





**POLÍTICA COMPLEMENTAR DE
GESTÃO DE INCIDENTES DE
SEGURANÇA DA INFORMAÇÃO**

DEZEMBRO – 2022

	POLÍTICA COMPLEMENTAR DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO	Última Revisão – 04/2024		
		Página 2 de 11	Revisão: 02	Publicação: 12/2022

Sumário


1 – SIGLAS, ABREVIACÕES E DEFINIÇÕES	3
2 – INTRODUÇÃO	4
3 – PAPÉIS E RESPONSABILIDADES	4
3.1 - Responsável pela Segurança da Informação / Cibernética	4
3.2 – Comitê de Segurança da Informação / Cibernética.....	5
3.3 – Gerência e ou Alta Direção	6
4 – OBJETIVOS	6
5 – METODOLOGIA	7
6 – ESCOPO	7
7 – DIRETRIZES GERAIS	8
7.1 – Estrutura de Gestão de Incidentes	8
7.2 – Gestão e Planejamento de Incidentes	8
7.3 – Tratamento e Resposta de Incidentes.....	9
7.4 – Encerramento de Incidentes	9
7.5 – Manutenções e Melhoria Contínua	10
7.6 – Treinamento e Conscientização	10
8 - CONSIDERAÇÕES FINAIS	11

	POLÍTICA COMPLEMENTAR DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO	Última Revisão – 04/2024		
		Página 3 de 11	Revisão: 02	Publicação: 12/2022

Responsável:	Emilson Queiroz (Gerente TI e Cloud)
Aprovado por:	Suleiman Bragança (CEO)
Políticas Relacionadas:	Política da Segurança da Informação / Política Complementar da Segurança da Informação / Cibernética / Plano e Política de Continuidade de Negócio
Localização de Armazenamento:	Escritórios de Barueri (SP) / Cuiabá (MT) e Florianópolis (SC)
Data de Aprovação:	12/2022
Data de Revisão:	04/2024
Versão atual:	2.0

1 – SIGLAS, ABREVIACÕES E DEFINIÇÕES

TERMO	DESCRIÇÃO
Continuidade de Negócios	Capacidade estratégica e tática da organização de se planejar e responder a incidentes e interrupções de negócios, para conseguir continuar suas operações em um nível aceitável previamente definido
Erradicação	Eliminação de vetores causadores do incidente de segurança da informação
Estratégias de Contenção	Documento que estabelece estratégia e procedimentos para conter, reprimir e controlar um incidente de segurança da informação
Estratégias de Recuperação do Ambiente	Documento que incorpora o roteiro de recuperação para garantir a restauração, de forma controlada, dos sistemas ou ativos afetados pelo incidente de segurança da informação
Evento de Segurança da Informação	É uma ocorrência identificada de um sistema, serviço ou rede que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida que possa ser relevante para a segurança da informação
Gestão de Riscos	Desenvolvimento estruturado e aplicação de uma cultura de gestão, políticas, procedimentos e práticas às tarefas de identificação, análise e controle dos riscos
Impacto	Consequência avaliada de um evento em particular
Incidente	Situação que pode representar ou levar a uma interrupção de negócios, perdas, emergências ou crises
Incidente de Segurança da Informação	Um simples evento ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação
Malware	Definição genérica para qualquer software de computador com intenção maliciosa
Organização	Grupo de pessoas e instalações com uma série de responsabilidades, autoridades e relacionamentos. Exemplo: Companhia, corporação, firma, empresa, instituição de caridade, profissional liberal ou associação, ou partes ou combinações destas
Partes interessadas	Aqueles que possuem algum interesse nos resultados de uma organização

	POLÍTICA COMPLEMENTAR DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO	Última Revisão – 04/2024		
		Página 4 de 11	Revisão: 02	Publicação: 12/2022

Processo	Atividade ou conjunto de atividades executados por uma organização que produzem ou suportem um ou mais produtos ou serviços
Risco	Algo que pode ocorrer e seus efeitos nos objetivos da organização
Riscos cibernéticos	Ameaças cibernéticas que comprometem os pilares de: confidencialidade, integridade e disponibilidade dos ativos da organização
Segurança da Informação (S.I.)	Conjunto de ações e boas práticas com o objetivo de proteger os ativos da organização
TIC	Tecnologia da Informação e Comunicação

2 – INTRODUÇÃO

A Política Complementar de Gestão de Incidentes de Segurança da Informação visa descrever as diretrizes necessárias para prover a gestão dos incidentes de segurança da informação antes, durante e após os eventos.

Essa Política está alinhada às demais políticas da organização, dentre as quais destacamos as seguintes:


- Política de Segurança da Informação
- Política Complementar da Segurança da Informação - Cibernética
- Política de Continuidade de Negócios

3 – PAPÉIS E RESPONSABILIDADES

Os papéis e responsabilidades definidos nessa Política descrevem as funções exercidas pelos colaboradores da Vector que atuam diretamente neste processo.

3.1 - Responsável pela Segurança da Informação / Cibernética


- Definir ferramentas e tecnologias que assegurem eficiência e eficácia na prevenção, no monitoramento, na resolução e no pós-incidente;
- Estabelecer e documentar as ações e os procedimentos operacionais para resposta a incidentes;
- Implantar controles de segurança da informação de acordo com os requisitos mapeados;
- Monitorar o ambiente operacional para identificar e gerar alerta da ocorrência de incidentes de segurança da informação;
- Elaborar o relatório anual sobre incidentes, reportando dados e a efetividade do processo de Gerenciamento de Incidentes de Segurança da Informação;

	POLÍTICA COMPLEMENTAR DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO	Última Revisão – 04/2024		
		Página 5 de 11	Revisão: 02	Publicação: 12/2022

- Planejar o programa de conscientização, treinamento e/ou educação em segurança da informação para as partes interessadas;
- Assegurar o registro dos incidentes de segurança da informação e das atividades relacionadas durante todo o seu ciclo de vida;
- Assegurar a categorização e classificação do incidente de segurança da informação;
- Realizar a análise, investigação e o diagnóstico do incidente de segurança da informação, compreendendo o seu impacto;
- Realizar, quando necessário, a contenção do incidente de segurança da informação para atenuar os danos e impedir o comprometimento de outros recursos;
- Erradicar os componentes que causaram o incidente de segurança da informação;
- Assegurar, caso o ambiente continue comprometido, o correto escalonamento conforme situação atual do incidente de segurança da informação;
- Recuperar o ambiente operacional para o seu estado de normalidade de forma controlada;
- Comunicar o encerramento para as partes interessadas;
- Assegurar o correto arquivamento da solução;
- Manter a base de conhecimento de incidentes (lições aprendidas) atualizada.

3.2 – Comitê de Segurança da Informação / Cibernética

- Assegurar o envolvimento de colaboradores qualificados na Vector, implementação e manutenção dos procedimentos e processos de incidentes de segurança da informação;
- Estabelecer as diretrizes para a gestão de incidentes de segurança da informação;
- Estabelecer e comunicar formalmente os papéis, responsabilidades e níveis de autoridades da estrutura de gestão de incidentes de segurança da informação;
- Aprovar a Política Complementar de Gestão de Incidentes de Segurança da Informação;
- Analisar o relatório gerencial de incidentes de segurança da informação;
- Definir e catalogar os incidentes de segurança da informação a serem monitorados;
- Planejar a notificação de incidentes de segurança da informação;
- Emitir, quando necessário, o alerta de emergência para acionar o processo de Gerenciamento de Continuidade do Negócio.


	POLÍTICA COMPLEMENTAR DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO	Última Revisão – 04/2024		
		Página 6 de 11	Revisão: 02	Publicação: 12/2022

3.3 – Gerência e ou Alta Direção

- Coordenar os planos relacionados à Gestão de Incidentes de Segurança da Informação;
- Assegurar que o programa de conscientização, treinamento e/ou educação em segurança da informação para as partes interessadas seja documentado e executado anualmente;
- Revisar e atualizar os mecanismos de acompanhamento e controles internos do processo.
- Assegurar a realização periódica de testes de segurança, durante o ciclo do Plano de Continuidade de Negócios - PCN, incluindo o cenário de ataque cibernético.

4 – OBJETIVOS

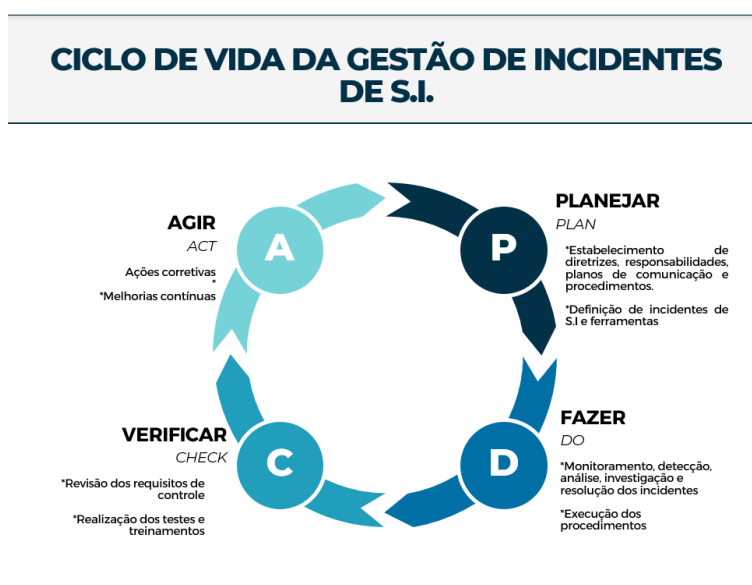
A Política Complementar de Gestão de Incidentes de Segurança da Informação estabelece diretrizes, responsabilidades e orientações sobre o funcionamento do processo, de forma que os incidentes de segurança da informação sejam prevenidos, monitorados, detectados, tratados e encerrados com a finalidade de atenuar ao máximo o impacto nos ativos e consequentemente nos negócios da Vector.

	POLÍTICA COMPLEMENTAR DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO	Última Revisão – 04/2024		
		Página 7 de 11	Revisão: 02	Publicação: 12/2022

METODOLOGIA

A metodologia de Gestão de Incidentes de Segurança da Informação implantada na Vector baseia-se nas suas políticas, normas e regulamentos, e tem como objetivo buscar a prevenção e atenuação dos impactos de incidentes de segurança da informação por meio de procedimentos e a melhoria contínua do seu processo.


Figura 1 - Ciclo de vida da gestão de incidentes de S.I.



6 – ESCOPO

Esta Política abrange os incidentes de segurança da informação. São considerados incidentes de segurança da informação, mas não limitando-se a estes:

- Qualquer vulnerabilidade técnica ou evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de informação, redes de computadores, bem como as estruturas físicas e lógica associadas, que comprometa um ou mais princípios básicos da segurança da informação: confidencialidade, integridade, disponibilidade e conformidade;
- Indisponibilidade do ambiente tecnológico em virtude de ataque cibernético;
- Violação de dados confidenciais (informações de clientes, informações estratégicas, dados pessoais, outros);
- Tentativas interna ou externa de acesso não autorizado;

	POLÍTICA COMPLEMENTAR DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO	Última Revisão – 04/2024		
		Página 8 de 11	Revisão: 02	Publicação: 12/2022

- Uso ou acesso não autorizado a um sistema;
- Violação, explícita ou implícita, de políticas de Segurança da Inf;
- Modificações em um sistema, sem o conhecimento, instruções ou consentimento prévio do dono do sistema;
- Compartilhamento de senhas.

7 – DIRETRIZES GERAIS


Esta Política abrange os incidentes de segurança da informação. São considerados incidentes de segurança

7.1 – Estrutura de Gestão de Incidentes

- A Gerência de Segurança da Informação foi designada como responsável pelo processo de Gerenciamento de Incidentes de segurança da informação;
- Os demais papéis, responsabilidades e autoridades na gestão de incidentes de segurança da informação devem estar definidos formalmente;
- Devem ser realizadas ações de busca ativa em legislações e guias de melhores práticas que assegurem a identificação dos requisitos a serem atendidos que estejam relacionados à Gestão de Incidentes de Segurança da Informação;
- Devem ser alocados recursos humanos com habilidade, experiência e competência em segurança da informação.

7.2 – Gestão e Planejamento de Incidentes

- Deve ser implementado e mantido um catálogo de incidentes de segurança da informação, incluindo a categorização e a classificação dos incidentes;
- Devem ser instituídas regras que estabeleçam os processos de gestão para tratamento e respostas a incidentes de segurança da informação;
- Deve ser documentado um plano de tratamento e respostas a incidentes, bem como os procedimentos operacionais relacionados a contenção, erradicação e recuperação, além de comunicado para todas as partes interessadas;

	POLÍTICA COMPLEMENTAR DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO	Última Revisão – 04/2024		
		Página 9 de 11	Revisão: 02	Publicação: 12/2022


- Deve ser instituída e mantida a equipe de tratamento e resposta a incidentes;
- Deve ser planejado, implementado e documentado um processo de notificação de eventos adversos de segurança da informação (incidentes).

7.3 – Tratamento e Resposta de Incidentes

- O ambiente operacional deve ser monitorado continuamente por meio de ferramentas e/ou tecnologias que auxiliem na geração de alertas de eventos de segurança da informação;
- Os eventos adversos devem ser avaliados e escalonados para o processo de gestão de incidentes;
- O escalonamento deve ser feito com base nas informações de todo o ciclo de vida do incidente de segurança da informação até o momento atual, definindo o encaminhamento para o processo que melhor responder a situação atual;
- Os incidentes devem ser registrados e atualizados desde o momento de sua detecção até a sua resolução final, sendo armazenado todas as evidências;
- Os incidentes devem ser classificados e categorizados de acordo com um padrão pré-estabelecido;
- Os incidentes, após confirmados, devem ser analisados, investigados e diagnosticados sua causa-raiz;
- O Comitê Executivo de TIC deverá ser notificado sempre que for identificado um incidente classificado como grave, muito grave e extremamente grave ou o tempo de resolução ter excedido o prazo pré-estabelecido.

7.4 – Encerramento de Incidentes

- O chamado técnico só deve ser encerrado após resolução do problema e atualização do registro do incidente - com a inclusão de evidências e soluções aplicadas;
- As partes interessadas devem ser comunicadas sobre o encerramento do chamado técnico;
- Análises de problemas pós-incidentes devem ser realizadas, sempre que a causa-raiz não for constatada, para garantia da identificação e da correção de vulnerabilidades técnicas;
- Uma base de conhecimento de incidentes deve ser criada, atualizada e utilizada.


	POLÍTICA COMPLEMENTAR DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO	Última Revisão – 04/2024		
		Página 10 de 11	Revisão: 02	Publicação: 12/2022

7.5 – Manutenções e Melhoria Contínua

- A gestão do processo de Gerenciamento de Incidentes de Segurança da Informação deverá ser contínua e sistematicamente atualizada;
- O plano de tratamento e respostas a incidentes deve ser revisado e testado anualmente ou sempre que modificações significativas ocorrerem;
- Os recursos e as documentações do processo de Gerenciamento de Incidentes de Segurança da Informação devem ser mantidos para garantir que permaneçam eficazes e alinhados com as prioridades do negócio, além de garantir a geração das evidências necessárias;
- Os dados sobre os incidentes ocorridos devem ser mantidos, documentados e submetidos ao Comitê Estratégico de Governança, Riscos e Compliance, aos órgãos fiscalizadores solicitantes e aos demais envolvidos na ocorrência.

7.6 – Treinamento e Conscientização

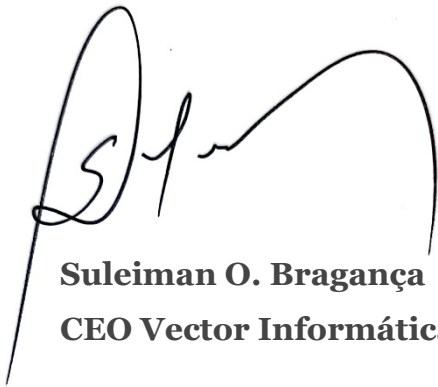
- Todos os colaboradores e terceirizados da Vector devem estar cientes da relevância e importância de suas atividades dentro do processo de Gerenciamento de Incidentes de Segurança da Informação;
- Realizar treinamentos para toda equipe, de acordo com suas responsabilidades dentro do processo.

	POLÍTICA COMPLEMENTAR DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO	Última Revisão – 04/2024		
		Página 11 de 11	Revisão: 02	Publicação: 12/2022

8 - CONSIDERAÇÕES FINAIS

As dúvidas decorrentes de fatos não descritos nesta Política Complementar de Gestão de Incidentes de Segurança da Informação deverão ser encaminhadas à Diretoria para avaliação e decisão. Esta Política entra em vigor a partir da data de publicação e pode ser alterada a qualquer tempo, por decisão da Direção, mediante o surgimento de fatos relevantes que apareçam ou não tenham sido contemplados neste documento.

Barueri, dezembro de 2022



Suleiman O. Bragança
CEO Vector Informática Ltda.