Política de Segurança da Informação

Security Office

Novembro 2024

Índice

1. Princípios

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. Uma estrutura de Cyber Security visa realizar tanto o monitoramento e a proteção dos ativos digitais e do ambiente, através de controles e procedimentos.

2. Objetivos

O objetivo dessa política é estabelecer as diretrizes para a atuação Security Office e definir as responsabilidades dos usuários. Ela é complementada pelas demais políticas que compreendem o Sistema de Gestão da Segurança da Informação (SGSI) e de Privacidade (SGPI).

3. Funções e Responsabilidades

3.1. 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.

3.2. Usuários

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

Em situações em que o usuário pode acabar expondo informações do BTG Pactual e/ou de seus clientes e funcionários, o usuário deve procurar o direcionamento do Security Office. O usuário deve conhecer o risco de segurança das suas ações e atuar de maneira a minimizá-lo.

3.3. Gestão de TI

A gestão de TI deverá implementar os controles solicitados pelo Security Office que estão sob sua gestão, assegurando a conformidade com essa política.

4. O Security Office

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

A estratégia de defesa cibernética do BTG Pactual 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 que os incidentes sejam respondidos com eficácia.

Os objetivos da Gestão da Segurança da Informação (SGSI) e de Privacidade (SGPI) do BTG Pactual 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 Pactual; 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 Pactual se recupere tempestivamente de incidentes; e evoluir nossas defesas a partir das lições aprendidas com os incidentes.

Fazem parte da Segurança da Informação as seguintes estruturas:

- Security Governance;
- Security Architecture;
- Application Security;
- Cyber Defense Center;
- IDM.

4.1. Estrutura de Cibersegurança

Diretoria de Segurança da Informação

O BTG Pactual 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 (Chief Information Security Officer) como responsável pelas questões de Segurança da Informação, a área reporta direto ao Senior Management através de diferentes fóruns e comitês 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 Pactual, além de todos os requisitos previamente detalhados no nosso Sistema de Gestão da Segurança da Informação (SGSI) e de Privacidade (SGPI), que contempla também a melhoria contínua.

O Security Office é responsável pelo Sistema de Gestão de Segurança da informação (SGSI) e o Sistema de Gestão de Privacidade (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 BTG Pactual.

5. Atuação do Security Office

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 Pactual 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, consequentemente, 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 follow-up 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.

5.2. Privacidade

O Security Office, em conjunto com o Departamento Jurídico, 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.

5.3. Proteção de Dados

O Security Office é responsável por evitar vazamento de dados na estrutura do BTG Pactual, 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.

Os dados são classificados de acordo com sua criticidade, tendo hoje cinco níveis de classificação. Contamos com política específica que descreve em detalhes os níveis de classificação e demais procedimentos relacionados.

Nossos canais de comunicação homologados são monitorados ativamente.

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. Gestão de Vulnerabilidades & Segurança Ofensiva

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, 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. Certifica que os alertas das ferramentas de controle estão funcionando corretamente para todos os ambientes e localidades.

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.

O time de Segurança da Informação também realiza scans na rede para identificar vulnerabilidades na infraestrutura. As vulnerabilidades são corrigidas conforme política específica.

5.6. Gestão de Terceiros

Ao contratar quaisquer novos produtos ou suporte para o ambiente, seja de IT ou qualquer outra área, é obrigatório que o responsável pelo contrato submeta a requisição à área de Contracts & Procurement.

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 Pactual. Tal fluxo engloba tanto o processo de avaliação na contratação do fornecedor, quanto possíveis inserções ou alterações em contratos que abranjam os requisitos.

Os contratos com terceiros com processamento em nuvem são reportados aos reguladores (BACEN, SUSEP, CSSF) de acordo com sua criticidade.

5.7. Arquitetura

O Security Office possui um time focado em Cloud Security e arquitetura e atua na 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.

Além disso, o Security Office faz segurança em camadas, considerando camadas de perímetro, dados, aplicação, endpoint, nuvem e redes para garantir que a proteção contra ameaças funcione adequadamente.

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 crítico, ele será reportado pelo BTG Pactual aos órgãos competentes e aos titulares de dados e terceiros envolvidos, caso seja necessário.

A área também concentra as atividades de Proteção de Dados e Inteligência de Ameaças. Esta última é responsável por identificar antecipadamente, compreender as técnicas, e atuar contra os variados "Threat actors" que miram as unidades de negócio do banco, a marca ou nossas investidas, seja através de nossa rede, da dark web, de mídias sociais ou de insiders e de terceiros mal-intencionados.

5.9. Gestão de Identidades

Equipe responsável por conceder, revisar, remover e mudar 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 Pactual 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.

5.10. Comitês

Comitê de Riscos

O Comitê de Riscos tem por objetivo assessorar o Senior Management na supervisão da tomada de riscos da Instituição, bem como na gestão dos riscos financeiros e não financeiros, incluindo os riscos de mercado, crédito, operacional, liquidez, socioambiental e tecnológicos. Desta forma, as principais preocupações identificadas pela equipe de Segurança da Informação, bem como os planos de ação, são discutidos neste fórum com o intuito de compartilhar com o CRO (Chief Risk Officer) o nível de exposição ao risco que a instituição apresenta. Participam deste fórum as áreas de Risco de Mercado, Risco de Crédito, Risco Operacional e Segurança da Informação.

Comitê de Controles Internos

Este comitê reúne os gestores das áreas de Segurança da Informação, Risco Operacional, Auditoria, Compliance, além do Chief Risk Officer (CRO), Chief Financial Officer (CFO) e Chief Executive Officer (CEO) para que todos obtenham uma visão integrada e analítica a respeito do funcionamento e qualidade dos controles internos. Realiza uma reunião destinada para as áreas de controles avaliarem a efetividade e consonância do sistema de controles internos de uma área gestora específica ou da organização, certificando a conformidade de procedimentos com as normas, regulamentos e leis aplicáveis, devendo submeter à área avaliada e ao Senior Management o diagnóstico obtido.

6. Medidas Disciplinares

O BTG Pactual 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 escritas, suspensão e demissão, ou até mesmo em ações judiciais, segundo legislação.
O BTG Pactual se compromete a colaborar com possíveis investigações e decisões judiciais, na extensão da confidencialidade permitidas por lei.

7. Renúncias / Exceções

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