Getnet

Política de Segurança Cibernética



ÍNDICE

1. OBJETIVO 3
2. ABRANGÊNCIA 3
3. APLICAÇÃO NORMAS E CERTIFICAÇÕES 3
4. TERMOS E DEFINIÇÕES 3
5. DISPOSIÇÕES GERAIS 4
6. DIRETRIZES 4
7. RESPONSABILIDADES 8
8. CONTROLES E INDICADORES 8
9. ANEXOS 8
10. REFERÊNCIAS 8
11. HISTÓRICO DE REVISÕES 9

As informações contidas neste documento são classificadas de acordo com seu conteúdo e protegidas por sigilo profissional.

1. OBJETIVO

Esta política define as diretrizes para identificar, proteger, detectar, responder e recuperar de ameaças cibernéticas, a fim de proteger o ambiente, os ativos, informações e clientes da Getnet. Estabelece medidas para garantir a confidencialidade, a disponibilidade e a integridade dos dados, das informações e dos sistemas de informação utilizados pela Getnet, através de controles tecnológicos e organizacionais estruturados para proteger, detectar e reduzir vulnerabilidades que possam gerar incidentes de segurança da informação, bem como manter a conformidade com as diretrizes corporativas e regulatórias aplicáveis.

2. ABRANGÊNCIA

(x) Getnet ( ) Auttar ( ) SCD ( ) GetAtende ( ) Eyemobile ( ) Mobyan

3. APLICAÇÃO NORMAS E CERTIFICAÇÕES

( ) Auditoria (x) BACEN ( ) ISO ( ) PCI ( ) SOx ( ) Outros

Outros, especificar:

4. TERMOS E DEFINIÇÕES

Confidencialidade: Preservar as restrições autorizadas ao acesso e divulgação de informações, incluindo meios para proteger a privacidade pessoal e informações proprietárias.

Criptografia: O processo de transformar texto simples em texto cifrado usando um algoritmo criptográfico e uma chave.

Disponibilidade: a propriedade que garante o acesso e o uso oportunos e confiáveis das informações.

Evento cibernético: Uma ocorrência de risco de segurança cibernética observável em um sistema de informação ou nas informações que o sistema processa, armazena ou transmite.

Integridade: A propriedade de que os dados não foram modificados ou excluídos de maneira não autorizada e não detectada.

5. DISPOSIÇÕES GERAIS

Todo documento sem tarja (obsoleto/em revisão) é considerado vigente desde que disponível na Plataforma de Documentos.

Os colaboradores envolvidos no processo em questão estão cientes de que as diretrizes definidas neste documento poderão ser auditadas e devem auxiliar o Auditor na obtenção de dados que subsidiem seu trabalho com informações suficientes, fidedignas, relevantes e úteis, como base sólida para emissão de seu relatório final.

Portanto, recomenda-se não salvar cópias dos normativos na área de trabalho/diretórios da rede ou imprimi-los. O colaborador deve sempre acessar a Plataforma de Documentos.

Este documento encontra-se no padrão de formatação definido pela ABNT NBR 14724:2011, portanto, o redator deve garantir que a formatação e estrutura do documento siga os padrões já definidos.

6. DIRETRIZES

Diretrizes sobre princípios, procedimentos e controles de Segurança Cibernética, aplicáveis a todos os dados, sistemas de informação, processos, pessoas e terceiros que suportam as operações da Getnet.

• **Autenticação forte e gestão de identidades e acessos (IAM/PAM):** a Getnet adota configurações seguras de autenticação de usuários, bem como de gestão de acessos padrão e privilegiado para o adequado gerenciamento do ciclo de vida da identidade do usuário. Mecanismos adequados de controle de acesso protegem contra o acesso não autorizado a sistemas ou dados, o que poderia levar à perda de confidencialidade, disponibilidade e integridade.

• **Criptografia em trânsito e em repouso, certificados digitais e gestão de chaves:** são aplicados protocolos seguros de criptografia para dados em trânsito e em repouso, para proteção adequada de dados. Chaves de criptografia são protegidas gerenciadas por meio de processos e ferramentas específicas. Certificados digitais são armazenados e gerenciados de maneira segura para garantir sua proteção e validade.

• **Prevenção e detecção de intrusão (IDS/IPS), proteção contra DDoS:** são configurados e monitorados os mecanismos e ferramentas de proteção e detecção de ameaças.

• **Inteligência cibernética:** informações sobre ameaças de diversas fontes internas e externas são coletadas para antecipar intenções, ferramentas e técnicas de ameaças cibernéticas, e disseminadas para conscientização e implementação de ações recomendadas de prevenção e/ou mitigação.

• **Prevenção de vazamento de informações:** são definidas medidas para prevenção de perda de dados para garantir que a informação esteja protegida contra modificação, perda, divulgação ou acesso não autorizado, por meio de diretrizes e ferramentas para o processamento, armazenamento e transmissão de dados. Todos as pessoas colaboradoras contribuem para a proteção dos dados contra ameaças online e físicas.

• **Mecanismos de rastreabilidade (logging e trilhas de auditoria):** a Getnet mantém mecanismos de rastreabilidade que garantem logs, trilhas de auditoria e retenção adequada, com proteção contra alterações não autorizadas.

• **Testes e varreduras periódicas de vulnerabilidades e correções com SLA:** são realizados testes regulares para a identificação, gestão e correção de vulnerabilidades através de:

- Classificação de vulnerabilidades de acordo com o CVSS.
- Identificação de ativos e inventário atualizado de sistemas e informações de TI.
- Testes de segurança regulares, incluindo varredura de vulnerabilidades, aplicação de patches, testes de penetração, testes contínuos ofensivos e testes de penetração orientados a ameaças.

As informações contidas neste documento são classificadas de acordo com seu conteúdo e protegidas por sigilo profissional.

- Gestão e correção de vulnerabilidades baseadas em risco.

• **Proteção contra softwares maliciosos (antimalware/EDR) e filtragens de e-mail/web:** é implementada proteção adequada contra malwares, bem como filtragem de mensagens e conteúdo online para navegação segura. São definidos requisitos de segurança nos dispositivos e redes a fim de identificar, bloquear e responder a esses ataques de segurança cibernética.

• **Controles de acesso e segmentação de redes (firewalls, DMZ, microsegmentação):** as redes e os fluxos de informação são devidamente protegidos por meio de sistemas, ferramentas e serviços instalados, operados e mantidos, seguindo uma série de diretrizes e processos de segurança.

• **Cópias de segurança:** a organização mantém procedimentos específicos para garantir a cópia e recuperação de dados e informações quando necessário.

• **Desenvolvimento e aquisição seguros de soluções de TI:** são estabelecidos os requisitos de cibersegurança ao longo de todo o ciclo de vida de desenvolvimento ou aquisição de soluções de TI e as bases para processos seguros para novas ou grandes alterações em soluções de TI. Estes requisitos estendem-se à integração de sistemas de informação por meio de interfaces eletrônicas.

• **Segurança em nuvem:** são estabelecidos critérios e requisitos mínimos de segurança para o armazenamento, processamento e/ou transferência de dados na nuvem, de acordo com os níveis de confidencialidade de dados definidos.

• **Gestão de riscos de terceiros:** são estabelecidos critérios para certificar serviços de terceiros de acordo com seus riscos, incluindo o de segurança cibernética, e relevância, além de monitorar e tentar controlar o risco cibernético decorrente de serviços de terceiros durante o período do contrato.

As informações contidas neste documento são classificadas de acordo com seu conteúdo e protegidas por sigilo profissional.

6.1. Gerenciamento de Incidentes Cibernéticos

Os incidentes cibernéticos são registrados, analisados quanto à causa raiz e impacto, e tratados de acordo o seu nível de gravidade a fim de conter efeitos indesejados. O processo considera também informações recebidas ou relatadas através de prestadores de serviços terceirizados.

Caso um incidente de origem cibernética seja identificado pelo público geral, o mesmo deverá ser reportado pelo e-mail cybersecurityincidents@gruposantander.com .

6.2. Gestão de Continuidade de Negócio

A Getnet mantém um Plano de Continuidade de Negócios (PCN) que inclui um Plano de Continuidade de Tecnologia (PCT) com objetivo de que a entidade esteja preparada para manter a disponibilidade dos processos de negócios críticos. Estão estabelecidos mecanismos de ativação dos planos de continuidade de negócios em caso de desastres, tanto de origem cibernética como operacional.

Os requisitos de segurança cibernética são aplicáveis às seguintes atividades:

- É realizada uma avaliação de cenários de contingência considerando os cenários cibernéticos.
- Os requisitos e controles de segurança cibernética são incluídos no PCT para mitigar o risco identificado na avaliação de cenários cibernéticos.
- O plano anual de testes de recuperação incorpora cenários cibernéticos.

A Getnet realiza, pelo menos anualmente, testes de continuidade dos serviços de negócio críticos, prevendo indisponibilidade por incidentes, bem como define que devem ser testados cenários que envolvam a indisponibilidade de seus serviços críticos de negócio (definidos de acordo com a análise de impacto ao negócio – BIA) que ocasionem a paralisação das operações normais do seu ambiente produtivo de tecnologia da informação.

As informações contidas neste documento são classificadas de acordo com seu conteúdo e protegidas por sigilo profissional.

7. RESPONSABILIDADES

Cyber Segurança

- Gestão das políticas e procedimentos de segurança
- Definição de diretrizes específicas para tecnologias críticas
- Implementação e manutenção de ferramentas e controles de segurança
- Assegurar que as pessoas, processos e produtos estejam em conformidade com as diretrizes de segurança
- Detectar e tratar incidentes de segurança

Gestão de Continuidade de Negócio

- Manter um plano de continuidade de negócio atualizado e aderente às necessidades da entidade

ITSM – Information Technology Service Management

- Executar testes de recuperação de desastre.

Suprimentos

- Realizar a gestão e avaliação de fornecedores.

8. CONTROLES E INDICADORES

N/A

9. ANEXOS

N/A

10. REFERÊNCIAS

RESOLUÇÃO BCB Nº 85, DE 8 DE ABRIL DE 2021

As informações contidas neste documento são classificadas de acordo com seu conteúdo e protegidas por sigilo profissional.

11. HISTÓRICO DE REVISÕES

Versão	Data	Descrição alteração	Responsável
1	02/10/2019	Criação do Documento. Document Creation	Guilherme de Sá Gattino
2	24/08/2020	Atualização do normativo para o novo padrão de políticas da Getnet. Inclusão de referência à Política de Privacidade da Getnet. Inclusão do termo COMEX nas referências do documento com relação ao Conselho de Administração da Getnet. Update of the regulation to the new Getnet policy standard. Inclusion of a reference to Getnet's Privacy Policy. Inclusion of the term COMEX in the document's references to Getnet's Board of Directors.	Guilherme de Sá Gattino
3	15/02/2021	Alterada a diretriz 7.3 para incluir definição de cenários de incidentes considerados nos testes de continuidade dos serviços de pagamento. Amended guideline 7.3 to include definition of incident scenarios considered in payment service continuity testing.	Guilherme de Sá Gattino e Adriano Moraes
4	30/03/2022	Atualização do normativo para o novo padrão de políticas da Getnet. Atualização das Resoluções vigente no item 8. Update of the regulation to the new Getnet policy standard. Update of the Resolutions in force in item 8.	Priscila Souza
5	24/03/2023	Atualização para o novo modelo padrão de políticas. Ajuste da terminologia de políticas e procedimentos 6.4 Atualização da alçada de aprovação do procedimento. 6.6 Ajuste do nome do comitê. Updated to the new default policy template.	Raquel Oliveira

As informações contidas neste documento são classificadas de acordo com seu conteúdo e protegidas por sigilo profissional.

		Adjusting policy and procedure terminology 6.4 Update of the approval authority of the procedure. 6.6 Adjustment of the Committee Name.	
6	18/03/2024	Ajuste para novo modelo de política. Atualização da terminologia de políticas e procedimentos mencionados no corpo da política. Inclusão do parágrafo 6.6 Adjustment for a new policy model. Updated the terminology of policies and procedures mentioned in the body of the policy. Inclusion of paragraph 6.6	Raquel Oliveira
7	07/03/2025	Ajuste para novo modelo e a inclusão dos campos 7 Responsabilidade e 8 controles e indicadores. Aprovado pelo Conselho de Administração em nov/24. Adjustment to the new model and the inclusion of fields 7 Responsibility and 8 controls and indicators. Approved by the Board of Directors in Nov/24.	Gabriel Gulart Rodrigues
8	17/09/2025	Ajuste e tradução da política para português (BR) o inglês (US). Adjustment and translation of the policy into Portuguese (BR) or English (US).	Valter Filho
9	01/04/2026	Atualização geral da política para adequação à atualização da Resolução BCB 85 em 18/12/2025	Raquel Oliveira

As informações contidas neste documento são classificadas de acordo com seu conteúdo e protegidas por sigilo profissional.