Norma de Códigos Maliciosos

Alsar Tecnologia em Redes

SHN Qd. 01 Bloco A Conjunto A Sala 1419 Ed. Le Quartier – CEP: 70.701-010
FONE: (61) 3327-3699 – e-mail: alsar@alsar.com.br

Classificação Pública

ÍNDICE

- **OBJETIVOS**

- Esta Norma tem por objetivo definir regras de segurança para evitar e tratar códigos maliciosos no ambiente tecnológico da **Alsar**.

- **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.

- **PAPÉIS E RESPONSABILIDADES**

- Responsáveis pela elaboração – **Dirigentes da Alsar**.
- Público Alvo – Dirigentes, colaboradores, parceiros e fornecedores.

- **DIRETRIZES GERAIS**

- No intuito da proteção ao ambiente tecnológico da **Alsar**, prioritariamente, o suporte a TI deve prover operação e monitoramento das soluções de segurança da informação e comunicação, gestão de vulnerabilidades, monitoramento cibernéticos, respostas aos incidentes de segurança, sistemas de detecção e bloqueio de programas maliciosos, testes de invasão, gestão de disponibilidade e conscientização de segurança da informação e comunicação.
- Quando houver correções ou atualizações do *software* de antivírus, este deve ser testado e rapidamente implementado, para que proteja o ambiente de ações maliciosas ou qualquer tentativa de ataque.
- As atualizações e as correções do *software* de detecção e bloqueio de programas maliciosos devem ser homologadas antes de serem aplicadas ao ambiente de produção.
- É obrigatório o uso de *software* de antivírus corporativo, homologado e aprovado nos equipamentos computacionais que realizem troca direta de arquivos com os usuários, mantendo-os permanentemente ativado e atualizado.
- O *software* de antivírus deve monitorar os arquivos e programas quanto à contaminação por vírus eletrônico antes de sua utilização.
- Padrões e procedimentos para instalação, configuração, utilização e atualização de *software* de antivírus devem ser estabelecidos pela área de suporte a TI.

- O usuário não deve ter acesso as configurações e possibilidade de desativar o *software* de antivírus na sua estação de trabalho.
- Os técnicos de TI devem participar e estar sempre monitorando novidades sobre prováveis vírus novos, e isolá-los antes de disponibilizados paths no *software* de antivírus.
- Os arquivos anexados às mensagens de correio eletrônico, logo após seu recebimento, devem ser verificados quanto à contaminação por vírus através do *software* de antivírus homologado e instalado nas estações de trabalho dos dirigentes, colaboradores, parceiros e fornecedores que estão na rede da **Alsar**.
- O *software* de antivírus deve monitorar os arquivos e programas quanto à contaminação por vírus eletrônico antes de sua utilização e emitir um alerta se a contaminação não for solucionada.
- Os usuários devem comunicar qualquer identificação de intrusão/vírus em suas estações de trabalho para tratamento pelo suporte.
- Os usuários não podem instalar aplicações não licenciadas e que não façam parte dos sistemas homologados no ambiente corporativo da **Alsar**.
- Os usuários ao usarem *pendrives* devem passar o *software* de antivírus antes de utilizar o dispositivo.
- O suporte deve implementar controle de *blacklist*, para garantir o bloqueio de sites que foram previamente denunciados como disseminadores de mensagens, ou propagadores de aplicações maliciosas.
- 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.