NEW WAVE

PROCEDIMENTO DE REGISTRO DE NÃO CONFORMIDADE

Comitê de Segurança da Informação

DOCUMENTO	CLASSIFICAÇÃO	DATA	APROVADO POR:	VERSÃO
PRO-11302-0002	Informação Interna	10/08/2023	Rodrigo Nunes	1.0

PROCEDIMENTO DE REGISTRO DE NÃO CONFORMIDADE				
DOCUMENTO	**CLASSIFICAÇÃO**	**DATA**	**APROVADO POR:**	**VERSÃO**
PRO-11302-0002	Informação Interna	10/08/2023	Rodrigo Nunes	1.0

SUMÁRIO

PROCEDIMENTO DE REGISTRO DE NÃO CONFORMIDADE				
DOCUMENTO	**CLASSIFICAÇÃO**	**DATA**	**APROVADO POR:**	**VERSÃO**
PRO-11302-0002	Informação Interna	10/08/2023	Rodrigo Nunes	1.0

1. INTRODUÇÃO

1.1. Este procedimento deve ser usado quando for detectada uma não conformidade real ou potencial que afete a segurança da informação da NEW WAVE.

2. PROPÓSITO

2.1. O objetivo deste procedimento é estabelecer uma sistemática para executar ações corretivas e/ou preventivas para eliminar as causas de não conformidades reais e potenciais, que possam afetar o Sistema de Segurança da Informação da NEW WAVE garantindo o cumprimento das Políticas e Procedimentos definidos no Sistema de Segurança da Informação da NEW WAVE.

3. ESCOPO

3.1. Este procedimento se aplica a todo o Sistema de Segurança da Informação da NEW WAVE.

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

- **POL-11302-0001 - Política de Segurança da Informação**;
- **PRO-11302-0001 - Procedimento de Resposta a Incidentes de Segurança da Informação**.

4. PROCEDIMENTO

4.1. Registro de Não-Conformidade:

4.1.1. Todo colaborador, ao detectar uma não conformidade real ou potencial, deve imediatamente abrir um tíquete em nosso sistema de chamados.

NOTA: O Comitê de Segurança da Informação também poderá emitir um RNC quando detectar uma não conformidade; por força de auditoria interna ou por solicitação de qualquer colaborador que se sinta desconfortável em explicitar seu nome (o Comitê manterá sigilo neste caso).

4.1.2. O gestor do Comitê delibera sobre o assunto e indica a área/responsável para a tratativa do problema. Caso o assunto não proceda em relação ao Sistema de Segurança da Informação implantado, o gestor notificará o emitente e o Comitê para o cancelamento do RNC.

4.1.3. Quando procedente, o Comitê encaminha o tíquete aberto para o responsável da investigação da causa da não-conformidade, que deverá também determinar as ações corretivas ou preventivas para a eliminação do problema, e quando se tratar de reclamações de clientes, fornecedores ou titulares de dados, posicioná-los sobre a solução aplicada.

4.1.4. Após as ações executadas pelo responsável da investigação, o RNC deverá ser reencaminhado ao Comitê de Segurança da Informação, com a descrição da solução aplicada e, se for o caso, com arquivo de documentos complementares anexados.

4.1.5. O gestor do Comitê providenciará em tempo hábil a apresentação da ocorrência ao Comitê de Segurança da Informação, nas reuniões de análise crítica do sistema. Caso o Comitê entenda que a tratativa dada ao caso não atendeu a não conformidade, será solicitada para a área envolvida novas providências quanto ao RNC.

4.1.6. Semestralmente deverá ser analisado pelo Comitê:

- A frequência e o impacto das RNC nos processos da organização;
- Resultados dos indicadores de desempenho;
- RNCs abertas e considerando os prejuízos com materiais consumidos etc.

4.2. Detecção e análise de incidentes

Através das investigações de um RNC, um 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.

4.3. Avaliação de impacto

A avaliação inicial de impacto deve ser realizada pelo Comitê para decidir a resposta apropriada.

Esta avaliação de impacto deve estimar:

- A extensão do impacto na infraestrutura de TI, incluindo computadores, redes, equipamentos e acomodações;
- Os ativos de informação que podem estar em risco ou foram comprometidos;
- A provável duração do incidente, ou seja, quando pode ter começado;
- As áreas de negócios afetadas e a extensão do impacto para eles; e
- Indicação inicial da provável causa do incidente.

Essas informações devem ser documentadas para uma compreensão mais clara da situação e para que ela esteja disponível para consultas e/ou posterior revisão.

Uma lista dos ativos de informação, atividades, produtos, serviços, equipes e processos que possam ter sido afetados pelo incidente, deve ser criada juntamente com uma avaliação da extensão do impacto.

4.3.1. Priorização de incidentes

Com base na avaliação de impacto, um incidente será classificado com os níveis de prioridade Alta, Média ou Baixa, de acordo com as orientações da tabela abaixo:

Nível de Prioridade	Descrição
Alta	Interrupção real ou potencialmente significativa para os negócios. Exemplos: • Um malware foi detectado e está se espalhando pela rede • Um acesso não autorizado em quantidades significativas de dados confidenciais foi detectado • O Site ou o Portal não estão disponíveis para os clientes, devido a um possível problema nos serviços
Média	Interrupção localizada, afetando várias áreas de negócio. Exemplos: • Rede única indisponível • Rede executando lentamente • Perda de um disco rígido
Baixa	Inconveniência localizada, afetando um único usuário. Exemplos: • Pequena violação da política de segurança da informação • Alerta de vírus em um único computador • Compartilhamento de senha

Tabela 1: Níveis de Prioridade dos Incidentes

Como resultado dessa análise inicial, o Comitê ou qualquer membro da equipe tem autoridade para entrar em contato com o gestor do comitê de resposta ao incidente a qualquer momento, para pedir que avalie se o procedimento PRO-11302-0001 - Procedimento de Resposta a Incidentes de Segurança da Informação deve ser ativado. Este é provavelmente o caso para todos os incidentes de alta prioridade e para incidentes de prioridade média, quando considerado apropriado.

5. PAPÉIS E RESPONSABILIDADES

5.1. COMITÊ DE SEGURANÇA DA INFORMAÇÃO

5.1.1. Analisar periodicamente os Registros de Não Conformidade gerados.

5.1.2. Analisar se o RNC é procedente, registrar e encaminhar à área competente para a solução da não-conformidade.

5.1.3. Analisar semestralmente:

- A frequência e o impacto dos RNC´s na NEW WAVE;
- Resultados dos indicadores de desempenho; e
- RNC´s abertas, considerando os prejuízos ou danos gerados.

5.2. GESTOR DA EQUIPE DE RESPOSTA A INCIDENTES

5.2.1. Apoiar o Comitê na avaliação de impacto do incidente detectado nas investigações de um RNC;

5.2.2. Decidir pela ativação do procedimento PRO-11302-0001 - Procedimento de Resposta a Incidentes de Segurança da Informação.

5.3. GESTOR DA ÁREA

5.3.1. Tratar o RNC de acordo com seus itens e identificar/implantar ações para a solução do problema.

5.4. TODOS OS COLABORADORES

5.4.1. Ao detectar uma não conformidade ou necessidade de registro de RNC real ou potencial, comunicar o Comitê para a formalização do registro.

6. REGISTROS

REGISTRO	RESP. PELA COLETA	MEIO/LOCAL DE ARQUIVO	INDEXAÇÃO	ACESSO	TEMPO DE ARQUIVO	DESTINO APÓS PRAZO
RNC	Comitê	Portal	Sequencial/ano	Geral	3 anos	Arquivo
Matriz de Não-Conformidades	Comitê	Portal	Sequencial/ano	Geral	3 anos	Arquivo

7. REVISÕES

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

8. GESTÃO DO PROCEDIMENTO

8.1. O Procedimento de Resposta a Incidentes de Segurança da Informação é aprovado pelo Comitê de Segurança da Informação, em conjunto com a Diretoria da NEW WAVE.

9. 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

GLOSSÁRIO

AÇÃO CORRETIVA – Ação aplicada para eliminar as causas de não - conformidades reais ou desvio ocorrido.

AÇÃO PREVENTIVA – Ação aplicada para eliminar as causas de não-conformidades potenciais, ou seja, ainda não ocorridas.

RNC – Registro de Não Conformidade é o ***documento*** utilizado para ações de disposições em requisitos não atendidos e/ou preventivo.