POLÍTICA DE SEGURANÇA DO SISTEMA DE INFORMAÇÃO GLOBAL

STATUS : VALIDADO

VERSÃO: 2,2

PÚBLICO INTERNO RESTRITO SEGREDO

X

Shaping a World of Trust

Aprovador

Nome	Posição
Francois VILJOEN	Vice-presidente Sênior, Grupo CIO
Julien ANICOTTE	Diretor de Segurança da Informação do Grupo

Documentos de referências

Título do documento	Nome do documento

Classificação

Nível	Confidencialidade
C1	Público

SUMÁRIO

GLOSSÁRIO

B

BCP: Plano de Continuidade de Negócios.

BL: Linha de Negócios.

C

CIO: Diretor de Informação.

CISO: Diretor de Segurança da Informação.

G

Global ISSP: Política Global de Segurança do Sistema de Informação. Documento atual.

I

ISMS: Sistema de Gestão de Segurança da Informação.

Políticas ISS: Políticas de Segurança do Sistema de Informação. Inclui as ISSP e políticas operacionais globais.

O

OG: Grupo Operacional.

S

Serviços: todos os tipos de serviços executados por um Fornecedor do Bureau Veritas, incluindo, mas não se limitando a, assistência técnica, serviços de manutenção, quaisquer serviços baseados em nuvem, como SaaS, IaaS ou PaaS…; eles podem ser fornecidos no local ou fora dele.

SO: Oficial de segurança.

Fornecedor: Licitante que foi selecionado pelo Bureau Veritas para executar os Serviços sob um Contrato.

Pessoal do Fornecedor: funcionários do Fornecedor designados pelo Fornecedor para a execução dos Serviços.

1. INTRODUÇÃO

A Política Global de Segurança do Sistema de Informação define a estrutura de referência para a segurança da informação do Bureau Veritas, destacando questões e objetivos de segurança. Ele também fornece princípios de governança e requisitos de segurança fundamentais que se aplicam ao Bureau Veritas.

O Global ISSP visa garantir a proteção das informações por meio de quatro critérios de classificação: Disponibilidade; Integridade; Confidencialidade e Rastreabilidade.

1.1. SEGURANÇA DA INFORMAÇÃO, UMA QUESTÃO VITAL

A informação em todas as suas formas, seja escrita, oral, eletrônica, processada manual ou automaticamente, é um recurso estratégico no qual dependem o desempenho, a sustentabilidade e a capacidade da empresa para desenvolver as suas atividades e resultados.

Para fazer frente às ameaças acidentais e maliciosas que podem afetar a segurança do seu sistema de informação, o Bureau Veritas deve proteger de forma eficiente o seu sistema de informação, implementando medidas de segurança adequadas, em conformidade com os desafios de segurança.

Estas medidas de segurança devem permitir ao Bureau Veritas respeitar os seus compromissos contratuais, as restrições legais e regulamentares e a continuidade dos serviços prestados aos clientes, bem como a sua qualidade. Além disso, isso contribui para a proteção e o aprimoramento da imagem do Bureau Veritas.

1.2 OBJETIVOS COMUNS PARA UMA PROTEÇÃO EFICAZ

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

Os princípios de governança e as regras comuns formalizadas nas Políticas do ISS devem garantir a proteção efetiva da informação 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 os princípios fundamentais de segurança aplicáveis aos serviços contratados pelo Bureau Veritas com os fornecedores.

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

1.2.2 PERÍMETRO FUNCIONAL

Todos os recursos de 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 em ou usando:

- Equipamentos dos usuários (por exemplo, desktops e laptops, 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 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 ABORDAGEM

Além das melhores práticas da indústria, as políticas de ISS devem levar em consideração o seguinte:

- Gestão de riscos da informação: as regras estabelecidas em cada política devem ser construídas para gerenciar e reduzir os riscos que têm impacto significativo nas operações do negócio e ameaçam a confidencialidade, integridade, disponibilidade e rastreabilidade das informações;
- Conformidade: as regras de segurança devem impor a avaliação de conformidade para requisitos com regulamentação, termos contratuais, padrões da indústria, bem como implementação de medidas adequadas para o seu cumprimento;

- Objetivos de negócios: as políticas de ISS, além de apoiar a governança, devem cooperar e coordenar-se com os negócios para alinhar a estratégia de segurança com os objetivos e estratégia do Bureau Veritas: resiliência e proteção de dados.

2. DOCUMENTAÇÃO 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 linha com a ISO 27001;
- **Políticas Operacionais:** definir 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, padrões 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.

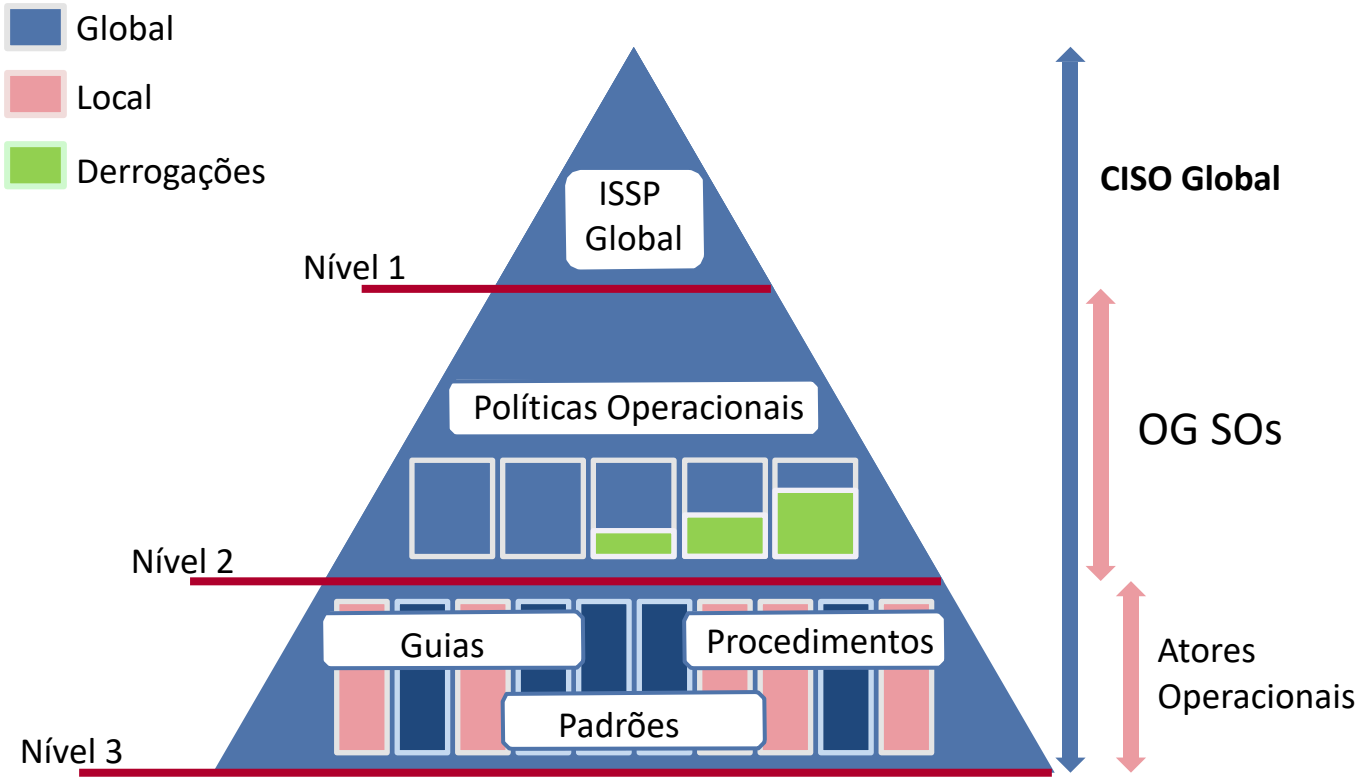

Figura 1 - Repositório documental e responsabilidades

2.2 IMPLEMENTAÇÃO DA POLÍTICA DE SEGURANÇA

2.2.1 VIDA ÚTIL

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 uma melhoria contínua.

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

- **Definição e planejamento (Plano):** o CISO Global estabelece um plano de ação incluindo: Políticas ISS para atualização, 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 ISS correspondentes; 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 da ISS é controlada.
- **Manutenção e melhoria (Ato):** 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.

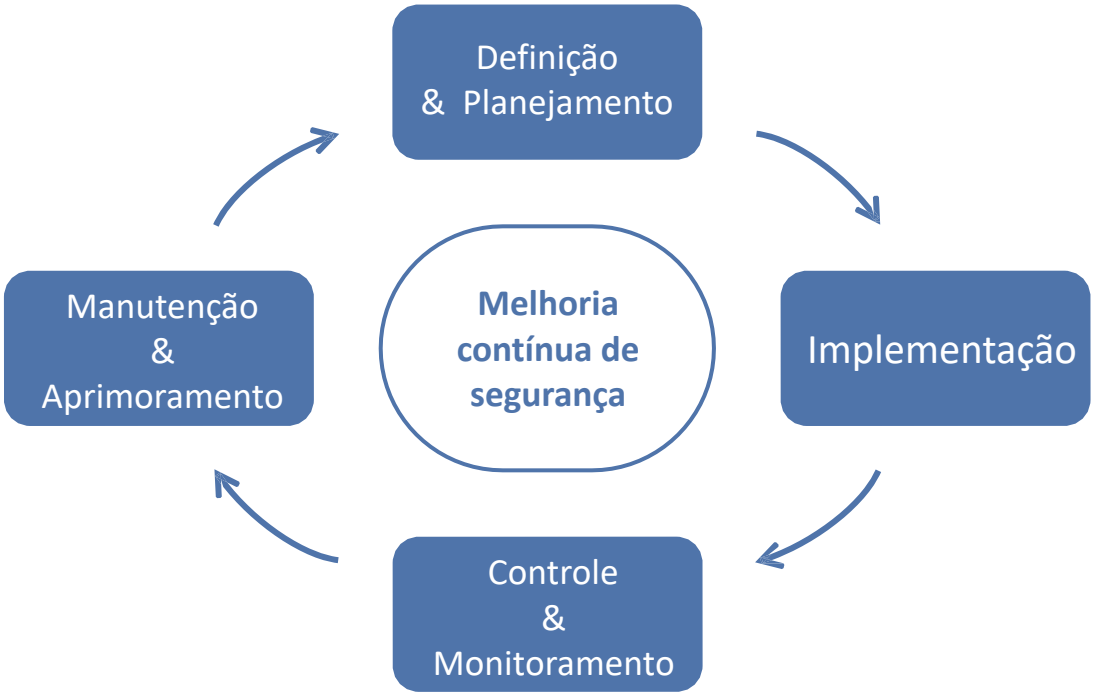

Figura 2 - Ciclo de vida de melhoria contínua

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 ISS atualizadas são submetidas à validação da Diretoria Executiva do Bureau Veritas.
Todo o ciclo de vida das Políticas do ISS deve estar inserido no Sistema de Gestão da Segurança da Informação (SGSI), garantindo 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

As políticas da ISS devem ser implementadas e aplicáveis.

O não cumprimento das Políticas da ISS deve estar sujeito a planos de ação corretiva formal com um cronograma de conclusão definido ou derrogações.

2.2.3 PUBLICANDO

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 estar acessíveis 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.

3. GOVERNANÇA DA INFORMAÇÃO SISTEMA DE SEGURANÇA

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, animando o fluxo e disponibilizando o material necessário (Políticas ISS, apoios de formação e sensibilização, guias).

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

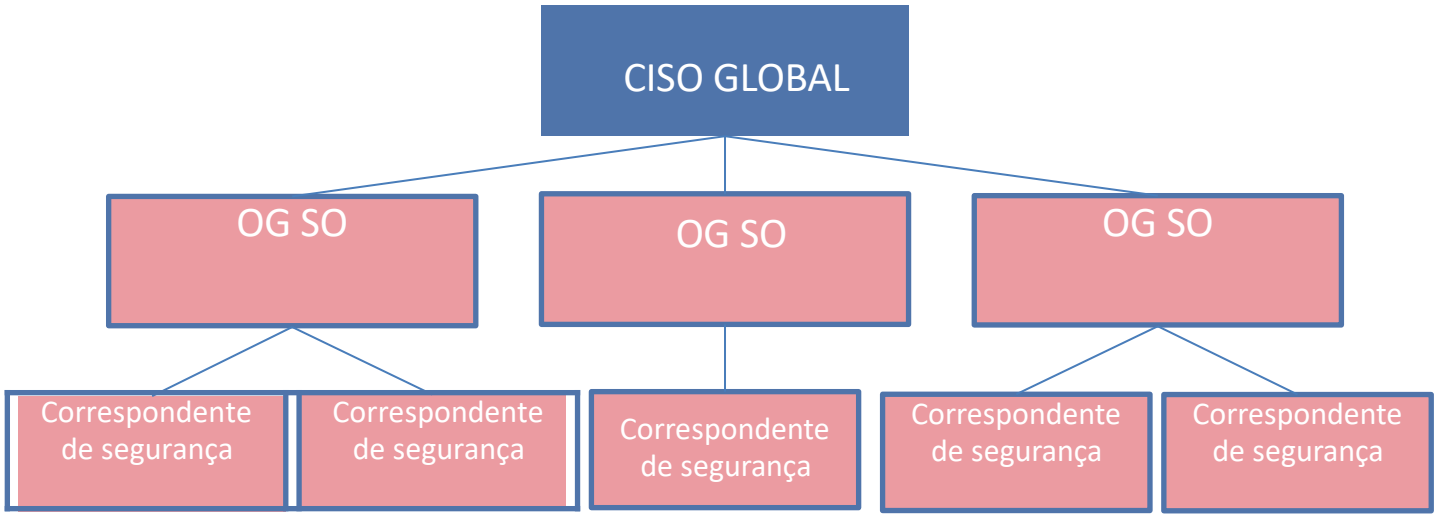

Figura 3 - Organização da governança do ISS do Bureau Veritas

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

3.2.1 APRESENTAÇÃO DO CISO GLOBAL

O CISO Global do Bureau Veritas é o garante da segurança e da continuidade do sistema de informação do grupo Bureau Veritas, das suas entidades e filiais. Como tal, 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 o 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 OG SOs;
- 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 ISS;
- Obter a aprovação da Gerência Executiva para as Políticas ISS;
- Aplicar e acompanhar a implementação das Políticas ISS dentro do grupo Bureau Veritas, suas entidades e subsidiárias;
- Monitorar o cumprimento das Políticas ISS dentro do grupo Bureau Veritas;
- Lidar com derrogações às políticas da 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, assessorar e monitorar as auditorias locais de segurança da informação com o OG SO;
- Participar dos Conselhos Consultivos de Mudança (CAB), em particular para mudanças com um impacto crítico ou grande no sistema de informação do Bureau Veritas;
- Acompanhar a implantação e a manutenção nas condições operacionais do processo de gestão de incidentes de segurança do Bureau Veritas e seus testes regulares, em particular para garantir a eficácia do processo de gestão de incidentes de segurança do Bureau Veritas e seus testes regulares, em particular para garantir a eficácia do plano de gestão de crises e da unidade de crise; 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 OFICIAIS DE SEGURANÇA DO GRUPO OPERACIONAL (OG SO) DO BUREAU VERITAS

3.3.1 APRESENTAÇÃO DO OG SO

Oficiais de Segurança OG é o garante da segurança e da continuidade do sistema de informação do 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 equipas técnicas, mas também assegurar a implementação de iniciativas globais no respetivo âmbito, nomeadamente a aplicação de políticas e enquadramentos de compliance.

3.3.2 ATRIBUIÇÕES DE OG SO

Os Oficiais de Segurança OG do Bureau Veritas são responsáveis pela implementação do Sistema de Gestão da Segurança da Informação e pela sua manutenção em condições operacionais nos respetivos âmbitos. Como parte de seu dever, suas missões são:

- Relatar informações importantes ao CISO Global;
- Reforçar a implementação das Políticas ISS;
- Lidar com derrogações às Políticas ISS em seu escopo;
- Garantir que as boas práticas de segurança sejam seguidas;
- Definir treinamentos dedicado se campanhas de conscientização;
- Produzir painéis de segurança locais, analisar indicadores de segurança e enviá-los ao CISO Global;
- Coordenar ações de segurança local;
- Contribuir com empresas e departamentos de TI/SI, para a transcrição de Políticas Operacionais em procedimentos técnicos (por exemplo, instalação, operação, manuseio de eventos), guias e normas;
- Aprovar, aconselhar e monitorar as auditorias locais de segurança da informação com o CISO Global;
- Participar de Conselhos Consultivos de Mudanças (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 no seu âmbito;
- Garantir a manutenção em condições operacionais do Plano Continuidade de Negócios em seu escopo.

3.4. CORRESPONDENTES DE SEGURANÇA LOCAIS

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

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

4. ANEXOS

4.1. ANEXO 1: HISTÓRICO DE REVISÕES

Versão	Autor	Descrição	Data
1.5	Conformidade ISS	Nomeação do Grupo CISO	12/01/2017
2.0	Conformidade ISS	Atualização do conteúdo para cumprir a estratégia do grupo	27/03/2017
2.1	Conformidade ISS	Atualização das funções de segurança Atualização da frequência da revisão da política Adicionando uma nova política operacional ao apêndice	19/12/2019
2.2	Conformidade ISS	Adicionando abordagem de criação de políticas Adicionando requisitos de publicação	19/03/2021

4.2 ANEXO 2: POLÍTICAS OPERACIONAIS

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

- Segurança de Recursos Humanos
- Classificação da Informação
- Controle de acesso lógico
- Segurança física
- Operações de Segurança
- Gestão de rastros de TI
- Manuseio de mídia
- Equipamento do usuário
- Segurança de rede
- Segurança na nuvem
- Desenvolvimento e manutenção de aplicativos
- Relacionamento com Fornecedores
- Gestão de Incidentes de Segurança
- Continuidade de Atividades