Norma de Gestão de Vulnerabilidade Técnica

Niva Tecnologia da Informação

www.nivati.com.br
SIG QUADRA 01 N° 985 SALAS 236 A 243 - CENTRO EMPRESARIAL PARQUE BRASILIA
- CEP: 70.610.410 - BRASILIA – DF TEL: (61) 3326-8673

Classificação Pública

ÍNDICE

1. OBJETIVOS

Esta Norma tem por objetivo a análise contínua de ativos críticos para identificar e tratar riscos de segurança da informação, identificando vulnerabilidades, alertando e acionando os responsáveis para as correções identificadas.

2. DOCUMENTOS DE REFERÊNCIA

2.1. ABNT NBR ISO/IEC 27002:2013 – Tecnologia da Informação – Técnicas de segurança – Código de prática para a Gestão da Segurança da Informação.

2.2. ABNT NBR ISO/IEC 27001:2013 – Tecnologia da Informação – Técnicas de segurança – Sistemas de Gestão de Segurança da Informação – Requisitos.

2.3. Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018.

2.4. Lei de Acesso a Informação (LAI) 12.527 de 18/11/2011.

2.5. Política de Segurança da Informação – PSIC.

2.6. Norma de Classificação da Informação.

3. PAPÉIS E RESPONSABILIDADES

3.1. Responsáveis pela elaboração – **Dirigentes da NIVA**.

3.2. Público Alvo – Canal de atendimento – Suporte TI.

4. DIRETRIZES GERAIS

4.1. Prevenção da exploração de vulnerabilidades técnicas

4.1.1. Analisar e identificar fraquezas e brechas de segurança pelos quais ameaças poderão concretizar riscos e incidentes.

4.1.2. Avaliação de riscos junto aos ativos que suportam os processos críticos e relevantes.

4.2. Ações de gerenciamento

4.2.1. Mapear todas as informações relevantes da **NIVA** que devem ter maior gestão e proteção.

4.2.2. Definir os responsáveis pela gestão e proteção destas informações.

4.2.3. Fazer o mapeamento de riscos com uma análise e definir priorização.

4.2.4. Criar relatórios para ajudar na análise, tratamento e melhorias.

4.2.5. Realizar os tratamentos de forma estruturada em procedimentos.

4.2.6. Ter indicadores de tempo de identificação, tempo de mitigação para as vulnerabilidades detectadas.

4.2.7. Detectar e corrigir falhas que podem acarretar em riscos de segurança, funcionalidade e desempenhos.

4.2.8. Alterar configurações de sistemas para deixá-los mais eficientes.

4.2.9. Implantar mecanismos de segurança e realizar suas atualizações.

4.2.10. Focar na melhoria contínua dos sistemas de segurança.

4.2.11. Deve-se definir e desenhar o processo a ser executado.

4.2.12. Disponibilizar treinamentos para os técnicos que analisam e tratam estas vulnerabilidades.

4.3. Ações de monitoramento

4.3.1. Estabelecer ações que permitam medir ciclos de identificação de vulnerabilidades no intuito de definir assertivamente controles de tratamento para reincidências.

4.3.2. Definir indicadores relacionados aos tipos de vulnerabilidades e frequência de incidência buscando o tratamento das causas.

4.3.3. Definir indicadores de acerca das ações de tratamento de vulnerabilidades antecipando a materialização de riscos ocasionados pela mesma.

4.4. Ações de tratamento

4.4.1. Ações preventivas de tratamento aos riscos identificados por meio das vulnerabilidades ou aceitação dos riscos em consonância à tolerância de riscos estabelecida pela **NIVA**.

4.4.2. O levantamento e análise devem ser rotinas periódicas e repetidas, para determinar quais mudanças ocorreram comparadas com a última avaliação realizada.

4.4.3. Estabelecer critérios e fluxos de comunicação aos responsáveis pelos ativos de tecnologia acelerando a identificação dos responsáveis pelo tratamento.

4.5. Em casos de quebra de Segurança da Informação por meio de recursos de informática, o Canal de Atendimento (suporte@nivati.com.br) deve ser imediatamente acionado para adotar as providências necessárias.

4.6. Esta norma entra em vigor a partir da data de sua divulgação e sua revisão deve ocorrer em intervalos planejados, pelo menos anualmente, ou sempre que existirem alterações das regras acima expostas.

4.7. Dúvidas: Qualquer dúvida relativa a esta Norma deve ser encaminhada ao CSIC.