

**Plano de Respostas a Incidentes de Segurança da Informação**

Setembro/2021

**Sobre este artefato**

O objetivo deste artefato é descrever em alto nível, os processos e procedimentos que visam gerenciar, controlar e reportar os dados relacionados a Incidentes de Segurança, o qual podem ter suas origens fontes internas ou externas de dados.

Cabe observar este artefato visa esclarecer todo o procedimento como forma para comunicação/report de vulnerabilidades na segurança de informação por agentes internos [Funcionários e clientes] ou externos [Auditores e a comunidade específica].

Importante que os registros de incidentes de Segurança da Informação, bem como vulnerabilidades reportadas sejam devidamente monitorados e investigados/gerenciadas. Tendo algumas circunstancias necessário que autoridades policiais sejam acionadas.

Desta forma, evidências devem ser coletadas e armazenadas para servir de provas em processos judiciais. Este processo garante que toda vulnerabilidade ou deficiências sejam tratadas tão logo descobertas, minimizando o risco e prevenindo o impacto de incidentes futuros dentro da arquitetura de informação, sistemas e infraestrutura.

|  |
| --- |
| **Controle de Versão** |
| **Versão** | **Data** | **Justificativa** | **Responsabilidade** |
| 01.00 | 25/05/2021 | Draft Inicial | Wagner Costa |
| 01.01 | 28/06/2021 | Análise Resolução 3.909 | Wagner Costa |
| 01.02 | 20/09/2021 | Revisão Geral Artefato | Wagner Costa |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. Escopo

As diretrizes descritas neste artefato têm como finalidade padronizar as ações referente ás áreas de processos, no que tange, o Plano de Respostas a Incidentes de Segurança da Informação e, definir quais atividades serão executadas em que momento, quem serão os responsáveis em executar e os conceitos envoltos neste processo.

1. Incidentes Segurança da Informação

Evento e/ou situação associada a qualquer serviço de Tecnologia da Informação que possa expor a CashWay ou seus sistemas a cenários de ameaças contra a integridade, confidencialidade e disponibilidade dos seus serviços com frente a tecnologia da informação e dados;

Todo evento que pode resultar em perdas, danos aos ativos de Tecnologia da Informação da CashWay;

Toda ação o qual viole as normas e Políticas de Segurança da Informação, não obstante incluindo os acontecimentos acidentais internos e externos.

1. Descrição e Tipos de Incidentes

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nº | Tipo | Descrição | Baixa | Média | Alta |
| Confidencialidade | Integridade | Disponibilidade |
| Assegurar que a informação apenas está acessível a quem está autorizado | Salvaguardar que a informação e o método de processamento são exatos e completos | Assegurar que os utilizadores autorizados têm acesso à informação quando necessário |
| 1 | Incidente Malicioso | Qualquer ação intencional que leve a perda, dano ou corrupção dos ativos de TI | Acesso não autorizado á informação tem um efeito adverso limitado nas operações | O acesso não autorizado á informação tem um efeito significativo nas operações | O acesso não autorizado à informação tem um efeito adverso catastrófico nas operações |
| 2 | Violação de Acesso | Uso não autorizado de sistema de TI, incluindo mau uso de contas e senhas |
| 3 | Furto/Roubo | Roubo ou furto de qualquer equipamento de TI | Uma alteração não autorizada á informação ou destruição da mesma tem um efeito adverso e limitado nas operações | Uma alteração não autorizada á informação ou destruição tem um efeito significativo nas operações | Uma alteração não autorizada a informação ou destruição tem um efeito catastrófico nas operações |
| 4 | Uso Inadequado | Mau uso de facilidades para acessar conteúdo |
| 5 | Acidente | Qualquer falha acidental ou não intencional | O não acesso ou impossibilidade de utilização da informação ou sistemas tem um efeito limitado nas operações | O não acesso ou impossibilidade de utilização da informação ou sistemas tem um efeito significativo nas operações | O não acesso ou impossibilidade de utilização informação ou sistemas tem um efeito catastrófico nas operações |
| 6 | Incidente Operacional | Evento de falha de sistema ou mudança em uma configuração que resulte em perdas de disponibilidade ou integridade de sistemas |

1. Priorização

Os incidentes devem ser priorizados conforme tabela abaixo:

|  |  |  |  |
| --- | --- | --- | --- |
| Nível Prioridade | Descrição Prioridade | Observação | Resposta |
| 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 e Privacidade da Informação para resolução. | Acesso não autorizado a uma conta de serviço.Tentativa de acesso à sala de servidores.Escaneamento de portas em rede internaou externa.Múltiplos incidentes de vírus. | Precisa ser escalado para o Comitê de Segurança e Privacidade da Informação para coordenação, investigação e resolução. |
| Alta | Evento com impacto significante a serviços críticos de TI ou informações, dano a equipamento físico ou à pessoas | Violação em larga escala de dados sensíveis a pesquisa, dados financeiros ou pessoais.Pichação do website da instituição.Acesso não autorizado à sala de servidores. | Precisar ser escalado ao Gerente de Tecnologia da Informação e ao Comitê de Segurança e Privacidade da Informação Imediatamente.Todos os envolvidos precisam ser notificados. |

1. Notificar

Todos os incidentes devem ser notificados por qualquer usuário interno ou externo, como clientes, parceiros, colaboradores e afins. O canal para conduzir esta notificação é:

infraestrutura@cashway.io

(48)3036-0390

Ambos os canais citados acima devem ser divulgados para facilitar o registro de atividades suspeitas e/ou incidentes já notificados e identificados.

1. Evidências e Armazenamento

De acordo com o tratamento das atividades referente a incidentes todas as evidências devem ser coletadas e armazenadas, bem como, todas as ações devem ter seus registros através da solução de suporte cashway https://moviedesk.cashway.io permitindo a correta análise por parte de autoridades e pessoas autorizadas.

Toda evidência deve comtemplar o seguinte pacote de informações:

1. Logs de auditoria [Firewall, Banco de Dados, Proxys, Estação e Servidor);
2. Arquivos Malware;
3. Dumps de memória da estação ou servidor afetado;
4. Dados de e-mails;
5. Alertas de Segurança;
6. Dados, históricos, logs e Changes Requests sobre os sistemas comprometidos;
7. Imagem de disco virtual.

Todos os incidentes devem ser documentados na ferramenta de registro de trouble ticket, respeitando as informações abaixo como obrigatórias:

1. Todas as informações dadas como breve relato pelo usuário;
2. Ações identificadas pelo time de suporte, operações e infraestrutura;
3. Diagnóstico referente aos processos de investigações;
4. Toda informação de contato.

Durante o tratamento de qualquer incidente, os usuários não devem realizar qualquer tipo de alteração, modificação ou qualquer tipo de interferência nos sistemas comprometidos até que a equipe responsável pela resposta autorize.

1. Lista de verificação ao correto tratamento de incidentes

|  |
| --- |
| **Ações para o tratamento de incidentes de Segurança da Informação** |
| **Ação** | **Responsável** |
| 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 resposta a incidentes de segurança da informação |
| 2 | **Revisar detalhes e atribuir prioridade**- O incidente deve ser atribuído a um membro da equipe de resposta a incidente e deve ser tratado com uma solução já mapeada. | Equipe de resposta a incidentes de segurança da informação |

|  |
| --- |
| **Ações para o tratamento de incidentes de prioridade baixa** |
| **Ação** | **Responsável** |
| 1 | **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 resposta a incidentes de segurança da informação |
| 2 | **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 resposta a incidentes de segurança da informação |
| 3 | **Documentação dos resultados*** Toda a investigação e as ações de recuperação precisam ser registradas no sistema de ticket;
* Todos os detalhes relacionados a como o incidente foi resolvido deve ser anotado.
 | Equipe de resposta a incidentes de segurança da informação |

|  |
| --- |
| **Ações para o tratamento de incidentes de prioridade média** |
| **Ação** | **Responsável** |
| 1 | **Investigação Inicial**O Comitê de Segurança e Privacidade da Informação 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:* Dados pessoais ou privados foram comprometidos?
* O impacto é visivelmente público?
* O incidente pode impactar negativamente a reputação da CashWay?
 | Equipe de resposta a incidentes de segurança da informação |
| 2 | **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.
 | Equipe de resposta a incidentes de segurança da informação |
| 3 | **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.
 | Equipe de resposta a incidentes de segurança da informação |
| 4 | **Recuperação/restauração dos sistemas afetados** | Equipe de resposta a incidentes de segurança da |

|  |  |  |
| --- | --- | --- |
|  | * 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.
 | informação |
| 5 | **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 Gerente de Tecnologia da Informação;
* O comitê deve informar os usuários impactados diretamente e os que reportaram problema inicial.
 | Equipe de resposta a incidentes de segurança da informação |

|  |
| --- |
| **Ações para o tratamento de incidentes de prioridade alta** |
| **Ação** | **Responsável** |
| 1 | **Investigação Inicial**O Comitê de Segurança e Privacidade da Informação 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:* Dados pessoais ou privados foram comprometidos?
* O impacto é visivelmente público?
* O incidente pode impactar negativamente a reputação da CashWay?
 | Equipe de resposta a incidentes de segurança da informação |
| 2 | **Acionamento do Time de Resposta a incidentes**Dado o tamanho de um incidente de alta prioridade, o Gerente de tecnologia da Informação 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 instituição. 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 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.
 | Gerente de Tecnologia da Informação |
| 3 | **Notificar envolvidos relevantes**Em eventos de alta prioridade, o Gerente de Tecnologia da Informação irá determinar quem precisa ser notificado do incidente:* O mantenedor da instituição;
* Funcionários e clientes;
 | Gerente de Tecnologia da Informação |

|  |  |  |
| --- | --- | --- |
|  | * Agências do governo;
* Empresas parceiras;
* Comunidade.
 |  |
| 4 | **Condução de revisão e relatório pós-incidente**- O Gerente de Tecnologia da Informação 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. | Gerente de Tecnologia da Informação |
| 5 | **Revisão dos resultados**O Gerente de Tecnologia da Informação deve promover ações de melhoria para que .novos incidentes sejam evitados.O Gerente de Tecnologia da Informação deve avaliar todo o processo de tratamento em busca do aperfeiçoamento das ações tomadas para contenção e erradicação do incidente. | Gerente de Tecnologia da Informação |

Abaixo fluxo da lista de verificação



1. Papéis e Responsabilidades

Para a execução das atividades deverá promover os seguintes recursos necessários, sejam humanos, financeiros, infraestrutura assim como treinamentos no processo e ferramentas requeridas para a sua correta execução.

* 1. Comitê
* Analisar todos os tickets relevantes bem como apresentar relatório de auditoria periódico;
* Analisar ações de acordo com incidentes e suas corretas identificações que possam representar vulnerabilidades na segurança;
* Garantir que ações de melhoria tenham seus devidos impactos e recomendações implementadas;
* Conduzir revisões pós incidentes e resoluções implantadas;
* Comunicar o processo de cada resposta aos incidentes identificados aos envolvidos;
* Apresentar indicadores pós incidentes;
1. Diretor de Tecnologia da Informação

Deve aprovar o envolvimento correto dos recursos externos durante a atividade de resolução, análise e afins de incidentes críticos;

Aprovar adequadamente a comunicação interna relevantes e notificar as camadas de lideranças internas e externas quanto a identificação e resolução se necessário.

1. Squad de tratamento a incidentes de segurança e respostas

Promover suporte e orientação para detectar e resolver incidentes de segurança da informação de acordo com o item 3 deste artefato;

Reportar incidentes e vulnerabilidades conhecidas ao comitê interno de segurança e riscos se necessário;

Execução de ações corretivas para resolução de incidentes quanto a segurança da informação;

1. Comunicação aos envolvidos

Conforme a resposta a incidentes tem seu desfecho adequado, todo os envolvidos devem ser comunicados, internos e externos, precisam ser informados sobre o andamento e a resolução do incidente e resposta.

Em tempo de analise e resolução todas as informações devem ser mantidas com confidencialidade;

Quando de um incidente de alta prioridade e impacto confore sessão 3 deste artefato, deve ser apropriado notificar agentes externos, como agências do governo ANDP quando tema for LGPD e demais orgãos;

Todas as notificações devem ser aprovadas conforme item 9 deste artefato.