Norma de Códigos Maliciosos

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

ÍNDICE

1. OBJETIVOS

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

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.

3. PAPÉIS E RESPONSABILIDADES

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

3.2. Público Alvo – Dirigentes, colaboradores, parceiros e fornecedores.

4. DIRETRIZES GERAIS

4.1. No intuito da proteção ao ambiente tecnológico da **NIVA**, 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.

4.2. 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.

4.2.1. 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.

4.3. 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.

4.3.1. O *software* de antivírus deve monitorar os arquivos e programas quanto à contaminação por vírus eletrônico antes de sua utilização.

4.3.2. Padrões e procedimentos para instalação, configuração, utilização e atualização de *software* de antivírus devem ser estabelecidos pela área de suporte a TI.

4.3.3. O usuário não deve ter acesso as configurações e possibilidade de desativar o *software* de antivírus na sua estação de trabalho.

4.3.4. 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.

4.4. 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 **NIVA**.

4.4.1. 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.

4.5. Os usuários devem comunicar qualquer identificação de intrusão/vírus em suas estações de trabalho para tratamento pelo suporte.

4.6. Os usuários não podem instalar aplicações não licenciadas e que não façam parte dos sistemas homologados no ambiente corporativo da **NIVA**.

4.7. Os usuários ao usarem *pendrives* devem passar o *software* de antivírus antes de utilizar o dispositivo.

4.8. 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.

4.9. 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.

4.10. 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.

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