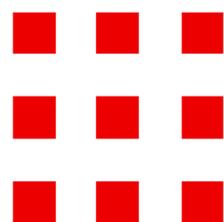


Getnet

Política de Segurança Cibernética



	POLÍTICA				
	() INTERNA		() CORPORATIVA		(X) REGULATÓRIA
	Política de Segurança Cibernética			SIGLA	PL 321
				DATA DE LIBERAÇÃO	07/03/2025
				DATA DE VIGÊNCIA	07/03/2026
RESPONSÁVEL:	SEGURANÇA DA INFORMAÇÃO		VERSÃO	07	
Classificação da Informação: (x) PÚBLICO () INTERNO () CONFIDENCIAL () CONFIDENCIAL RESTRITO () SECRETO					

ÍNDICE

1. OBJETIVO	2
2. TERMOS E DEFINIÇÕES.....	2
3. DIRETRIZES	2
4. RESPONSABILIDADES	6
5. ANEXOS.....	6

	POLÍTICA				
	() INTERNA		() CORPORATIVA		(X) REGULATÓRIA
	Política de Segurança Cibernética			SIGLA	PL 321
				DATA DE LIBERAÇÃO	07/03/2025
				DATA DE VIGÊNCIA	07/03/2026
RESPONSÁVEL:	SEGURANÇA DA INFORMAÇÃO		VERSÃO	07	
Classificação da Informação: (x) PÚBLICO () INTERNO () CONFIDENCIAL () CONFIDENCIAL RESTRITO () SECRETO					

1. OBJETIVO

Definir as diretrizes para garantir a confidencialidade, a disponibilidade e a integridade dos dados e das informações da Getnet e dos sistemas de informação utilizados, através de controles tecnológicos e de recursos humanos capacitados para prevenir, detectar e reduzir vulnerabilidades que possam gerar incidentes de segurança da informação. Definir diretrizes para identificar, proteger, detectar, responder e recuperar rapidamente de uma ameaça cibernética, a fim de proteger a confidencialidade, integridade e disponibilidade dos ativos tecnológicos e informações.

2. TERMOS E DEFINIÇÕES

N/A

3. DIRETRIZES

- 3.1. A Getnet mapeia, gerencia e controla todos os riscos de segurança da informação, conforme definido no **PR 107 - GN.TEC.SEI Procedimento De Gestão De Riscos De Segurança Da Informação.**
- 3.2. A Getnet implementa diretrizes específicas para a proteção das informações de sua responsabilidade tais como:
- a) Implementação de hardening em todos os seus ativos tecnológicos, conforme definido na **PL 022 – GN.TEC.SEI Política de Hardening.**
 - b) Identificação de vulnerabilidades técnicas, através de processos de análise periódicos e implementação de correções dentro de prazos definidos, conforme o **PR 018 - GN.GTI.SIN Procedimento de Gestão de Vulnerabilidades Técnicas.**

	POLÍTICA				
	() INTERNA		() CORPORATIVA		(X) REGULATÓRIA
	Política de Segurança Cibernética			SIGLA	PL 321
				DATA DE LIBERAÇÃO	07/03/2025
				DATA DE VIGÊNCIA	07/03/2026
RESPONSÁVEL:	SEGURANÇA DA INFORMAÇÃO		VERSÃO	07	
Classificação da Informação: (x) PÚBLICO () INTERNO () CONFIDENCIAL () CONFIDENCIAL RESTRITO () SECRETO					

c) Segmentação das redes lógicas, uso de detectores de intrusão, instalação de antimalware nos servidores aplicáveis e rastreamento lógico através de trilhas de auditoria, conforme as diretrizes da **PL 066 - GN.GTI.SIN Política de Rotinas Operacionais**.

d) Definição de diretrizes específicas para tecnologias críticas, tais como utilização da internet (**PL 042 - GN.GTI.SIN Política de Uso da Internet**), disponibilização de recursos (**PL 067 GN.GTI.SIN Política de Disponibilização de Recursos**), envio de mensagens eletrônicas (**PL 068 - GN.GTI.SIN Política de Uso de Mensagens Eletrônicas**), uso de dispositivos móveis e trabalho remoto (**PL 070 - GN.GTI.SIN Política de Uso de Dispositivos Móveis e Trabalho Remoto**).

e) Controle dos acessos físicos e lógicos, conforme as diretrizes da **PL 065 - GN.TEC.SEI Política de Controle de Acessos Físico e Lógico**.

f) Definição de diretrizes para o manuseio e proteção das cópias de segurança (i.e., backup), conforme a **PL 043 - GN.GPN.ITI Política de Cópias de Segurança**.

3.3. A Getnet realiza, pelo menos anualmente, testes de continuidade dos serviços de pagamento, prevendo indisponibilidade destes serviços por incidentes, conforme definições na Política **PL 497 - GN.RCO.GRI Política Corporativa de Gestão de Continuidade de Negócios** e no procedimento **PR 039 - GN.TEC.GVT Procedimento de DRP**.

a) A Getnet define que devem ser testados cenários que envolvam a indisponibilidade de seus serviços críticos de pagamento (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. Os cenários abrangem, pelo menos:

- i. Situações de incêndio/inundação;
- ii. Impedimentos de acesso ao Data Center;
- iii. Greve;

	POLÍTICA				
	() INTERNA		() CORPORATIVA		(X) REGULATÓRIA
	Política de Segurança Cibernética			SIGLA	PL 321
				DATA DE LIBERAÇÃO	07/03/2025
				DATA DE VIGÊNCIA	07/03/2026
RESPONSÁVEL:	SEGURANÇA DA INFORMAÇÃO		VERSÃO	07	
Classificação da Informação: (x) PÚBLICO () INTERNO () CONFIDENCIAL () CONFIDENCIAL RESTRITO () SECRETO					

- iv. Falha prolongada em equipamentos de processamento de dados, infraestrutura e/ou instalações físicas e serviços de provedores externos;
- v. Catástrofes da natureza;
- vi. Terrorismo;
- vii. Catástrofes gerais não naturais, como queda de avião e explosão.

3.4. A Getnet possui definições específicas para o gerenciamento de incidentes de segurança da informação através da **PL 208 - GN.GTI.SIN Política de Gestão de Incidentes de Segurança da Informação**.

- a) As notificações de incidentes de segurança da informação seguem de acordo com a política mencionada acima em 6.4.
- b) Os incidentes identificados pela Getnet são tratados de acordo com o **PR 038 - GN.GTI.SIN Procedimento de Resposta a Incidentes de Segurança da Informação**.
- c) A Getnet elabora um relatório anual sobre a implementação dos planos de resposta a incidentes, com data-base de 31 de dezembro. Este relatório deve, conter, no mínimo:
 - i. A efetividade da implantação dos planos de resposta a incidentes.
 - ii. O resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias utilizadas para a prevenção e na resposta a incidentes.
 - iii. Os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período.
 - iv. Os resultados dos testes de continuidade dos serviços de pagamento, considerando cenários de indisponibilidade ocasionada por incidentes.
- d) O relatório deve ser apresentado ao Conselho de Administração, ou na sua ausência, à Diretoria da Getnet até 31 de março do ano seguinte ao da data-base.

3.5. A Getnet executa regularmente campanhas de conscientização aos seus colaboradores e disponibiliza a eles treinamento online e/ou presencial para as diretrizes de segurança da

	POLÍTICA				
	() INTERNA		() CORPORATIVA		(X) REGULATÓRIA
	Política de Segurança Cibernética			SIGLA	PL 321
				DATA DE LIBERAÇÃO	07/03/2025
				DATA DE VIGÊNCIA	07/03/2026
RESPONSÁVEL:	SEGURANÇA DA INFORMAÇÃO		VERSÃO	07	
Classificação da Informação: (x) PÚBLICO () INTERNO () CONFIDENCIAL () CONFIDENCIAL RESTRITO () SECRETO					

informação e cibernética e os assuntos pertinentes de segurança da informação e cibernética (boletim informativo de segurança da informação).

3.6. A Getnet disponibiliza periodicamente informativos aos clientes e usuários finais sobre conscientização e utilização segura dos serviços e ferramentas oferecidos.

3.7. A Getnet possui um Comitê de Segurança da Informação e Proteção de Dados, no qual membros da gerência e da alta direção são parte integrante e atuante nas tomadas de decisão referentes à segurança da informação e cibernética.

3.8. A Getnet define diretrizes para o desenvolvimento seguro de suas aplicações, conforme o **PR 1868 - GN.TEC.SEI_Desenvolvimento Seguro**.

3.9. A Getnet classifica as suas informações de acordo com a sua criticidade ao negócio, e segue as diretrizes definidas na **PL 064 - GN.TEC.SEI Política de Classificação da Informação**.

3.10. A Getnet implementa mecanismos para a prevenção da perda de informações, conforme as definições na **PL 069 - GN.GTI.SIN Política de Prevenção a Perda de Informação**.

3.11. A partir a sua data de publicação a Política de Segurança Cibernética é revisada pelo menos anualmente, e sempre que uma nova versão é publicada os colaboradores recebem um resumo contendo as suas diretrizes gerais.

a) Esta Política de Segurança Cibernética é divulgada e compartilhada com os prestadores de serviço da Getnet.

3.12. A Getnet mantém, por um período de pelo menos 5 anos, a salva guarda:

a) Do documento desta Política de Segurança Cibernética.

b) Do plano de resposta a incidentes.

c) Do relatório anual, citado na diretriz 6.4.c.

	POLÍTICA				
	() INTERNA		() CORPORATIVA		(X) REGULATÓRIA
	Política de Segurança Cibernética			SIGLA	PL 321
				DATA DE LIBERAÇÃO	07/03/2025
				DATA DE VIGÊNCIA	07/03/2026
RESPONSÁVEL:	SEGURANÇA DA INFORMAÇÃO		VERSÃO	07	
Classificação da Informação: (x) PÚBLICO () INTERNO () CONFIDENCIAL () CONFIDENCIAL RESTRITO () SECRETO					

3.13. A Getnet realiza avaliação nos fornecedores, conforme as diretrizes da **PL 071 - GN.AFI.SUP**
Política de Segurança da Informação na Cadeia de Suprimentos.

3.14. A Getnet implementa controles criptográficos, conforme as definições direcionadas pela **PL 468**
- GN.GTI.SIN Gerenciamento De Chaves Criptográficas.

4. RESPONSABILIDADES

1. Segurança da informação
 - i. Gestão do documento
 - ii. Definição de diretrizes específicas para tecnologias críticas
 - iii. Assegurar que as áreas estejam de acordo com a Política.
2. Segurança Tecnológica
 - i. Implementação de hardening
 - ii. Identificação de vulnerabilidades técnicas
 - iii. Monitoramento e tratativas de incidentes de Segurança da informação
 - iv. Implementação de Controles criptográficos
 - v. Desenvolvimento seguro
3. Gestão de Serviços de TI
 - i. Execução do DRP
4. Suprimentos
 - i. Avaliação de fornecedores

5. ANEXOS

N/A