTEM SECURITY POLICY	20/04/2023

Classificação

Nível	Confidencialidade
C1	Público

SUMÁRIO

TERMOS & DEFINIÇÕES

CIO: Chief Information Officer

CISO O Chief Information Security Officer (CISO) Global é quem garante a segurança e a continuidade do sistema de informação do grupo Bureau Veritas e das suas entidades e filiais. Nessa condição, é responsável pelo Sistema de Gestão da Segurança da Informação do Grupo Bureau Veritas.

Fornecedor: Licitante que foi selecionado pelo Bureau Veritas para executar Serviço(s) de acordo com um Contrato.

Funcionário do Fornecedor: Profissional contratado e designado pelo Fornecedor (Licitante) para execução das tarefas do(s) Serviço(s)

ISO 27001: Norma de gestão de Segurança da Informação. Fornece requisitos para a implantação e funcionamento do Sistema de Gestão de Segurança da Informação (SGSI) do Grupo Bureau Veritas.

LN: Linha de negócio

OG: Grupo Operacional (Operational Group).

PCN: Plano de Continuidade de Negócio

Política de Segurança de Sistemas de Informação Global: Este documento.

Security Officer (SO): O Security Officer é o ponto focal para todos os assuntos vinculados à Segurança de Informação nos respectivos OG do Bureau Veritas. Especificamente, o Security Officer é o responsável de assegurar que os objetivos e o funcionamento de todos processos e atividades do Sistema de Gestão de Segurança da Informação (SGSI) estão em conformidade com os requisitos da norma ISO 27001 e de relatar e informar o desempenho do SGSI para o CIO da OG e o CISO Global.

Serviços: Todo tipo de serviço entregue por Fornecedores para o Bureau Veritas. Abrange a assistência técnica, manutenção e Serviços, todo serviço baseado na Nuvem como SaaS, PaaS, etc. Todos os serviços podem ser entregues no formato On-Site ou Off-Site.

SGSI: Sistema de Gestão de Segurança da Informação.

1. INTRODUÇÃO

A Política Global de Segurança de Sistemas de Informação é a referência estrutural da Segurança da Informação do Grupo Bureau Verita que destaca os objetivos e pontos de atenção para assegurar a efetiva aplicação das política. A política também apresenta os princípios de governança e requisittos fundamentais de Segurança da Informação aplicáveis ao Grupo Bureau Veritas.

A Política Global de Segurança de Sistemas de Informação visa garantir a proteção da Informação através dos quatro critérios de classificação, a saber: Confidencialidade; Disponibilidade; Integridade e Rastreabilidade.

1.1. SEGURANÇA DA INFORMAÇÃO, UMA QUESTÃO VITAL

A Informação, em todas as duas formas, seja escrita, oral, eletrônica, processada manualmente ou automaticamente é um recurso precioso e estratégico, que sustenta o desempenho, a sustentabilidade e capacidade de atingir os objetivos e resultados do Grupo Bureau Veritas

Atuando contra ameaças maliciosas ou acidentais que possam afetar a segurança dos seus sistemas de informação, o Bureau Veritas deve proteger de forma eficiente seus sistemas de informação mediante a implementação de medidas de segurança acorde com os desafios da propria seguranca.

As medidas de Segurança devem permitir que o Bureau Veritas cumpra compromissos contratuais, obrigações legais e regulamentares e a continuidade e qualidade dos serviços prestados aos seus clientes. Além disso, isto contribui para a proteção e o aprimoramento da Imagem do Bureau Veritas.

1.2. OBJETIVOS COMUNS PARA UMA PROTEÇÃO EFICAZ

A estrutura operacional de Segurança de Sistemas de Informação do Bureau Veritas é definida pela Política Global de Segurança de Sistema de Informação, que se apoia nos detalhamentos das regras e responsabilidades que tratam da gestão de Segurança da Informação em temas específicos.

Os princípios e regras comuns da governança formalizadas nessas políticas visam assegurar a efetiva proteção da informação no escopo do Bureau Veritas e a coerência do Sistema de Gestão da Segurança da Informação. **Esses princípios também devem viabilizar a capitalização das medidas de segurança já implementadas e as melhores práticas adotadas nas diferentes entidades e subsidiárias da Companhia**.

1.2.1. PERÍMETRO ORGANIZACIONAL

A Política Global de Segurança dos Sistemas de Informação deve ser aplicada em todas as entidades e subsidiárias do Grupo Bureau Veritas a nível global.

As Políticas de Segurança dos Sistemas de Informação também devem ter impacto nos Fornecedores. Essas políticas devem definir os princípios de segurança fundamentais para os Serviços contratados pelo Bureau Veritas com os fornecedores.

Algumas subsidiárias ou entidades do Bureau Veritas podem estar sujeitas a políticas de Segurança da Informação específicas e dedicadas devido à sua atividade, o país em que estão localizadas (por exemplo, restrições legais locais) e requisitos contratuais do Cliente ou Fornecedores.

1.2.2. PERÍMETRO FUNCIONAL

Todos os recursos de suporte às informações do Bureau Veritas fazem parte do Sistema de Gestão de Segurança da Informação, bem como todas os meios destinadas a criar, adquirir, processar, armazenar, distribuir ou destruir essas informações mediabte a utulização de:

- Equipamento de usuário (exemplo. desktop e laptop, smartphones, tablets);
- Recursos computacionais (exemplo. servidores, impressoras, elementos de rede);
- Software (exemplo. sistemas operacionais, bases de dados);
- Documentação Física (exemplo. contratos, processos e políticas impressos);
- Recursos humanos e organizacionais.

1.2.3. PERÍMETRO TÉCNICO

A Política Global de Segurança dos Sistemas de Informação está implementada pelo Grupo Bureau Veritas e em todas as suas entidades e subsidiárias. Essas políticas tem como objetivo garantir a aplicabilidade (independente do contexto técnico) e o não fornecimento de detalhes acerca das tecnologias a serem implementadas, mas somente o requerimentos funcionais e organizacionais.

1.2.4. ABORDAGEM

Seguindo as melhores práticas da industria, a Política Global de Segurança dos Sistemas de Informação leva em consideração o seguinte:

- **Gestão de Riscos de Informação:** As regras estabelecidas em cada política devem ser construídas de forma a gerir e reduzir os riscos que exercem um impacto significativo nas operações do negócio e que ameaçam a confidencialidade, integridade, disponibilidade e rastreabilidade da informação;
- **Conformidade**: As regras de segurança devem fazer cumprir os requisitos de avaliação de conformidade com os regulamentos, termos contratuais, padrões da indústria, bem como implementar medidas adequadas para assegurar a conformidade;
- **Objetivos de Negócios**: As políticas de Segurança dos Sistemas de Informação, além de apoiar a governança, devem contribuir e coordenar-se com os negócios para alinhar a estratégia de segurança com os objetivos e estratégia do Bureau Veritas, a saber: resiliência e proteção de dados.

2. DOCUMENTAÇÃO DA POLÍTICA DE SISTEMAS DE SEGURANÇA

2.1. ESTRUTURA DA DOCUMENTAÇÃO DE SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO

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

- A Política Global de Segurança de Sistema de Informação (este documento): Documento de referência, que estabelece desafios, princípios de governança e princípios fundamentais de segurança da informação para todo o grupo Bureau Veritas, alinhados com a norma ISO 27001;
- Políticas Operacionais: Definem regras de segurança da informação por tema aplicável ao Bureau Veritas. Derrogações temporárias podem ser concedidas a entidades ou subsidiárias se o cumprimento não puder ser garantido. 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.

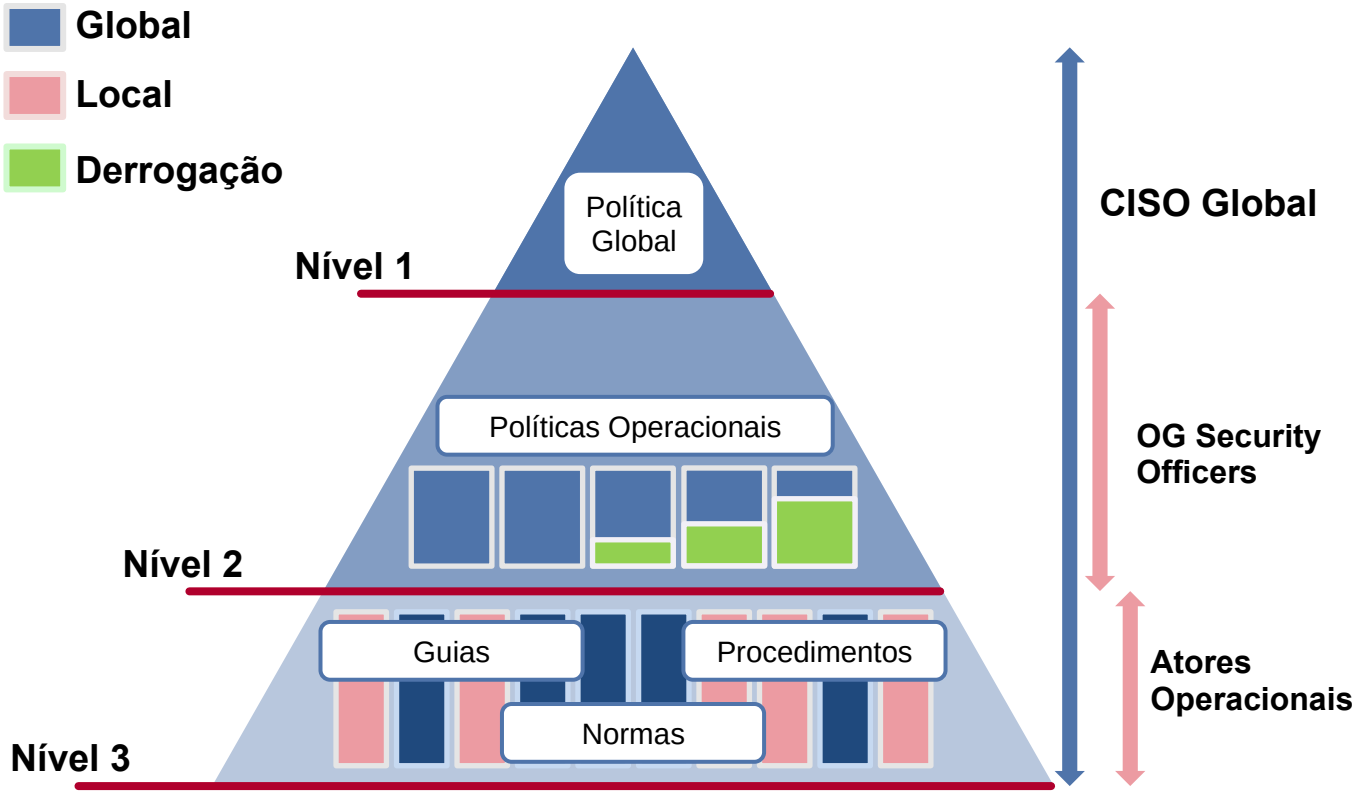

Figura 1 - Repositório documental e responsabilidades

2.2. IMPLEMENTAÇÃO DA POLÍTICA DE SEGURANÇA

2.2.1. CICLO DE VIDA

A fim de garantir a eficiência e sustentabilidade das políticas de Segurança da Informação ao longo do tempo e sua adequação aos requisitos de segurança do Bureau Veritas, as políticas da de Segurança da informação devem ser objeto de uma melhoria contínua.

Este processo de melhoria contínua deve ser cíclico, com base no princípio Plan-Do-Check-Act (PDCA):

- Definição e planejamento (Plan): O CISO Global estabelece um plano de ação que inclui: Políticas de Segurança de Sistemas de Informação a serem atualizadas, as melhorias necessárias e a fase de comunicação;
- Implementação (Do): O plano de ação definido na fase anterior é implementado. As melhorias são aplicadas às Políticas de Segurança da Informação aplicáveis. As políticas atualizadas são comunicadas às pessoas relevantes para feedbacks e validação.
- Controle e monitoramento (Check): esta fase permite identificar impactos nas atividades operacionais. A aplicação das políticas de Segurança da Informação é controlada.
- Manutenção e aprimoramento (Act): Os Security officers e outras partes interessadas (i.e., representantes de segurança) identificam as brechas e informam o CISO Global. Essa retroalimentação é analisada para identificar as melhorias necessárias e alimentar a próxima fase Plano.

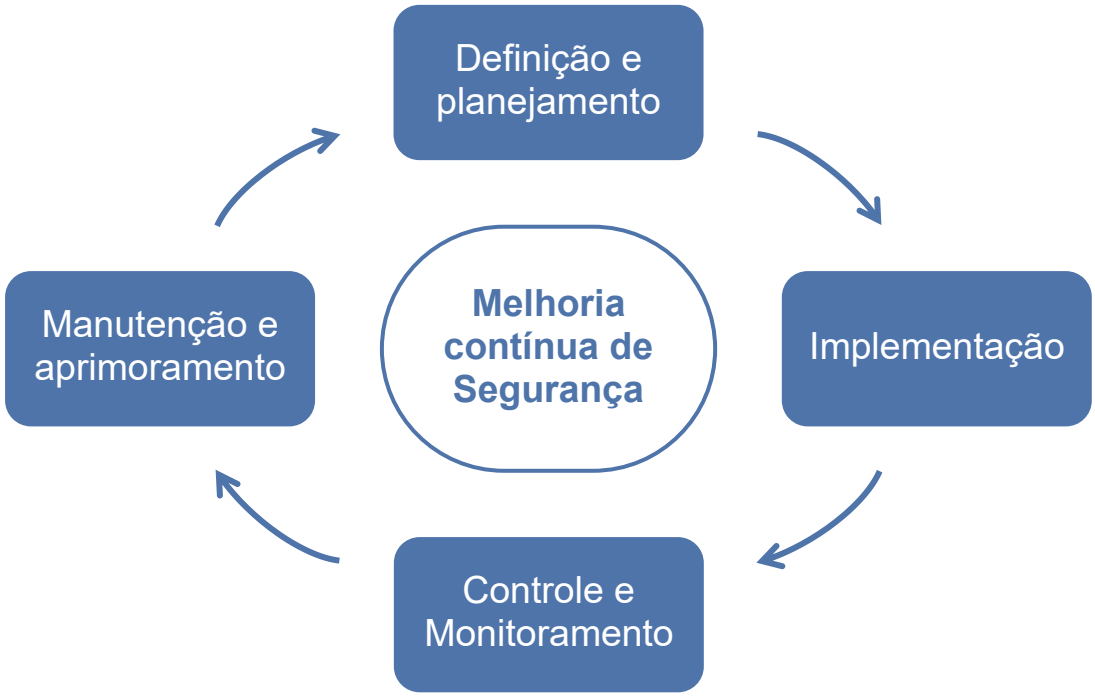

Figura 2 - Ciclo continuo de Melhoria

A Política de Segurança de Sistema de Informação Global deve ser revisada 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 revisões das Políticas de Segurança de Sistema de Informação Global serão submetidas para validação à Direção Executiva do Bureau Veritas.

Todo o ciclo de vida das Políticas de Segurança de Sistema de Informação devem estar inserido no Sistema de Gestão da Segurança da Informação (SGSI), para assim garantir

sua implementação. Os diversos elementos do SGSI devem ser formalizados e documentados de forma a garantir a rastreabilidade de suas operações.

2.2.2. APLICABILIDADE

A Política de Segurança de Sistema de Informação deve ser implementada e executável.

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

2.2.3. PUBLICAÇÃO

A Política de Segurança de Sistema de Informação deve ser publicada no portal da Companhia com o objetivo de demonstrar 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 estar acessíveis exclusivamente a todos os funcionários do Bureau Veritas.

Todas as atualizações das políticas devem ser seguidas por uma comunicação às partes interessadas relevantes para informá-los sobre as novas mudanças.

2.2.4. PROCEDIMENTOS DE TRATAMENTO DAS ISENÇÕES E EXCEÇÕES

Espera-se que todos os componentes do Sistema de Informação Bureau Veritas estejam em conformidade com as políticas e padrões da Segurança da Informação. Há várias situações e razões porem o cumprimento de algumas regras não pode materializado. O procedimento de derrogação para a gestão, documentação e controle dessas isenções e exceções deve ser formalizado e aplicado.

Os pedidos de derrogação devem ser analisados e aprovados pelo CISO Global, pela equipe de Compliance ou pelo Security Officer da entidade requerente.

3. GOVERNANÇA DA SEGURANÇA DE SISTEMAS DE INFORMAÇÃO

3.1. VISÃO GERAL DA GOVERNANÇA

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

Através desta governança, o objetivo é enquadrar a atividade do fluxo de segurança do sistema de informação do Bureau Veritas, definindo os processos relevantes, mediabte a dinalkização do o fluxo e disponibilizando o material necessário (Políticas de Segurança, Treinamento e Conscientização, Guias).

A governança também inclui qualquer papel relevante para a dinamização da segurança do sistema de informações nas atividades de negócios, funções de controle, propriedade e gestão de projetos.

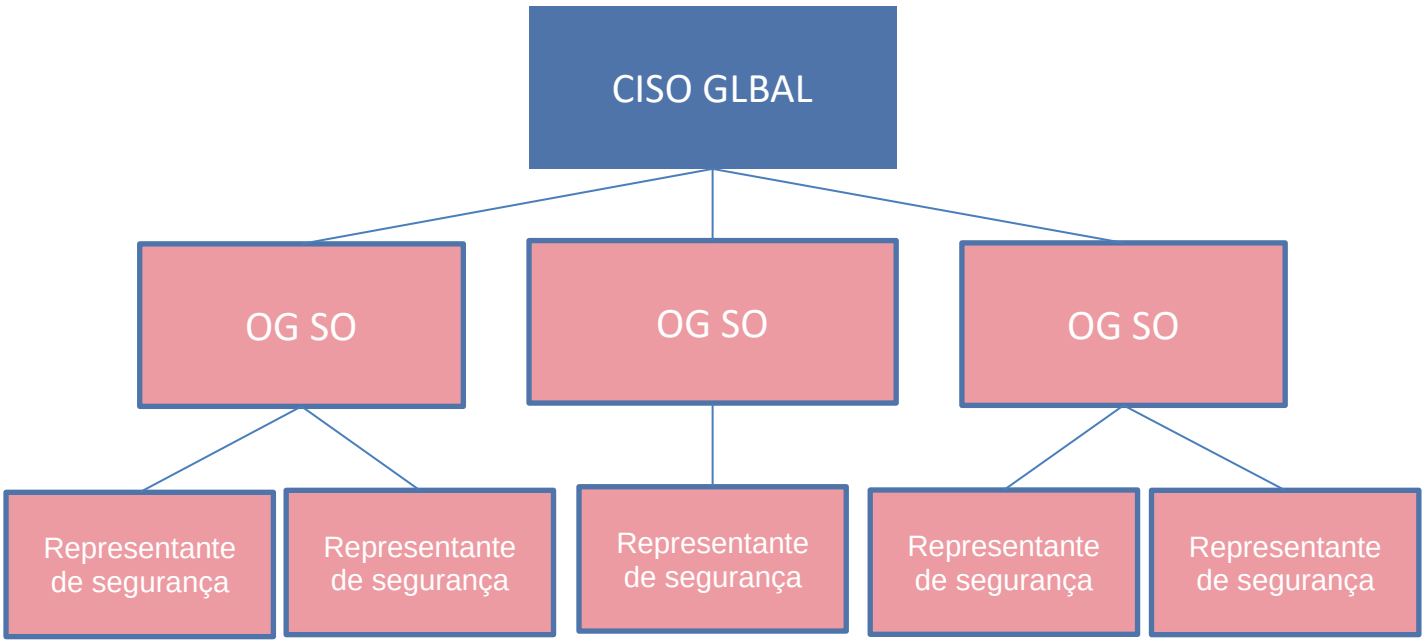

Figure 3 – Organização de Governança apra Segurança de Sistemas de informação do Bureau Veritas

3.2. O CHEFE GLOBAL DE SEGURANÇA DA INFORMAÇÃO (GLOBAL CISO) DO BUREAU VERITAS

3.2.1. APRESENTAÇÃO DO CISO GLOBAL

O Chief Information Security Officer (CISO) Global é quem garante a segurança e a continuidade do sistema de informação do grupo Bureau Veritas e das suas entidades e filiais. Nessa condição, é responsável pelo Sistema de Gestão da Segurança da Informação do Bureau Veritas.

O CISO Global desempenha suas funções dentro do Bureau Veritas e junto a 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 é responsável pelo Sistema de Gestão da Segurança da Informação da organização e sua manutenção em condições operacionais. Como parte desse dever, suas missões são:

- Formalizar, coordenar e manter em condições operacionais a organização do fluxo de segurança do sistema de informação do Bureau Veritas;
- Definir treinamentos e campanhas de conscientização;
- Aprovar a nomeação de Security Officers dos OG;
- Produzir painéis de segurança globais, centralizar indicadores de SOs OG e realizar análises globais de desempenho de segurança do sistema de informação;
- Desenvolver e atualizar as Políticas da segurança do sistema de informação;
- Obter Aprovações da Gerência Executiva para as Políticas da segurança do sistema de informação;
- Aplicar e acompanhar a implementação das Políticas da Segurança do Sistema de Informação no Grupo Bureau Veritas, suas entidades e subsidiárias;
- Monitorar o atendimento das Políticas da segurança do Sistema de Informação dentro do Grupo Bureau Veritas;
- Tratar os efeitos das Políticas da Segurança do Sistema de Informação com um escopo global ou impacto crítico;
- Planejar e supervisionar auditorias no sistema de informação para fins de segurança e acompanhar o plano de ação corretiva resultante das recomendações de auditorias;
- Aprovar, assessorar e monitorar as auditorias Locais de Segurança da Informação com o Security Officer dos OG;
- Participar dos Conselhos Consultivos de Mudança (CAB), em particular para mudanças com um impacto crítico ou maior no sistema de informações do Bureau Veritas;
- Acompanhar a implementação e a manutenção em condições operacionais do processo de gestão de incidentes de segurança do Bureau Veritas e dos seus testes periódicos e – no particular - para garantir a eficácia do plano de gestão de crises e da unidade de crise;
- Acompanhar a implementação e a manutenção em condições operacionais do Plano de Continuidade de Negócios do Bureau Veritas e seus testes periódicos.

3.3. SECURITY OFFICER DO GRUPO OPERACIONAL (OG) DO BUREAU VERITAS

3.2.1. APRESENTAÇÃO DO SECURITY OFFICER DO OG

O Security Officer do OG é o garantidor da segurança e da continuidade do sistema de informação do grupo Bureau Veritas a Nível de OG. Eles são nomeados no nível OG e serão parceiros de confiança da equipe central.

As suas principais funções são a execução e supervisão das atividades de segurança da informação do seu âmbito nas empresas e equipes técnicas, e também assegurar a implementação de iniciativas globais no respetivo âmbito, nominalmente a aplicação de políticas e marcos de referencia do Compliance.

3.2.2. ATRIBUIÇÕES DO SECURITY OFFICER DO OG

O Security Officer do OG do Bureau Veritas é responsável da implementação do Sistema de Gestão de Segurança da Informação (SGSI) ISO 27001 e pela manutenção do SGSI em condições operacionais no respectivo escopo. As principais atribuições do Security Officer são:

- Relatar o desempenho do SGSI ao CIO da OG e CISO Global;
- Assegurar a implementação das Políticas de Segurança do Sistema de Informação;
- Tratar os efeitos das Políticas de Segurança do Sistema de Informação em seu escopo de atuação;
- Garantir que as boas práticas de Segurança da Informação sejam seguidas e aplicadas;
- Definir treinamentos dedicados e campanhas de conscientização;
- Elaborar painéis de segurança locais, analisar indicadores de Segurança da Informação e enviá-los ao CISO Global;
- Coordenar ações de segurança locais;
- Contribuir, com as empresas e Departamentos de TI / SI, para a materialização de Políticas Operacionais em procedimentos técnicos (por exemplo, instalação, operação, tratamento de eventos), guias e normas;
- Aprovar, assessorar e monitorar as auditorias locais de segurança da informação com o CIO da OG e o CISO Global;
- Participar dos Conselhos Consultivos de Mudança (CAB) para mudanças no sistema de informação que impactem seu escopo;
- Garantir a manutenção em condições operacionais do processo de gestão de incidentes de segurança em seu escopo de atuação;
- Garantir a manutenção em condições operacionais do Plano de Continuidade de Negócios em seu escopo de atuação.

3.4. O REPRESENTANTE LOCAL DE SEGURANÇA DA INFORMAÇÃO

Além do CISO Global e Security Officers de OG descritos acima, a organização de Segurança da Informação abrange representantes locais de segurança.

Os OG Security Officers identificam e supervisionam representantes de Segurança da Informação locais em entidades, subsidiárias, departamentos, negócios e sempre que necessário. Os Representantes Locais de Segurança auxiliam os Security Officers de OG em suas missões, implementam segurança da informação em seu escopo de atuação e/ou desenvolvem projetos baseados em necessidades específicas de segurança.

4. ANEXOS

4.1. Anexo 1: POLÍTICAS OPERACIONAIS

As Políticas Operacionais vinculadas à Política Global sobre assuntos temáticos do Bureau Veritas (conforme estabelecido na ISO 27001) são:

- Segurança de Recursos Humanos (Human Resource Security).
- Classificação da Informação (Classification of Information).
- Controle de Acesso Lógico (Logical Access Control).
- Segurança Física (Physical Security).
- Segurança da Operação (Operations Security).
- Gestão de log's (Management of IT Traces).
- Manuseio de Mídia (Media Handling).
- Equipamento de Usuários (Users' Equipment).
- Segurança da Rede (Network Security).
- Cloud Security (Segurança na Nuvem).
- 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 de Negócios (Activity Continuity).