NEW WAVE

PROCEDIMENTO DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Comitê de Segurança da Informação

DOCUMENTO	CLASSIFICAÇÃO	DATA	APROVADO POR:	VERSÃO
PRO-11302-0001	Informação Interna	10/08/2023	Rodrigo Nunes	1.0

PROCEDIMENTO DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO				
DOCUMENTO	**CLASSIFICAÇÃO**	**DATA**	**APROVADO POR:**	**VERSÃO**
PRO-11302-0001	Informação Interna	10/08/2023	Rodrigo Nunes	1.0

SUMÁRIO

PROCEDIMENTO DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO				
DOCUMENTO PRO-11302-0001	**CLASSIFICAÇÃO** Informação Interna	**DATA** 10/08/2023	**APROVADO POR:** Rodrigo Nunes	**VERSÃO** 1.0

1. INTRODUÇÃO

1.1. Este procedimento deve ser usado quando ocorrer um incidente que afete a segurança da informação da NEW WAVE, com o objetivo de garantir uma resposta rápida, eficaz e coordenada.

2. PROPÓSITO

2.1. Os objetivos deste procedimento de resposta a incidentes são:

2.1.1. Fornecer uma visão geral de como a NEW WAVE responderá a um incidente que afete a sua segurança da informação;

2.1.2. Definir quem responderá a um incidente, seus papéis e responsabilidades;

2.1.3. Descrever os recursos que estão em vigor para auxiliar na gestão do incidente;

2.1.4. Definir como serão tomadas as decisões sobre nossa resposta a um incidente;

2.1.5. Explicar como será a comunicação dentro da organização e com as partes interessadas;

2.1.6. Fornecer detalhes de contato para as partes interessadas; e

2.1.7. Definir o que acontecerá quando o incidente for resolvido.

3. ESCOPO

3.1. Todos os membros da equipe nomeados neste documento, receberão uma cópia que deverá estar disponível quando necessário.

3.2. Os detalhes de contato serão verificados e atualizados pelo menos três vezes ao ano. Alterações no contato ou outros detalhes relevantes que ocorram fora das verificações programadas, devem ser enviadas para **comite@newwavetech.com.br** o mais rápido possível, após a mudança ter ocorrido.

3.3. Todas as informações pessoais coletadas como parte do procedimento de resposta a incidentes e contidas neste documento, serão usadas puramente para fins de

gerenciamento de incidentes de segurança da informação e estão sujeitas à legislação de proteção de dados.

3.4. Este procedimento deve ser considerado em conjunto com os seguintes documentos:

- POL-11302-0001 - Política de Segurança da Informação;
- PRO-11302-0002 - Procedimento de Registro de Não Conformidades.

4. PROCEDIMENTO

4.1. Fluxograma de resposta a incidentes:

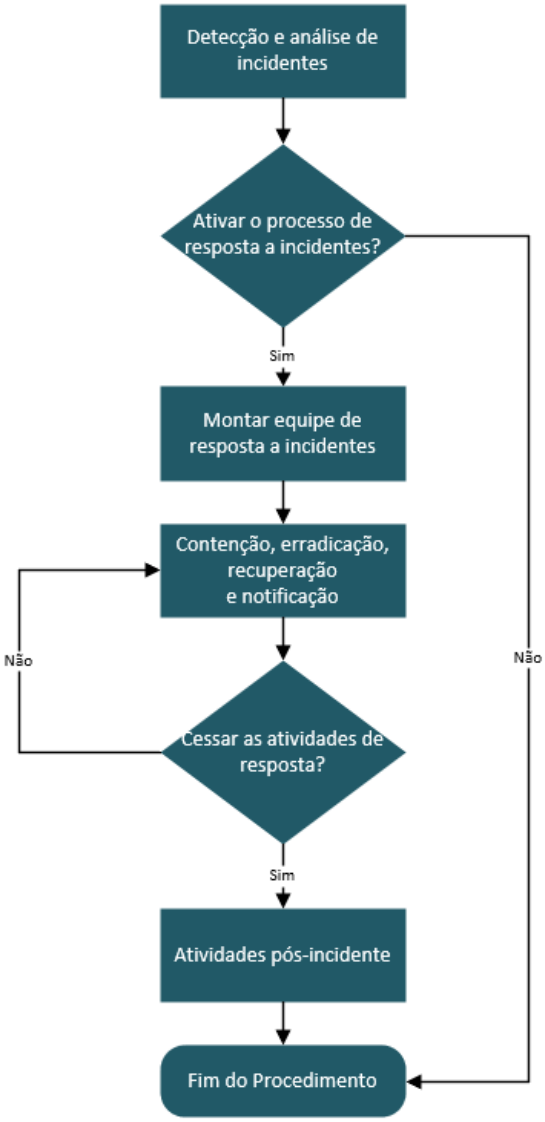

Figura 1: Fluxograma do procedimento de resposta a incidentes

4.2. Detecção e análise de incidentes

O incidente pode ser detectado de várias maneiras e através de várias fontes diferentes, dependendo da natureza e localização do incidente. Alguns incidentes podem ser detectados através de softwares usadas dentro da NEW WAVE ou por colaboradores que notam atividades incomuns. Outros podem ser notificados por terceiros, como um cliente, fornecedor ou autoridade que tomou conhecimento de uma violação, talvez porque as informações violadas foram usadas de alguma forma para fins maliciosos.

Não é incomum que haja um atraso entre a ocorrência do incidente e sua detecção real. Um dos objetivos do Sistema de Segurança da Informação é reduzir esse tempo. O fator mais importante é que o procedimento de resposta a incidentes deve ser iniciado o mais rápido possível após a sua detecção, para que uma resposta eficaz possa ser dada.

4.2.1. Avaliação de impacto

Todas essas detecções serão registradas como não-conformidades, conforme o **PRO-11302-0002 - Procedimento de Registro de Não Conformidades** e uma avaliação inicial de impacto deve ser realizada pelo Comitê para decidir a resposta apropriada.

4.3. Ativando o procedimento de resposta a incidentes

Uma vez notificado de um incidente, o gestor do comitê da Equipe deve decidir se o impacto real ou potencial do incidente justifica a ativação do Procedimento de Resposta a Incidentes e a convocação da Equipe de Resposta a Incidentes.

Uma avaliação inicial de impacto já terá sido feita pelo Comitê, mas o gestor do comitê, antes de decidir se uma resposta formal a incidentes deve ser iniciada, deve avaliar se algum dos seguintes se aplicam:

- Há perda real ou potencial significativa de informações confidenciais
- Há uma interrupção real ou potencial significativa nas operações comerciais
- Há risco significativo para a reputação do negócio
- Qualquer outra situação que possa causar impacto significativo para a organização

Em caso de discordância ou incerteza sobre se ativará uma resposta a incidentes, a decisão do gestor do comitê será definitiva.

Se for decidido não ativar o procedimento, então um plano deve ser criado para permitir uma resposta de nível de prioridade mais baixa.

Se o incidente justificar a ativação do Procedimento de Resposta a Incidentes, o gestor do comitê começará a montar Equipe de Resposta a Incidentes.

4.4. Montar Equipe de Resposta a Incidentes

Uma vez tomada a decisão de ativar o Procedimento de Resposta a Incidentes, o gestor do comitê da Equipe garantirá que todos os membros da equipe sejam contatados, informados da natureza do incidente e solicitados a se reunirem em um local apropriado.

A exceção é o Facilitador de Equipe, que será solicitado a comparecer ao local do incidente para começar a coletar informações, para que a Equipe possa conduzir o processo de forma apropriada.

4.4.1. Membros da Equipe de Resposta a Incidentes

A Equipe de Resposta a Incidentes será composta das seguintes pessoas, com as funções específicas e com os nomes indicados, embora a composição da equipe possa variar de acordo com a natureza do incidente:

NOME	TÍTULO	PAPEL NO PLANO
Rodrigo Nunes	Gerente TI	Gestor do comitê
Humberto Costa	Infraestrutura de TI	Responsável pela infraestrutura, instalações e TI
Iago Lima	Suporte	Facilitador da Equipe
José Eduardo	Especialista em Segurança	Responsável pelo monitoramento e análise da segurança
Isabela Resende de Moraes	Comunicação	Responsável pelas Comunicações
Rosane Toledo	Supervisora de RH	Responsável pelas pessoas
Ingrid Frugoli	Jurídico	Responsável pelas implicações legais

Tabela 2: Membros da Equipe de Resposta a Incidentes

Os detalhes de contato acima estão listados no apêndice A deste documento.

4.5. Papéis e responsabilidades

As responsabilidades dos papéis dentro da equipe de resposta a incidentes são as seguintes:

4.5.1. Gestor do comitê

- Decide se inicia uma resposta;
- Monta a equipe de resposta a incidentes;
- Gestão geral da equipe de resposta a incidentes;
- Atua como interface com o conselho e outras partes interessadas;
- Tomador de decisão final em casos de discordância.

4.5.2. Facilitador de equipe

- Suporta a equipe de resposta a incidentes;
- Coordena recursos dentro da sala de comando ou local de encontro;
- Prepara as reuniões registrando ações e decisões;
- Atualiza os membros da equipe sobre o último status em seu retorno ao centro de comando;
- Facilita a comunicação por e-mail, telefone ou outros métodos;
- Monitora informações externas, como notícias.

4.5.3. Tecnologia da informação

- Fornece informações sobre questões relacionadas à tecnologia;
- Auxilia na avaliação de impacto.

4.5.4. Gestão das instalações

- Lida com aspectos de segurança física e acesso;
- Fornece presença de segurança, se necessário.

4.5.5. Recursos Humanos

- Avalia e aconselha sobre questões de política de RH e contrato de trabalho;
- Representa os interesses dos funcionários da organização;
- Assessoria em questões de capacidade e disciplina.

4.5.6. Comunicações (Relações públicas e mídia)

- Responsável por garantir que as comunicações internas sejam eficazes;
- Decide o nível, a frequência e o conteúdo das comunicações com partes externas como a mídia;
- Define abordagem para manter as partes afetadas informadas, por exemplo, clientes, acionistas.

4.5.7. Jurídico

- Aconselha sobre o que deve ser feito para garantir o cumprimento das leis e marcos regulatórios relevantes;
- Avalia as implicações legais reais e potenciais do incidente e as ações subsequentes.

4.6. Gerenciamento de incidentes, monitoramento e comunicação

Uma vez identificada uma resposta adequada ao incidente, a Equipe de Respostas a Incidentes precisa ser capaz de gerenciar a resposta geral, monitorar o estado do incidente e garantir que uma comunicação eficaz esteja ocorrendo em todos os níveis.

As reuniões regulares da Equipe de Respostas a Incidentes devem ser realizadas em uma frequência apropriada, decidida pelo gestor do comitê. Uma agenda para essas reuniões está no Apêndice C. O objetivo dessas reuniões é garantir que os recursos de gerenciamento de incidentes sejam gerenciados de forma eficaz e que as decisões sejam tomadas prontamente, com base em informações adequadas.

4.7. Procedimentos de comunicação

É vital que as comunicações eficazes sejam mantidas entre todas as partes envolvidas na resposta ao incidente.

Os principais meios de comunicação durante um incidente serão inicialmente presenciais e telefônicos, tanto fixos quanto móveis. O e-mail não deve ser usado, a menos que a permissão para fazê-lo tenha sido dada pela Equipe de Respostas a Incidentes.

As seguintes diretrizes devem ser seguidas em todas as comunicações:

- Fique calmo e evite conversas longas;
- Aconselhar a todos sobre a necessidade de encaminhar solicitações de informações à Equipe de Respostas a Incidentes;
- Se a chamada for atendida por alguém que não seja o contato, pergunte se o contato está disponível em outro lugar;
- Se não puder ser contatado, deixe uma mensagem para entrar em contato com você em um determinado número;
- Não forneça detalhes sobre o incidente; e
- Sempre documente detalhes do horário de atendimento, respostas e ações tomadas.

Todas as comunicações devem ser registradas com clareza e precisão, pois os registros podem ser necessários como parte de uma ação legal posteriormente.

4.7.1. Comunicação externa

Dependendo do incidente, pode haver uma variedade de partes externas que serão comunicadas durante o curso da resposta. É importante que as informações divulgadas a terceiros sejam gerenciadas para que seja oportuna e precisa.

As chamadas que não são de agências diretamente envolvidas na resposta ao incidente (como a mídia) devem ser passadas ao membro da Equipe de Respostas a Incidentes responsável pelas comunicações.

Pode haver uma série de partes externas que, embora não estejam diretamente envolvidas no incidente, podem ser afetadas por ele e precisam ser alertadas para este fato. Estes podem incluir:

- Clientes;
- Fornecedores;
- Franquias;
- Órgãos reguladores;
- Autoridades fiscalizadoras.

O responsável pelas Comunicações deve fazer uma lista de tais partes interessadas e definir a mensagem que deve ser dada a eles. Uma lista de algumas agências externas é dada no Apêndice B.

Os interessados que não foram alertados pela Equipe de Respostas a Incidentes podem ligar para obter informações sobre o incidente e seus efeitos. Essas chamadas devem ser gravadas em um registro de mensagem e passadas para o responsável pelas Comunicações da Equipe de Respostas a Incidentes.

4.7.2. Comunicação com a mídia

Em geral, a estratégia de comunicação em relação à mídia, será emitir atualizações via alta gestão. Nenhum membro da equipe deve dar uma entrevista para a mídia, a menos que seja previamente autorizado pela Equipe de Respostas a Incidentes.

A interface preferencial com a mídia, será emitir comunicados de imprensa previamente escritos. Em circunstâncias excepcionais, uma coletiva de

imprensa será realizada para responder a perguntas sobre o incidente e seus efeitos. É responsabilidade pelas Comunicações, organizar o local e fazer contato com a imprensa que desejar participar.

Na elaboração de uma declaração para a mídia, devem ser observadas as seguintes diretrizes:

- Informações pessoais devem estar sempre protegidas;
- Não especular sobre o incidente ou sua causa;
- Certifique-se das orientações jurídicas antes de emitir quaisquer declarações;
- Tente antecipar respostas para perguntas que possam ser feitas;
- Enfatize que ações estão sendo tomadas e que, tudo o que for possível será feito.

Os seguintes membros da equipe serão nomeados porta-vozes da organização, caso mais informações precisem ser emitidas, como por exemplo, em uma conferência de imprensa:

Nome	Cargo	Classificação do Incidente
José Eduardo S. Soares	Especialista em SI	Baixo
Rodrigo Nunes	Gerente de TI	Médio
Ingrid Frugoli	Advogada	Médio
Newton Souza	Diretor Jurídico	Alto
Sérgio Pedreiro	CFO	Alto

Tabela 4: Membros indicados para conferência com a imprensa

O porta-voz mais apropriado dependerá da escala do incidente e de seus efeitos sobre clientes, fornecedores, titulares de dados e outras partes interessadas.

4.8. Contenção de incidentes, erradicação, recuperação e notificação

4.8.1. Contenção

O primeiro passo será tentar impedir que o incidente piore, ou seja, contê-lo. No caso de um ataque de vírus, isso pode implicar a desconexão das partes afetadas da rede. Para um ataque de hackers, pode ser necessário desativar certos perfis ou portas no firewall ou talvez, até mesmo desconectar a rede interna da Internet completamente. As ações específicas a serem realizadas dependerão das circunstâncias do incidente.

Nota: se for considerado provável que as provas digitais precisem ser coletadas para serem usadas judicialmente, devem ser tomadas precauções para garantir que tais evidências permaneçam intactas. Isso significa que os dados relevantes não devem ser alterados deliberadamente ou acidentalmente. Recomenda-se que uma assessoria especializada seja obtida neste momento - veja contatos no Apêndice B.

Particularmente (mas não exclusivamente), se houver suspeita de crime no incidente, devem ser mantidos registros precisos das ações tomadas e das evidências reunidas, de acordo com as diretrizes forenses digitais. Os principais princípios dessas diretrizes são os seguintes:

Princípio 1: Não altere nenhum dado. Se algo for feito e resultar na alteração de dados relevantes, isso poderá afetar qualquer caso judicial subsequente.

Princípio 2: Apenas acesse os dados originais em circunstâncias excepcionais. Um especialista treinado usará ferramentas para tirar um pouco da cópia de qualquer dado mantido na memória, seja em um disco rígido, memória flash ou um cartão SIM de um telefone. Toda a análise ocorrerá na cópia e o original nunca deve ser tocado, a menos que em circunstâncias excepcionais, por exemplo, o tempo seja essencial e obter informações para prevenir um novo crime é mais importante do que manter as evidências admissíveis.

Princípio 3: Mantenha sempre um rastro de auditoria do que foi feito. Ferramentas forenses farão isso automaticamente, mas isso também se aplica às primeiras pessoas no local. Tirar fotos e vídeos é válido, desde que não haja impeditivos.

Princípio 4: O responsável deve garantir que as diretrizes sejam seguidas. Antes da chegada de um especialista, devem ser coletadas informações básicas. Isso pode incluir:

- Fotografias ou vídeos de mensagens ou informações relevantes;
- Registros da cronologia do incidente;
- Documentos originais, incluindo registros de quem os encontrou, onde e quando;
- Detalhes de quaisquer testemunhas.

Uma vez coletadas, as provas serão mantidas em um lugar seguro, onde não possam ser adulteradas e uma cadeia formal de custódia estabelecida.

A evidência pode ser necessária:

- Para análise posterior sobre a causa do incidente;
- Como prova forense para processos criminais ou cíveis;
- Em apoio a quaisquer negociações de compensação com fornecedores de software ou serviços.

Em seguida, uma imagem clara do que aconteceu precisa ser estabelecida. A extensão do incidente e as implicações devem ser apuradas, antes que qualquer tipo de ação de contenção possa ser adotado.

Os registros de auditoria podem ser examinados para juntar a sequência de eventos. Deve-se tomar cuidado para que, apenas cópias seguras de registros que não tenham sido adulterados sejam usadas.

4.8.2. Erradicação

Ações para corrigir os danos causados pelo incidente, como a exclusão do malware, devem ser submetidas ao processo de gerenciamento de mudanças (como uma mudança emergencial, se necessário). Essas ações devem ser destinadas a corrigir a causa atual e evitar que o incidente ocorra. Quaisquer vulnerabilidades que tenham sido exploradas como parte do incidente devem ser identificadas. Dependendo do tipo de incidente, a erradicação pode às vezes ser desnecessária.

4.8.3. Recuperação

Durante a fase de recuperação, os sistemas devem ser restaurados de volta à sua condição pré-incidente. Embora as ações necessárias sejam realizadas para enfrentar quaisquer vulnerabilidades exploradas como parte do incidente, elas também podem envolver atividades como instalação de patches, alteração de senhas, configuração de servidores e procedimentos de alteração.

4.8.4. Notificação

A notificação de um incidente de segurança da informação e a consequente perda de dados, é uma questão sensível que deve ser tratada com cuidado e com total aprovação da gestão. A EQUIPE DE RESPOSTAS A INCIDENTES decidirá, com o apoio da assessoria jurídica e outros especialistas e com o máximo possível de entendimento do impacto do incidente, qual notificação será necessária e a ação que tomará.

A NEW WAVE sempre cumprirá integralmente os requisitos legais e regulamentares aplicáveis em relação à notificação de incidentes.

Os registros coletados como parte da resposta ao incidente podem ser exigidos como parte de quaisquer investigações de órgãos reguladores.

4.9. Atividades pós-incidente

O Gestor do comitê decidirá, com base nas últimas informações do incidente e outros membros da equipe, o ponto em que as atividades de resposta devem ser cessadas.

A recuperação e a execução de planos podem continuar além deste ponto, mas sob menor controle de gestão.

Esta decisão caberá ao Gestor do comitê, mas deve basear-se nos seguintes critérios:

- A situação foi totalmente resolvida ou está razoavelmente estável;
- O ritmo de mudança da situação diminuiu a um ponto em que poucas decisões são necessárias;
- A resposta apropriada está indo bem e os planos de recuperação estão progredindo;
- O grau de risco para o negócio diminuiu a um ponto aceitável;
- Responsabilidades legais e regulatórias imediatas foram cumpridas.

Se a recuperação do incidente estiver em andamento, o Gestor do comitê deve definir as próximas ações a serem tomadas. Estes podem incluir:

- Reuniões menos frequentes da Equipe de Respostas a Incidentes, dependendo das circunstâncias;
- Informar todas as partes envolvidas que a Equipe de Respostas a Incidentes está parada;
- Garantir que toda a documentação do incidente seja garantida;
- Solicitando que todos os colaboradores não envolvidos retornem às funções normais.

Todas as ações tomadas como parte dessa ação devem ser registradas. Depois que a EQUIPE DE RESPOSTA A INCIDENTES for desmobilizado, o Gestor do comitê realizará uma reunião com todos os membros, idealmente dentro de 24 horas. Os registros relevantes do incidente serão examinados pela Equipe de Respostas a Incidentes para garantir que eles reflitam os eventos reais e representem um registro completo e preciso do incidente. Quaisquer comentários da equipe serão gravados.

5. PAPÉIS E RESPONSABILIDADES

5.1. COMITÊ DE SEGURANÇA DA INFORMAÇÃO

5.1.1. Definir sobre quem deve ser incluído na estrutura de resposta a incidentes para que as pessoas certas estejam disponíveis no caso de um incidente de segurança da informação acontecer.

5.1.2. Buscar deixar sempre claros e concisos os procedimentos contidos neste documento, pois possivelmente serão utilizados em tempos de grande estresse pelas pessoas envolvidas.

5.1.3. Procurar sempre ter alternativas, como um Plano B, para cada aspecto do procedimento, como outros responsáveis e acesso a documentos e recursos críticos.

6. REVISÕES

6.1. Este procedimento é revisado com periodicidade anual ou conforme o entendimento do Comitê de Segurança da Informação.

7. GESTÃO DO PROCEDIMENTO

7.1. O Procedimento de Resposta a Incidentes de Segurança da Informação é aprovado pelo Comitê de Segurança da Informação, junto com a Diretoria da NEW WAVE.

8. CONTROLE DE VERSÃO

Data: 10/08/2023 - Versão 1.0 - Versão Inicial.

A presente política foi aprovada no dia 17/08/2023, por:

Sérgio Pedreiro

Diretor Financeiro

Apêndice A: Formulário de contato inicial

A tabela abaixo deve ser usada para registrar o contato inicial bem-sucedido e malsucedido com os membros da Equipe de Respostas a Incidentes.

Nota: Para a coluna Resultado, escolha entre "Contatado", "Sem resposta", "Mensagem deixada e "Incomunicável"

Nome	Função no Plano	Fone Fixo	Celular	Data/Hora	Resultado
José Eduardo	Seg. Informação				
Rodrigo Nunes	Gerente de TI				
Humberto Costa	Infra de TI				
Isabela Moraes	Comunicação				
Ingrid Frugoli	Jurídico				

Tabela 5: Formulário de contato inicial

Apêndice B: Contatos externos úteis

A tabela a seguir mostra os detalhes de contato de terceiros que podem ser úteis, dependendo da natureza do incidente:

Órgão/Empresa	Contato	Telefone	E-mail
Provedor de Internet			
Broadcast			
ANPD			

Tabela 6: Formulário de contatos externos úteis

Apêndice C: Reunião da equipe de resposta a incidentes

Recomenda-se que a seguinte agenda seja usada para reuniões da Equipe de Resposta a Incidentes.

AGENDA	
Participantes	Todos os membros da Equipe de Resposta a Incidentes
Local	Torre do Rio Sul
Frequência	Manhã e Tarde
Condutor da reunião	Gestor do comitê ou o facilitador

1. Ações da reunião anterior
2. Atualização de status de incidente
3. Decisões necessárias
4. Alocação de tarefas
5. Comunicações internas
6. Comunicações externas
7. Outros assuntos pertinentes