



# Política de Segurança da Informação

Security Office

Abril de 2026

## Controle de Informações

<b>Nome</b>	Política de Segurança da Informação
<b>Número de Referência</b>	POL_096
<b>Unidade Normativa</b>	BTG Pactual
<b>Número da Versão</b>	9
<b>Pública</b>	Sim
<b>Governança</b>	Interna
<b>Data da Aprovação</b>	29/04/2026
<b>Aplicabilidade (Pessoas)</b>	Colaboradores do BTG Pactual, incluindo aqueles de empresas subsidiárias e joint ventures sob a gestão e controle do BTG Pactual, inclusive consultores externos, equipes temporárias e terceiros contratados
<b>Jurisdição</b>	Global
<b>Normativos Relacionados</b>	ISSO 27001 BACEN 4893 SUSEP 638 PCI DSS
<b>Documentos Relacionados</b>	<ul style="list-style-type: none"> <li>• IT 001 – GLOBAL – Controle de Acesso</li> <li>• IT 002 – BRASIL – Segurança de Aplicativos</li> <li>• IT 003 – GLOBAL – Software e Hardware Aprovados</li> <li>• IT 006 – GLOBAL – Retenção, Backup e Recuperação de Dados</li> <li>• IT 008 – GLOBAL – E-mail e Mensagens Eletrônicas</li> <li>• IT 017 – GLOBAL – Acesso Remoto</li> <li>• IT 018 – GLOBAL – Registro de Logs e Monitoramento de Segurança</li> <li>• IT 019 – GLOBAL – Uso da Internet</li> <li>• IT 020 – GLOBAL – Proteção Contra Vírus e Malware</li> <li>• IT 021 – GLOBAL – Gestão de Vulnerabilidades</li> <li>• IT 022 – GLOBAL – Segurança, Classificação e Privacidade de Dados</li> <li>• IT 043 – GLOBAL – Gerenciamento de Incidentes de Segurança da Informação</li> <li>• IT 044 – BRASIL – Segurança da Informação para Terceiros</li> <li>• IT 045 – BRASIL – Segurança da Informação para Agentes Autônomos de Investimento</li> </ul>

## Índice

<b>1. Objetivo e Escopo</b> .....	<b>4</b>
<b>2. Abrangência e Aplicabilidade</b> .....	<b>4</b>
<b>3. Definições</b> .....	<b>4</b>
<b>4. Responsabilidades</b> .....	<b>6</b>
4.1. CISO (Chief Information Security Officer) .....	6
4.2. Security Office .....	6
4.3. Usuários .....	6
4.4. Gestores das Áreas de Tecnologia da Informação (TI) .....	7
<b>5. Processos Internos</b> .....	<b>7</b>
5.1. Diretrizes Corporativas .....	7
5.2. O Security Office .....	10
5.3. Estrutura de Gerenciamento .....	11
5.4. Diretoria do Security Office .....	11
5.5. Atuação do Security Office .....	12
5.6. Medidas Disciplinares .....	17
<b>6. Alçadas</b> .....	<b>17</b>
<b>7. Exceções</b> .....	<b>18</b>
<b>8. Documentos e Normativos Relacionados</b> .....	<b>18</b>

## 1. Objetivo e Escopo

Este documento tem por objetivo definir as diretrizes, as responsabilidades e os princípios relativos à Política de Segurança da Informação, elaborada em linha com as melhores práticas do mercado, considerando a natureza e a complexidade das operações, dos produtos, dos serviços, das atividades, dos processos, dos sistemas e dos requisitos de conformidade do banco BTG Pactual, em como em conformidade com a legislação e com regulamentações aplicáveis.

Esta Política é complementada por outros normativos, que compreendem o Sistema de Gestão da Segurança da Informação (SGSI) e de Privacidade (SGPI), assim como a adoção e manutenção da conformidade com o PCI DSS para todos os processos, sistemas e terceiros que armazenam, processam ou transmitam dados do portador do cartão.

## 2. Abrangência e Aplicabilidade

Esta Política tem abrangência Global, aplica-se a todas as empresas subsidiárias e joint ventures sob a gestão e controle do conglomerado prudencial do Banco, áreas e colaboradores do Conglomerado do BTG Pactual (“BTG Pactual”), inclusive consultores externos, equipes temporárias e prestadores de serviço (terceiros) contratados, salvo as empresas que tiverem normativo próprio.

## 3. Definições

**ABNT NBR ISO/IEC 27001:** Norma internacional que define os requisitos para implementar e manter um SGSI (Sistema de Gestão de Segurança da Informação).

**ABNT NBR ISO/IEC 27002:** Oferece orientações práticas sobre como implementar os controles de segurança da informação definidos na 27001.

**ABNT NBR ISO/IEC 27701:** Controles e orientações específicas para privacidade e proteção de dados pessoais.

**BACEN (Banco Central do Brasil):** Regulador do sistema financeiro. Define requisitos de segurança e continuidade de negócios para instituições financeiras.

**CDE:** Ambiente de Dados do Portador do Cartão (Cardholder Data Environment).

**CISO (Chief Information Security Officer):** Diretor de Segurança da Informação. Responsável por liderar estratégias e políticas de segurança cibernética da empresa.

**Chief Executive Officer (CEO):** Diretor Executivo. Principal líder da empresa, responsável pelas decisões estratégicas e pela cultura organizacional.

**Chief Financial Officer (CFO):** Diretor Financeiro. Cuida das finanças e relatórios contábeis da organização.

**Cibersegurança:** Cyber Security ou Cibersegurança, é um termo que determina um conjunto de tecnologias e processos que visam proteger os ativos digitais e do ambiente de eventuais tentativas de intrusões, danos, acessos indevidos a informações e roubo de propriedades intelectuais de uma entidade e/ou determinado grupo.

**CRO (Chief Risk Officer):** Diretor de Riscos. Responsável por gerenciar todos os riscos corporativos, incluindo riscos cibernéticos e de conformidade.

**CSIRT (Computer Security Incident Response Team):** Equipe especializada em responder e investigar incidentes de segurança, como vazamentos, ataques e malware.

**CSSF (Commission de Surveillance du Secteur Financier):** Autoridade financeira de Luxemburgo define normas de segurança e conformidade para instituições financeiras atuantes no país.

**Cyber Defense Center (CDC):** Centro responsável por monitorar, detectar, analisar e responder a incidentes cibernéticos engloba o SOC e o CSIRT.

**Dark Web:** Parte da internet usada muitas vezes para atividades ilegais, como venda de dados e acesso a sistemas comprometidos.

**Gestão da Segurança da Informação (SGSI):** Sistema de gestão baseado na ISO 27001 que define processos, políticas e controles para proteger informações contra acessos não autorizados, vazamentos e interrupções.

**GDPR (General Data Protection Regulation):** Regulamento europeu de proteção de dados pessoais.

**Insiders:** Funcionários ou prestadores de serviço que possuem acesso legítimo a sistemas.

**LGPD (Lei Geral de Proteção de Dados):** Lei brasileira que protege os direitos de privacidade e tratamento de dados pessoais de indivíduos.

**PAN:** Número Primário da Conta (Primary Account Number).

**Pentest (Teste de Penetração):** Simulação controlada de ataque cibernético para identificar vulnerabilidades em sistemas, redes ou aplicações.

**PCI DSS:** Padrão de Segurança de Dados da Indústria de Cartões de Pagamento (Payment Card Industry Data Security Standard)

**Playbooks:** Guias práticos que descrevem passo a passo como agir em cada tipo de incidente.

**SGPI:** Sistema de Gestão de Privacidade da Informação, baseado na ISO 27701, que estabelece práticas para garantir o tratamento correto de dados pessoais, conforme leis como LGPD e GDPR.

**Proteção de workloads:** Proteção de ambientes de trabalho em nuvem, servidores e containers contra ameaças, vulnerabilidades e acessos indevidos.

**SOC (Security Operations Center):** Centro operacional que monitora em tempo real os sistemas da empresa, usando alertas, logs e ferramentas SIEM para detectar ameaças.

**SGSI:** Acrônimo de Sistema de Gestão de Sistema de Informação, plano criado para viabilizar o alcance dos objetivos, constituindo uma declaração formal acerca de seu compromisso.

**Threat Actors:** Atores de ameaça pessoas ou grupos que executam ataques cibernéticos, como hackers, insiders, grupos criminosos ou ativistas.

## 4. Responsabilidades

### 4.1. CISO (Chief Information Security Officer)

O CISO é responsável por atuar no engajamento em Segurança da Informação e Cibernética do conglomerado prudencial do Banco BTG, incluindo o BTG, garantindo que as exigências legais e setoriais sejam devidamente atendidas, atuando no gerenciamento estratégico do tema. É responsável também pela execução do Plano de Ação e de Resposta a Incidentes, visando à implantação desta Política.

### 4.2. Security Office

O Security Office deverá estabelecer os requisitos de segurança para sistemas, infraestrutura, processos, usuários e qualquer outra questão relacionada à segurança na instituição. É a área responsável por garantir os requisitos mínimos de segurança para a instituição e por fazer o monitoramento e resposta à incidentes.

### 4.3. Usuários

Os usuários devem:

- Conhecer as políticas de Segurança da Informação, disponíveis no Security Portal e MyCompliance, e aplicá-las nas suas ações diárias.

- Saber identificar e reportar riscos de segurança da informação.
- Saber identificar e reportar incidentes de segurança da informação.
- Observar a confidencialidade dos dados tratados e tratá-los de acordo com ela.
- Envolver o Security Office no início de projetos que envolvam desenvolvimento de aplicações, armazenamento ou tratamento de dados sensíveis ou de clientes, serviços externos, integração de novas tecnologias ou aquisição de soluções.
- Procurar o direcionamento do Security Office sempre que precisar compartilhar e/ou expor informações sensíveis ou de clientes/funcionários.
- Realizar os treinamentos obrigatórios solicitados pelo Security Office.
- Utilizar apenas ferramentas, softwares e sistemas aprovados pelo BTG Pactual, incluindo suas políticas e critérios de acesso.
- Zelar pela segurança do ambiente e dados sob sua gestão.

#### 4.4. Gestores das Áreas de Tecnologia da Informação (TI)

Os Gestores das áreas de TI devem atuar gestão dos riscos associados à Segurança da Informação e Cibernética, inerentes à aplicação de controles de segurança na infraestrutura e em sistemas informatizados, desenvolvendo as soluções corporativas de forma segura e mantendo o parque tecnológico disponível e atualizado, assegurando que as exposições a esses riscos estejam compatíveis com os limites definidos pela Alta Administração e em linha com as estratégias de negócio do Banco. Os Gestores das Áreas de TI deverão implementar os controles solicitados pelo Security Office que estão sob sua gestão, assegurando a conformidade com essa política.

## 5. Processos Internos

### 5.1. Diretrizes Corporativas

As diretrizes corporativas desta Política, definem as linhas mestras que embasam os processos e os controles de segurança da informação implementados no BTG pelo Security Office.

- **Autenticação:** as credenciais de acesso a sistemas, aplicações e dados devem ser protegidas por controles robustos que garantam a comprovação da identidade do usuário e mitiguem o risco de uso indevido.

- **Mecanismos de Criptografia:** deve ser observada a necessidade da aplicabilidade da criptografia dos dados, em razão da confidencialidade, utilizando-a para proteger informações sensíveis ou críticas.
- **Mecanismos de Prevenção e Detecção de Intrusão:** deve ser implementado controles preventivos e detectivos em camadas para identificar, bloquear e responder a tentativas de intrusão em redes, endpoints, aplicações e serviços do Banco.
- **Mecanismos de Prevenção de Vazamento de Informações:** as informações devem ser atribuídas a proprietários e classificadas de acordo com a sua confidencialidade, sob a proteção necessária, prazo de manutenção, de transferência, de transporte e descarte, em observância às regras corporativas estabelecidas. Devem ser estabelecidos controles de Prevenção Contra Perda de Dados (Data Loss Prevention ou DLP), para bloqueio e restrição não autorizada de compartilhamento de dados internos.
- **Mecanismos de Proteção contra Software Malicioso:** deve ser implementado soluções e processos para prevenir, detectar, conter e erradicar software malicioso nos ativos da informação do BTG.
- **Mecanismos de Rastreabilidade:** os eventos lógicos de sistemas e de serviços, bem como os eventos físicos, capturados e/ou identificados por câmeras, catracas ou áreas restritas do BTG, devem ser devidamente registrados e monitorados.
- **Gestão de Cópias de Segurança dos Dados e das Informações:** deve ser garantida, de forma íntegra e confiável, a restauração de dados registrados nos sistemas de informações ou nos servidores de arquivos do BTG, com foco na preservação da confiabilidade, da integridade e da disponibilidade da informação.
- **Avaliação e Correção de Vulnerabilidades:** deve ter um processo para identificação, avaliação, priorização e correção de vulnerabilidades em ativos, aplicações e serviços, reduzindo a superfície de ataque e o risco cibernético. No processo de desenvolvimento e de atualização de sistemas e de serviços corporativos deve assegurar a aderência às regras e as boas práticas de desenvolvimento seguro. A fim de identificar e de reduzir vulnerabilidades nos ativos de informação, devem ser realizadas, por meio de testes de segurança (manuais e/ou automatizadas), varreduras para identificação de vulnerabilidades.
- **Controle de Acesso:** o acesso a sistemas e a serviços corporativos devem ser apropriados, autorizados e condizentes com as atividades e as funções exercidas pelo usuário (colaborador

ou prestador de serviço terceirizado), visando prevenir o acesso não autorizado e o acúmulo de privilégios.

- **Definição e implementação de perfis de configuração segurança em ativos de tecnologia:** deve ser estabelecido baselines de hardening para sistemas operacionais, dispositivos de rede, bancos de dados, aplicações, dispositivos móveis e serviços em nuvem, reduzindo falhas de configuração.
- **Mecanismos de Proteção da Rede:** deve ser aplicado controles para proteger o tráfego e a infraestrutura de rede contra ameaças, assegurando segmentação, confidencialidade, integridade e disponibilidade dos serviços.
- **Gestão de Certificados Digitais:** deve assegurar a emissão, uso, renovação e revogação seguras de certificados digitais e o resguardo de chaves criptográficas, evitando indisponibilidades e comprometimento.
- **Requisitos de integração de sistemas por meio de interfaces eletrônicas:** deve estabelecer processos a fim de garantir que integrações (APIs, filas, mensageria, EDI, conectores SaaS) sejam seguras, rastreáveis e governadas desde o desenho até a operação.
- **Ações de Inteligência no Ambiente Cibernético:** deve ser implementado processos e tecnologias para coletar, analisar e aplicar Cyber Threat Intelligence (CTI) para antecipar, detectar e responder a ameaças relevantes ao negócio.
- **Conscientização:** as diretrizes de Segurança da Informação, bem como os princípios que norteiam esta Política, devem ser disseminados por meio de programas de comunicação, conscientização e de capacitação, para colaboradores e prestadores de serviço terceirizados.
- **Gestão de Riscos:** os riscos de segurança da informação devem ser identificados, categorizados, reportados e mitigados, por meio de processo definido e devidamente formalizado, com o objetivo de implementar os mecanismos de proteção e os controles de segurança da informação e cibernéticos adequados.
- **Inteligência Artificial (IA):** a IA deve ser usada de forma ética, transparente e livre de vieses discriminatórios. Todo uso de IA deve atender as regras de segurança e legislações aplicáveis, incluindo, mas não se limitando a Lei Geral de Proteção de Dados (LGPD).
- **Utilização de Recursos da Informação:** apenas os equipamentos corporativos, gerenciados ou homologados pelo BTG, podem ser conectados à sua rede corporativa, conforme explicitado no Termo de Acesso e Uso de Sistemas e Informações.

- **Trabalho Remoto:** quando aplicável, o BTG permite o trabalho remoto de seus colaboradores e medidas de segurança da informação devem ser implementadas para garantir a proteção das informações acessadas, processadas ou armazenadas enquanto a execução do trabalho se der de forma remota.
- **Privacidade de Dados:** devem ser estabelecidas diretrizes para assegurar a proteção e o uso adequado de dados pessoais, em conformidade com as legislações aplicáveis, como Lei Geral de Proteção de Dados (LGPD) e outras normas locais.
- **Gestão de Incidentes:** incidentes de segurança da informação e cibernéticos devem ser registrados e classificados de acordo com o seu nível de criticidade, determinado pela exposição e pela relevância dos ativos da informação envolvidos. As ações de contenção, erradicação e de recuperação devem ser documentadas. Os incidentes relevantes, que possam impactar outras instituições ou mercado financeiro com um todo, devem ser reportadas e compartilhadas, conforme diretrizes dos órgãos reguladores vigentes.
- **Cenários de Crise Cibernética:** devem ser catalogados os cenários de crises cibernéticas relacionados a incidentes de segurança e inseridos no relatório de resposta a incidentes relevantes ocorridos no período, incluindo também os resultados dos testes de continuidade desses cenários; e
- **A Política de Segurança da Informação e o Relatório de Segurança Cibernética:** devem ser submetidos e aprovados pelo Conselho de Administração do BTG, no mínimo, anualmente. O Relatório de Segurança Cibernética deve conter o resumo dos resultados obtidos na implementação de rotinas, de processos e de tecnologias utilizados na prevenção e na resposta a incidentes de segurança, bem como incidentes relevantes relacionados com o ambiente cibernéticos, os resultados dos testes de continuidade de negócio considerando cenários de indisponibilidade ocasionada por incidentes e os resultados dos testes de intrusão, varreduras e análises periódicas para detecção de vulnerabilidades.

## 5.2. O Security Office

A área de Segurança da Informação (Security Office) é responsável pela defesa cibernética do BTG, ou seja: é responsável pela proteção dos ativos digitais e do ambiente através da prevenção, detecção e resposta aos incidentes, com o objetivo reduzir riscos e assegurar a resiliência da instituição frente a ameaças e atividades maliciosas.

A estratégia de defesa cibernética do BTG está estruturada de forma a garantir que a estrutura de defesa evolua continuamente, em velocidade compatível com o desenvolvimento dos riscos e

ameaças cibernéticas, aumentando a nossa resiliência a ataques e diminuindo nossas vulnerabilidades e garantindo que os incidentes sejam respondidos com eficácia.

Os objetivos da Gestão da Segurança da Informação (SGSI) e de Privacidade (SGPI) do BTG são:

- **Identificar:** Identificar ativos relevantes para o negócio e acompanhar a evolução dos riscos e ameaças cibernéticas para orientar e priorizar ações de defesa.
- **Proteger:** Desenvolver continuamente a cultura de segurança cibernética no BTG; reduzir nossas vulnerabilidades para assegurar a manutenção de um nível adequado de segurança; proteger a confidencialidade, a integridade, acessibilidade e a privacidade das informações dos nossos colaboradores e clientes.
- **Detectar:** Monitorar os ativos digitais e do ambiente para identificar eventos de segurança.
- **Responder e Recuperar:** Responder com eficácia a incidentes de segurança; assegurar que o BTG se recupere tempestivamente de incidentes; e evoluir nossas defesas a partir das lições aprendidas com os incidentes.

### 5.3. Estrutura de Gerenciamento

O BTG conta com estrutura de Segurança da Informação compatível com a sua natureza, com o porte, com a complexidade, com o perfil de risco e com o modelo de negócio, tendo como função principal assegurar a efetiva gestão dos Riscos de Segurança da Informação e Cibernéticos.

O reporte é feito para o CISO. Fazem parte da Segurança da Informação as seguintes estruturas:

- Security Governance;
- Security Architecture & Operations;
- Application & Offensive Security;
- Cyber Defense Center;
- Identity & Access Management.

### 5.4. Diretoria do Security Office

O BTG considera Segurança da Informação como um dos principais pilares para a sustentação das linhas de negócio, tanto para a estrutura do Brasil quanto para as entidades no exterior. Tendo o CISO como responsável pelas questões de Segurança da Informação, a área reporta direto ao Sênior Management através de diferentes fóruns estabelecidos, de forma a priorizar as ações conforme suas necessidades e sua relevância.

A alta direção se compromete em cumprir todos os requisitos relativos à segurança da informação, sejam estes requisitos legais, regulatórios, ou estabelecidos em contratos e acordos em nome do

BTG, além de todos os requisitos previamente detalhados no nosso SGSI e SGPI, que contempla também a melhoria contínua.

O Security Office é responsável pelo SGSI e o SGPI, monitorando, conduzindo as melhorias de forma contínua e ações corretivas e preventivas, e comunicando as ações para as partes interessadas. Com foco em atender os requisitos de certificação da norma ABNT NBR ISO/IEC 27001, aos controles da norma ABNT NBR ISO/IEC 27002 e aos requisitos de certificação da norma ABNT NBR ISO/IEC 27701:2019 a, visando aumentar o nível de confidencialidade, integridade e disponibilidade das informações e processos críticos de informação do Banco.

Ademais, é de responsabilidade do Security Office, a manutenção do PCI DSS. O BTG mantém a conformidade contínua com o PCI DSS vigente, aplicável a todas as áreas, processos, tecnologias e terceiros que armazenam, processam ou transmitem dados do portador do cartão. Essa diretriz assegura a proteção do PAN (Primary Account Number) e demais dados de conta, mitigando riscos de fraude e garantindo a aplicação consistente de controles de segurança em todo o Ambiente de Dados do Portador do Cartão (CDE).

## **5.5. Atuação do Security Office**

### **5.5.1. Gestão de riscos de segurança**

O Security Office é responsável pela gestão dos riscos de segurança da informação. A partir de uma metodologia que considera nível de comprometimento de confidencialidade, integridade e disponibilidade dos sistemas e informações e a probabilidade de materialização do risco, é dada uma criticidade a cada situação.

Qualquer colaborador do BTG pode identificar um risco de segurança da informação e tem o dever de reportá-lo ao Security Office, que registra, classifica e acompanha a solução do risco.

Uma vez identificados, são definidos planos de ação para minimizar a exposição a tais fatores de risco e, conseqüentemente, a probabilidade da ocorrência de um evento. Os processos realizados estão segregados da seguinte forma:

- Avaliação e identificação de riscos baseado em fatores internos e externos;
- Identificação recorrente de ameaças cibernéticas em âmbito global;
- Avaliação dos possíveis impactos financeiros, operacionais e reputacionais;
- Definição e priorização das respostas frente aos riscos identificados; e
- Revisão periódica dos processos.

Por ser um processo contínuo, a etapa de revisão, executada após a definição e implementação dos planos de ação, visa avaliar se os controles que estão implementados continuam íntegros e

funcionais para os riscos mapeados. Adicionalmente, durante esta etapa é realizado um trabalho de acompanhamento para os planos de ação em aberto, garantindo que foram executados e incluídos na esteira de monitoramento. Mais detalhes podem ser encontrados na Política de Gerenciamento de Riscos Cibernéticos.

### **5.5.2. Privacidade**

O Security Office, em conjunto com o Departamento Jurídico (Legal – LGPD), é responsável por garantir a adequação às leis de privacidade cabíveis aos países e regiões de operação, como por exemplo a GDPR e LGPD. O atendimento às requisições dos titulares de dados também fica à cargo do Security Office.

### **5.5.3. Proteção de Dados**

O Security Office é responsável por evitar vazamento de dados na estrutura do BTG, seja por atores maliciosos externos ou internos. O Security Office pode criar regras para o tratamento e prevenção a vazamento de dados em diversos canais. Nossos canais de comunicação homologados são monitorados ativamente.

Os dados são classificados de acordo com sua criticidade, tendo hoje cinco níveis de classificação. É estritamente proibido qualquer tentativa de vazamento, compartilhamento não autorizado ou exposição de informações confidenciais, dados de clientes/funcionários ou ativos internos do BTG. Essas ações configuram violação grave das políticas corporativas e podem resultar em medidas disciplinares severas, incluindo desligamento, além de responsabilização civil e criminal conforme a legislação vigente.

Contamos com política específica que descreve em detalhes os níveis de classificação e demais procedimentos relacionados

### **5.5.4. Awareness & Training**

A conscientização de segurança para os colaboradores é feita com treinamentos e abordagens específicas para diferentes áreas. O treinamento obrigatório de Segurança da Informação é revisado anualmente, portanto, os colaboradores precisam refazê-lo todos os anos.

O Security Office pode implementar políticas para limitar o acesso à rede do banco ou outros sistemas em caso de colaboradores que não concluírem o Treinamento Obrigatório de Segurança da Informação.

O Security Office envia periodicamente comunicados para todos os colaboradores com informações relevantes sobre Segurança da Informação. Os colaboradores devem ler atentamente e aplicar as informações no seu dia a dia.

#### **5.5.5. Segurança de Infraestrutura e Aplicações**

O Security Office é responsável pela segurança das aplicações desenvolvidas internamente, com a revisão do código feito pelos desenvolvedores e testes de penetração (pentest) nessas aplicações. Todas as vulnerabilidades encontradas são classificadas quanto ao nível de risco e direcionadas para correção, com prioridade conforme o risco.

Além disso, o Security Office atua para aprimorar as métricas do Cyber Defense Center por meio de exercícios periódicos que visam explorar as vulnerabilidades do ambiente e reproduzir ameaças através do uso de técnicas sofisticadas do mundo real.

Os desenvolvedores devem sempre contactar o Security Office antes do início do desenvolvimento de novos produtos para que haja um acompanhamento adequado. Vulnerabilidades críticas ou altas impedem o produto de ser lançado para produção. Todas as vulnerabilidades possuem SLA para correção, que precisam ser observados e cumpridos pelos desenvolvedores.

O Security Office também realiza scans na rede para identificar vulnerabilidades na infraestrutura. As vulnerabilidades são corrigidas conforme política específica.

Além da identificação de vulnerabilidades, o Security Office define regras para configuração dos dispositivos (workstations, servidores, ativos de redes e outros recursos) que devem ser cumpridas pelos times responsáveis por sua manutenção. Dentre os controles, destacam-se:

- Instalação de ferramentas de anti-malware;
- Remoção de administradores locais;
- Controle de saída de internet;
- Hardenização dos dispositivos;
- Configuração segura de protocolos (desativação de serviços inseguros);
- Criptografia de dados em repouso e em trânsito;
- Monitoramento e registro de logs para auditoria;
- Bloqueio de dispositivos não conformes antes do acesso à rede corporativa.

#### **5.5.6. Gestão de Terceiros**

Ao contratar quaisquer novos produtos ou suporte para o ambiente, seja de Tecnologia ou qualquer outra área, é obrigatório que o responsável pelo contrato informe ao Security Office.

As diretrizes e parâmetros para a gestão de terceiros são detalhados em políticas específicas, seja a que possui os requisitos de segurança e é divulgada aos prestadores de serviços e fornecedores, seja a que determina o fluxo de avaliação e gestão entre as áreas de controle do BTG. Tal fluxo engloba tanto o processo de avaliação na contratação do fornecedor, quanto possíveis inserções ou alterações em contratos que abrangem os requisitos.

O Security Office define critérios mínimos para conexão com o nosso ambiente ou utilização de serviços externos, de acordo com a natureza do produto. Esses critérios devem ser observados e seguidos sem exceções.

O Security Office pode identificar, através de Due Diligences ou ferramentas de monitoramento, falhas na infraestrutura ou produtos terceiros. Essas falhas serão reportadas e devem ser tratadas de forma tempestiva.

Os contratos com terceiros com processamento em nuvem são reportados aos reguladores (BACEN, SUSEP, CSSF), de acordo com diretrizes e regulamentações vigentes.

Mais detalhes encontram-se na Política de Segurança da Informação para Terceiros.

#### **5.5.7. Arquitetura e Segurança de Nuvem**

O Security Office possui um time focado em arquitetura e segurança para ambiente em nuvem (Cloud Security), responsável pela definição de políticas, procedimentos, controles e tecnologias para proteger dados, aplicativos e serviços de infraestrutura em nuvem pública, atuando nos pilares de gestão de acesso, monitoramento e detecção, proteção de workloads e dados.

Essas medidas de segurança protegem um ambiente de computação em nuvem contra ameaças, e vulnerabilidades externas e internas em relação à segurança cibernética.

A adoção de serviços em nuvem exige controles robustos para garantir a confidencialidade, integridade e disponibilidade das informações. O Security Office é responsável por implementar e manter práticas Gerenciamento de Identidades e Acessos (IAM), assegurando que apenas usuários autorizados tenham acesso aos recursos, com base no princípio do menor privilégio.

Entre as principais diretrizes estão:

- Gestão centralizada de identidades para todos os ambientes (on-premises e cloud).
- Autenticação forte (MFA) para acesso a serviços críticos.
- Segregação de funções e revisão periódica de permissões.
- Monitoramento contínuo de acessos e alertas para atividades suspeitas.
- Integração com políticas para garantir conformidade regulatória (CVM, Bacen, LGPD).

### 5.5.8. Resposta à incidentes

As atividades desempenhadas pelo SOC (Centro de Operações de Segurança) e pelo CSIRT (Time de Resposta a Incidentes de Segurança) são de suma importância para o monitoramento e resposta aos eventos e aos incidentes que porventura a instituição venha a sofrer. Seguindo as boas práticas de mercado, listamos as principais atividades desempenhadas:

- SOC 24x7;
- Resposta a todos os incidentes e ameaças, com o devido tratamento;
- Simulação de cenários de incidentes críticos de segurança;
- Automação de playbooks de resposta à incidentes; e
- Garantia da efetividade de regras preventivas nas ferramentas e manutenção do ambiente atualizado e operacional.

A simulação de cenários que podem causar a indisponibilidade dos processos avaliados como críticos para a continuidade das atividades considera nossas principais ameaças de segurança. Todos esses cenários possuem plano de resposta, garantindo a continuidade do negócio.

As atividades mencionadas visam, principalmente, estabelecer um fluxo de trabalho em resposta aos eventos de risco e aos incidentes de forma tempestiva, analisando a causa-raiz, bem como a definição de planos de ação, para que o problema seja corrigido de forma definitiva. Os alertas gerados pelas ferramentas de monitoramento do SOC são classificados em diferentes níveis de prioridade. Com isso, é possível priorizar a atuação dos esforços na análise e no tratamento dos eventos. As informações relevantes de possíveis ataques são compartilhadas com outras empresas do grupo.

Ao ser identificado um incidente relevante, ele será reportado pelo BTG aos órgãos competentes e aos titulares de dados e terceiros envolvidos, em até 72h após a identificação ou conforme legislação aplicável, a depender do business e países onde se encontra. Os detalhes do prazo de comunicação estão explicitados em nosso Plano de Resposta à Incidentes de Segurança da Informação. Essa comunicação considera as exigências de reguladores como: SUSEP, BACEN, CVM, DORA, S-P, NSI2, ANPD, OCC, SEC e FINRA, por exemplo.

A área também concentra a atividade Inteligência de Ameaças, responsável por identificar antecipadamente, compreender as técnicas, e atuar contra os variados atores de ameaça que miram as unidades de negócio do banco, a marca ou nossas investidas, seja através de nossa rede, da dark e deep web, de mídias sociais ou de insiders e de terceiros mal-intencionados.

### **5.5.9. Gestão de Identidades**

O Security Office concede, revisa, remove e muda o perfil de acesso de todos os usuários do banco ao ambiente corporativo e aos sistemas críticos do business. A principal missão é garantir que todos os usuários do BTG tenham apenas os acessos apropriados à execução de suas funções e com o mínimo privilégio necessário.

A concessão de acesso deve ser solicitada pelo usuário, pelo seu gerente direto, ou pelo RH, segundo um perfil de acesso específico e compatível às atividades realizadas, podendo ser requisitado a qualquer momento.

A revisão de acesso constitui a verificação periódica da necessidade de manutenção do acesso dos usuários, de troca do perfil ou de reestruturação dos acessos devidos à cada perfil. Com isso, busca-se garantir que os usuários possuam o mínimo privilégio necessário, que estão com o perfil apropriado associado, e que os acessos contemplados por cada perfil estão atualizados.

A remoção de acesso é efetuada após solicitação direta do usuário, finalização do processo de revisão de acesso, ou o desligamento do funcionário.

A mudança do perfil de acesso pode ocorrer em casos de mudança de funções por parte do usuário, ou identificação de perfil que melhor se adeque às necessidades do funcionário.

O Security Office estabelece critérios para autenticação dos sistemas de acesso do usuário, que devem ser seguidos pelos times que tem gestão sobre os sistemas e pelos usuários.

### **5.6. Medidas Disciplinares**

O BTG se compromete a aplicar as medidas cabíveis para detectar irregularidades e violações ao conteúdo dessa política. A apuração dos casos identificados será feita de forma justa e imparcial, de acordo com as normas e legislações vigentes, aplicando as medidas sancionatórias proporcionais aos atos praticados.

As sanções poderão atingir esferas administrativas e criminais, podendo resultar em advertências verbais ou escritas, suspensão e rescisão de contrato de trabalho, ou até mesmo em ações judiciais, segundo legislação. O BTG se compromete a colaborar com possíveis investigações e decisões judiciais, na extensão da confidencialidade permitidas por Lei.

## **6. Alçadas**

Não aplicável.

## 7. Exceções

Qualquer exceção à esta política deverá ser aprovada pelo Security Office.

## 8. Documentos e Normativos Relacionados

Esta política é regida por melhores práticas, regulamentações específicas, bem como suas eventuais atualizações e mudanças normativas, tais como:

- ISO 27001
- ISO 27701
- BACEN 4893
- SUSEP 638
- PCI DSS
- DORA
- S-P
- NSI2
- CVM
- IT 001 – GLOBAL – Controle de Acesso
- IT 002 – BRASIL – Segurança de Aplicativos
- IT 003 – GLOBAL – Software e Hardware Aprovados
- IT 006 – GLOBAL – Retenção, Backup e Recuperação de Dados
- IT 008 – GLOBAL – E-mail e Mensagens Eletrônicas
- IT 017 – GLOBAL – Acesso Remoto
- IT 018 – GLOBAL – Registro de Logs e Monitoramento de Segurança
- IT 019 – GLOBAL – Uso da Internet
- IT 020 – GLOBAL – Proteção Contra Vírus e Malware
- IT 021 – GLOBAL – Gestão de Vulnerabilidades
- IT 022 – GLOBAL – Segurança, Classificação e Privacidade de Dados
- IT 043 – GLOBAL – Gerenciamento de Incidentes de Segurança da Informação
- IT 044 – BRASIL – Segurança da Informação para Terceiros
- IT 045 – BRASIL – Segurança da Informação para Agentes Autônomos de Investimento

## Controle de Atualização

Versão	Motivo da Alteração	Responsável	Área	Data
1	-	Pedro Nejm	Security Office	Fevereiro/2019
2	Revisão anual	Leticia Rodrigues	Security Office	Janeiro/2021
3	Revisão anual	Leticia Rodrigues	Security Office	Janeiro/2022
4	Revisão anual	Leticia Rodrigues	Security Office	Setembro/2022
5	Revisão anual	Leticia Rodrigues	Security Office	Setembro/2023
6	Revisão anual	Leticia Rodrigues	Security Office	Abril/2024
7	Revisão anual	Leticia Rodrigues	Security Office	Novembro/2024
8	Reestruturação da política	Leticia Rodrigues	Security Office	Novembro/2025
9	Adequação a resolução CMN 5.274/25	Luiz Buononato	Security Office	Abril/2026