PLANO DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO / CIBERNÉTICA

Vector Informática Ltda.

Departamento TI – Segurança da Informação

JANEIRO - 2023

Sumário

1 - PLANO DE RESPOSTA A INCIDENTES

A VECTOR tem como missão atuar na detecção, resolução, prevenção e redução a ocorrência de incidentes de segurança da informação na empresa, proporcionando um ambiente cada vez mais confiável, disponível e íntegro. Para assegurar o atingimento da sua missão é fundamental que se faça a gestão dos incidentes de forma adequada, eficiente e eficaz, a fim de proteger a informação contra roubo, fraude, espionagem, perda não intencional, acidentes e outras ameaças. Para tal, a Vector tem como objetivo promover ações de redução, das ocorrências de incidentes de segurança da informação, propiciando o ambiente desejável por sua missão.

2 – OBJETIVO

O principal objetivo deste plano, é descrever os processos para reportar e gerenciar os dados relacionados a incidentes de segurança que podem ser originados de fontes internas ou externas. Também é objetivo deste plano esclarecer as formas para o reporte de vulnerabilidades na segurança observadas por agentes internos (funcionários) ou externos (clientes, fornecedores e parceiros).

É importante que os incidentes de segurança e as vulnerabilidades reportadas sejam devidamente investigadas e gerenciadas. Em algumas circunstâncias talvez seja necessário que autoridades policiais sejam acionadas. Desta forma, evidências devem ser coletadas e armazenadas pois podem servir de provas em processos judiciais. Uma investigação detalhada de uma atividade suspeita pode facilmente identificar uma vulnerabilidade ou deficiência nos computadores da Vector. Este processo garante que estas vulnerabilidades ou deficiências sejam tratadas tão logo que sejam descobertas diminuindo o risco e prevenindo o impacto de incidentes futuros.

3 – ESCOPO

Este plano descreve papéis, responsabilidades e processos relacionados ao tratamento de incidentes com a intenção de garantir agilidade na contenção e resolução de todos os incidentes de segurança e vulnerabilidades reportadas aos sistemas e ativos da Vector.

4 – DEFINIÇÕES

Um incidente de segurança da informação pode ser definido como:

- Um evento ou situação adversa associada a qualquer serviço de TI que exponha a Vector, seus clientes, e ameaças contra a Integridade, Confidencialidade ou Disponibilidade;
- Qualquer evento que pode resultar em perda ou dano à ativos de TI;
- Qualquer ação que pode ser considerada uma violação as normas e políticas de segurança, incluindo os acontecimentos acidentais.

5 – PAPÉIS E RESPONSABILIDADES

Os seguintes papeis e responsabilidades estão relacionados a este plano:

1 - Comitê de Segurança e Risco

- Analisar todos os achados relevantes em relatórios de auditoria;
- Analisar ações baseando-se em incidentes identificados que podem representar vulnerabilidades na segurança;
- Garantir que ações de melhoria são encomendadas as equipes responsáveis;
- Revisar todos os incidentes reportados e notificar instâncias superiores, quando necessário;
- Conduzir revisões pós-incidentes e coordenar a resolução dos incidentes;
- Acionar o time de resposta a incidentes (TI) e envolver recursos externos na resolução, quando necessário;
- Comunicar o progresso de resposta aos incidentes a todos os envolvidos (internos e externos);
- Gerenciar e classificar todos os incidentes e ações corretivas;
- Apresentar relatórios pós-incidentes ao Comitê de Segurança para discussão.

2 – Alta Direção

- Aprovar o envolvimento de recursos externos durante a resolução de incidentes críticos;
- Acompanhamento dos resultados dos processos;
- Aprovar comunicações internas relevantes.

3 - Equipe de Resposta a Incidentes (TI e DPO)

- Prover suporte e orientação para detectar e resolver incidentes de segurança;
- Reportar incidentes ou vulnerabilidades conhecidas ao Comitê de Segurança e Risco, quando necessário;
- Conduzir a resolução de incidentes de segurança através do fluxo normal de incidentes de TI, incluindo o registro numa ferramenta de gerenciamento de tickets;
- Executar ações corretivas para resolver incidentes de segurança;
- Priorizar requisições importantes para mudanças, quando necessário.

6 – COMUNICAÇÕES

Durante a reposta a incidentes é vital que todos os envolvidos, internos e externos da Vector, sejam informados sobre o andamento da resposta. Inicialmente, os detalhes técnicos e os achados devem ser mantidos de forma confidencial e as informações divulgadas somente para os diretamente envolvidos ou impactados pelo incidente.

Em um evento de segurança de alta prioridade, pode ser apropriado notificar agentes externos, que podem incluir:

- Agencias importantes do governo e ou forças policiais (para prover assistência adequada, caso necessário);
- Público externo (comunidade, empresas parceiras).

O comitê de segurança e risco deve indicar quem precisa ser notificado durante e no encerramento de um incidente. Todas as notificações precisam ser aprovadas pela Alta Direção.

7 – TIPOS DE INCIDENTES

Os tipos de eventos e incidentes de segurança devem incluir:

TIPO	DEFINIÇÃO
Incidente Malicioso	Qualquer ação intencional que leve, ou possa levar, a perda, dano ou corrupção dos ativos de TI da Vector
Violação de Acesso	Uso não autorizado de sistema de TI, incluindo mau uso de contas e senhas, visando ataques que vão de encontro a uma política de segurança
Roubo / Furto	Roubo ou furto de qualquer equipamento de TI ou informação de propriedade da instituição
Uso inapropriado	Mau uso de facilidades para acessar conteúdo inapropriado
Acidente	Qualquer falha acidental ou não intencional decorrente da não observação de política de segurança
Incidente Operacional	Evento de falha de sistema ou mudança em uma configuração que resulte em perdas de disponibilidade ou integridade de sistemas ou informações

8 – PRIORIDADES

Os incidentes devem ser priorizados de acordo com as seguintes definições:

PRIORIDADE	DESCRIÇÃO	EXEMPLO DE INCIDENTE	RESPOSTA ESPERADA
Baixa	Um evento de baixo impacto com pouco ou nenhum efeito operacional e que requer pouco esforço para gerenciar e resolver	• Incidente de vírus em um único computador ou dispositivo • Diversas tentativas mal-sucedidas de obter acesso não autorizado	Resolvido por agentes da equipe de resposta com ações já mapeadas.
Média	Possível brecha de segurança que requer investigação e envolvimento do Comitê de Segurança para resolução	• Acesso não autorizado a uma conta de serviço • Escaneamento de portas em rede interna ou externa • Múltiplos incidentes de vírus	Precisa ser escalado para o Comitê de Segurança e Risco para coordenação, investigação e resolução
Alta	Evento com impacto significante a serviços	• Violação em larga escala de dados	Precisar ser escalado ao Diretor e ao Comitê de

	críticos de TI ou informações, dano a equipamento físico ou à pessoas	sensíveis a pesquisa, dados financeiros ou pessoais • Pichação do website da instituição • Comprometimento de dados de pagamento	Segurança Imediatamente Todos os envolvidos precisam ser notificados Uma revisão pós-incidente precisa ser realizada

9 – NOTIFICAÇÃO DE INCIDENTE

Os incidentes podem ser notificados por qualquer usuário interno ou ainda de fontes externas, como clientes e parceiros. O canal preferencial é o e-mail dpo@vectorinf.com.br. Este canal deve ser amplamente divulgado para facilitar o registro de atividades suspeitas ou de incidentes já identificados.

10 – ARMAZENAMENTO DE DOCUMENTOS E EVIDÊNCIAS

Durante o tratamento de um incidente todas as evidências relevantes precisam ser coletadas e armazenadas. Além disso todas as ações devem ser registradas, para permitir análise posterior por parte de autoridades ou outras pessoas autorizadas.

As evidências podem incluir, mas não se limitar a:

- Logs de auditoria;
- Arquivos de malware;
- Dados e e-mail;
- Alertas de Segurança;
- Dados sobre os sistemas comprometidos;
- Imagem de disco virtual.

Todos os incidentes devem ser bem documentados na ferramenta de Ticket, ferramenta que a Vector utiliza e que está parametrizada para o registro e o acompanhamento dos incidentes. As informações obrigatórias no registro de um incidente são:

- Todas as informações repassadas pelo usuário;
- Ações tomadas pelo time de resposta;
- Resultados do processo de investigação;
- Informações acerca do contato com os envolvidos.

Durante o tratamento de incidentes, os usuários devem ser orientados a não realizar nenhuma alteração ou modificação nos sistemas comprometidos até que a equipe de resposta a incidentes autorize.

11 – CHECKLIST DE TRATAMENTO DE INCIDENTES

Ação		Responsável
Ações comuns		
1	**Procedimento para tratamento de notificação de incidente** • Reporte deve ser recebido via e-mail ou telefone • Todos os detalhes precisam ser registrados, incluindo detalhes de contato, e o ticket deve ser atribuído para um membro da equipe de resposta	Equipe de Segurança da Informação e o DPO
2	**Revisar detalhes e atribuir prioridade** • A equipe de resposta precisa revisar os dados iniciais da notificação de incidente para determinar a criticidade e deve atribuir uma prioridade para o caso	Equipe de Segurança da Informação e o DPO
Incidentes de baixa prioridade		
3	**Contenção ou remoção de ameaça** • O incidente deve ser atribuído a um membro da equipe de resposta a incidente e deve ser tratado com uma solução já mapeada • O membro responsável deve seguir a orientação descrita em roteiros já mapeados • As ações podem conter a remoção de vírus, reset de conta de usuário ou ainda o contato direto com o usuário impactado • Se um computador contiver um vírus de baixo impacto, o dispositivo deve ser desconectado da rede para prevenir a propagação. Outros computadores devem ser analisados para verificação de comprometimento	Equipe de Segurança da Informação e o DPO
4	**Recuperação/restauração dos sistemas afetados** • Uma vez que a causa do incidente foi solucionada, o computador ou a conta de usuário deve ser recuperada • Em eventos em que há comprometimento de sistemas, como numa infecção de vírus ou outra vulnerabilidade, o sistema operacional deve ser reinstalado para remover todos os traços da infecção. Após este processo, a máquina pode ser reconectada à rede	Equipe de Segurança da Informação e o DPO
5	**Documentação dos resultados** • Toda a investigação e as ações de recuperação precisam ser registradas no sistema • Todos os detalhes relacionados a como o incidente foi resolvido deve ser anotado	Equipe de Segurança da Informação e o DPO
Ações comuns a incidentes de alta e média prioridades		
6	**Investigação Inicial** O comitê de segurança precisa revisar um incidente antes de ser considerado médio ou alto, afim de validar as informações e definir quais os paços iniciais para iniciar a investigação. Os seguintes fatores precisam ser considerados ao elevar a prioridade de um incidente para Alta:	Comitê de Segurança e Risco

	• Dados pessoais ou privados foram comprometidos? • O impacto é visivelmente público? • O incidente pode impactar negativamente a reputação da Vector, clientes, fornecedores, parceiros ou funcionários?	
Incidentes de média prioridade		
7	**Contenção ou remoção de ameaça** • Os incidentes devem ser atribuídos a um membro do Comitê de Segurança que pode acionar qualquer outro funcionário, caso necessário • O comitê precisa determinar se algum computador será confiscado até que a investigação seja realizada. Em algumas circunstancias, o computador precisa ser desligado da rede até que se tenha um parecer favorável ao restabelecimento pela equipe técnica • Todos os vírus, material improprio ou outras causas de um incidente devem ser removidos durante a contenção para previr a propagação ou o comprometimento de outros sistemas.	Comitê de Segurança e Risco
8	**Remediar vulnerabilidades identificadas** • A investigação de um incidente pode revelar fraquezas ou vulnerabilidades nos processos de controle de segurança • O comitê deve identificar, documentar e tomar ação para remediar as fraquezas e as vulnerabilidades implementando ou improvisando controles para prevenir a recorrência do mesmo evento • A remediação pode se estender para análise de violações a políticas de segurança, e nestes casos o Comitê deve prover a conscientização ao usuário envolvido	Comitê de Segurança e Risco
9.1	**Recuperação/restauração dos sistemas afetados** • Uma vez que a causa do incidente foi solucionada, o computador ou a conta de usuário deve ser recuperada • O objetivo desta recuperação é restabelecer os sistemas afetados de forma a evitar futuros incidentes semelhantes • O comitê definirá se o sistema operacional deve ser reinstalado ou um backup disponibilizado para permitir a recuperação • Uma vez que isto ocorra, o sistema pode ser reconectado à rede, para retorno a suas atividades normais	Equipe de Segurança da Informação e o DPO
9.2	**Condução de revisão e relatório pós-incidente** • O comitê deverá rever a documentação e as evidências coletadas para determinar a causa raiz além de prover recomendações para prevenir a recorrência deste incidente • Recomendações levantadas devem ser entregues em relatório pós-incidente para o Diretor • O comitê deve informar os usuários impactados diretamente e os que reportaram problema inicial	Comitê de Segurança e Risco
10	**Acionamento do Time de Resposta** Dado o tamanho de um incidente de alta prioridade, o DPO será responsável por acionar e coordenar os trabalhos dos especialistas necessários. Isto irá permitir a coordenação centralizada das ações para resposta ao incidente com o intuito de evitar impacto negativo à Vector. A comunicação entre os envolvidos é fundamental para permitir a rápida resposta. A força tarefa pode ser dividida em três frentes: Investigação: Identificar a causa, motivação, usuários envolvidos e o dano	DPO

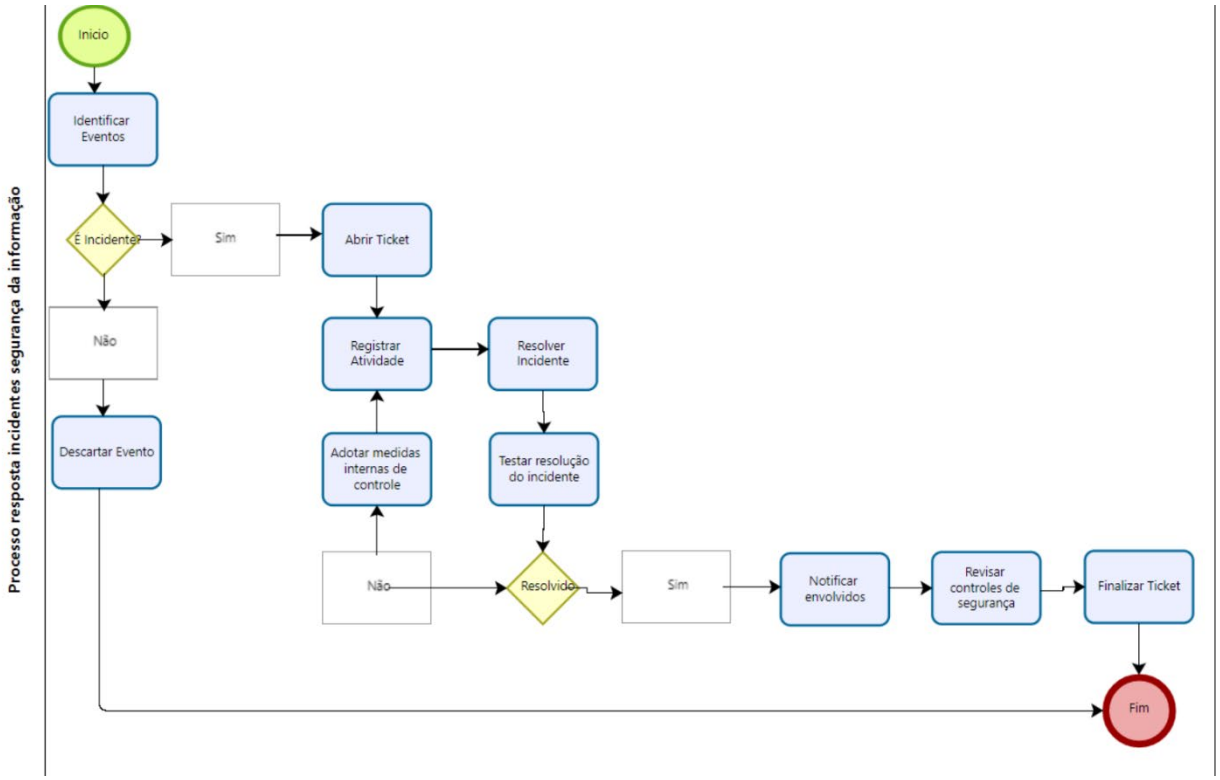
	causado pelo incidente Contenção: Implementação de ações de monitoração e de controles de correção para reduzir o impacto durante um incidente Restauração: Recuperação dos sistemas impactados ou ativação de plano de recuperação de desastres para restaurar os serviços para um estado seguro	
11	**Designar um coordenador de comunicação** O Diretor irá definir um coordenador de comunicação, para garantir eficácia e eficiência na comunicação com os usuários impactados e todos os outros envolvidos no incidente.	Diretor
12	**Notificar envolvidos relevantes** Em eventos de alta prioridade, o coordenador de comunicação nomeado irá trabalhar com o DPO para determinar quem precisa ser notificado do incidente	DPO – Coordenador de comunicação
13	**Condução de revisão e relatório pós-incidente** • O DPO deverá conduzir um processo formal de revisão do ocorrido apresentando uma breve discussão sobre a causa raiz do incidente, provendo feedback sobre a resposta dada para resolução do problema e sobre as recomendações de melhoria	DPO
14	**Revisão dos resultados** O DPO deve promover ações de melhoria para que novos incidentes sejam evitados O DPO deve avaliar todo o processo de tratamento em busca do aperfeiçoamento das ações tomadas para contenção e erradicação do incidente	DPO

Nestes quadros estão descritos os passos macro para a manipulação de incidentes de acordo com a prioridade descrita anteriormente. Os procedimentos podem ser ajustados para adequar-se às características de cada tipo de incidente. Além disso, as ações recomendadas devem ser melhoradas continuamente e ajustadas para otimizar o processo, a fim de estabelecer a melhor forma de contenção e erradicação de incidentes.

12 – FLUXO BÁSICO PARA TRATAMENTO DO INCIDENTES

Na figura 1 abaixo está descrito as etapas básicas durante o processo de tratamento de incidentes de segurança.

Figura 1:

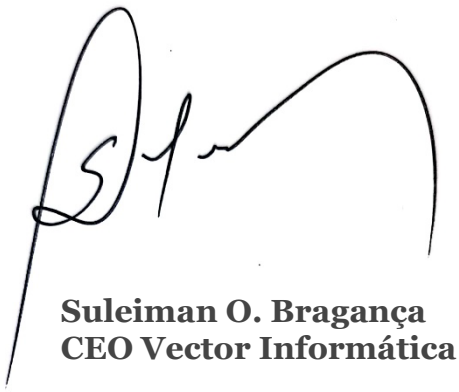


13 – VIGÊNCIA E REVISÕES

O presente documento entra em vigor em 16/01/2023 e será revisado no período máximo de um (01) ano ou havendo necessidade anterior, o que for menor, para que o documento permaneça sempre atualizado.

CONTROLE DE ALTERAÇÕES	
Histórico de Publicações	**Alterações**
01/2023	Publicação inicial
04/2024	Revisão do documento

Barueri, janeiro de 2023



Suleiman O. Bragança
CEO Vector Informática Ltda.