

Norma de Gestão de Vulnerabilidade Técnica

Alsar Tecnologia em Redes

Classificação Pública

ÍNDICE

1.	<u>OBJETIVOS</u>	3
2.	<u>DOCUMENTOS DE REFERÊNCIA</u>	3
3.	<u>PAPÉIS E RESPONSABILIDADES</u>	3
4.	<u>DIRETRIZES GERAIS</u>	3

- **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.

- **DOCUMENTOS DE REFERÊNCIA**

- ABNT NBR ISO/IEC 27002:2013 – Tecnologia da Informação – Técnicas de segurança – Código de prática para a Gestão da Segurança da Informação.
- ABNT NBR ISO/IEC 27001:2013 – Tecnologia da Informação – Técnicas de segurança – Sistemas de Gestão de Segurança da Informação – Requisitos.
- Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018.
- Lei de Acesso a Informação (LAI) 12.527 de 18/11/2011.
- Política de Segurança da Informação – PSIC.
- Norma de Classificação da Informação.

- **PAPÉIS E RESPONSABILIDADES**

- Responsáveis pela elaboração – **Dirigentes da Alsar**.
- Público Alvo – Canal de atendimento – Suporte TI.

- **DIRETRIZES GERAIS**

- **Prevenção da exploração de vulnerabilidades técnicas**
- Analisar e identificar fraquezas e brechas de segurança pelos quais ameaças poderão concretizar riscos e incidentes.
- Avaliação de riscos junto aos ativos que suportam os processos críticos e relevantes.
- **Ações de gerenciamento**
- Mapear todas as informações relevantes da **Alsar** que devem ter maior gestão e proteção.
- Definir os responsáveis pela gestão e proteção destas informações.
- Fazer o mapeamento de riscos com uma análise e definir priorização.
- Criar relatórios para ajudar na análise, tratamento e melhorias.
- Realizar os tratamentos de forma estruturada em procedimentos.
- Ter indicadores de tempo de identificação, tempo de mitigação para as vulnerabilidades detectadas.
- Detectar e corrigir falhas que podem acarretar em riscos de segurança, funcionalidade e desempenhos.

- Alterar configurações de sistemas para deixá-los mais eficientes.
- Implantar mecanismos de segurança e realizar suas atualizações.
- Focar na melhoria contínua dos sistemas de segurança.
- Deve-se definir e desenhar o processo a ser executado.
- Disponibilizar treinamentos para os técnicos que analisam e tratam estas vulnerabilidades.
- **Ações de monitoramento**
- Estabelecer ações que permitam medir ciclos de identificação de vulnerabilidades no intuito de definir assertivamente controles de tratamento para reincidências.
- Definir indicadores relacionados aos tipos de vulnerabilidades e frequência de incidência buscando o tratamento das causas.
- Definir indicadores de acerca das ações de tratamento de vulnerabilidades antecipando a materialização de riscos ocasionados pela mesma.
- **Ações de tratamento**
- Ações preventivas de tratamento aos riscos identificados por meio das vulnerabilidades ou aceitação dos riscos em consonância à tolerância de riscos estabelecida pela **Alsar**.
- O levantamento e análise devem ser rotinas periódicas e repetidas, para determinar quais mudanças ocorreram comparadas com a última avaliação realizada.
- Estabelecer critérios e fluxos de comunicação aos responsáveis pelos ativos de tecnologia acelerando a identificação dos responsáveis pelo tratamento.
- Em casos de quebra de Segurança da Informação por meio de recursos de informática, o Canal de Atendimento (suporte@alsar.com.br) deve ser imediatamente acionado para adotar as providências necessárias.
- 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.
- Dúvidas: Qualquer dúvida relativa a esta Norma deve ser encaminhada ao CSIC.