1. **Introdução**
   1. A Norma de segurança da informação **N-SI-006** complementa Política Geral de Segurança da Informação, definindo as diretrizes para proteção dos ativos/serviços de informação SOLUS METAL DO BRASIL contra ameaças e códigos maliciosos de qualquer natureza.
2. **Propósito**
   1. Estabelecer diretrizes para a proteção dos ativos/serviços de informação SOLUS METAL DO BRASIL contra ameaças e códigos maliciosos de qualquer natureza.
3. **Escopo**
   1. Esta norma obedece ao escopo definido na Política Geral de Segurança da Informação.
4. **Diretrizes**
   1. **Ferramenta de proteção contra códigos maliciosos**
      1. A SOLUS disponibiliza ferramentas para proteção dos seus ativos/serviços de informação e recursos computacionais, incluindo estações de usuários, dispositivos móveis e servidores corporativos, contra ameaças e códigos maliciosos tais como vírus, cavalos de Tróia, vermes, ferramentas de captura de tela e dados digitados, softwares de propaganda e similares;
      2. Apenas a ferramenta disponibilizada pela SOLUS deve ser utilizada na proteção contra códigos maliciosos;
      3. A ferramenta de proteção contra códigos maliciosos da SOLUS adota as seguintes regras de uso:
         1. Atualização em tempo real do arquivo de assinaturas de códigos maliciosos e varredura diária em estações de usuários e servidores corporativos;
         2. As varreduras diárias devem analisar todos os arquivos em cada uma das unidades de armazenamento locais das estações de usuários e dispositivos móveis;
         3. As varreduras diárias em servidores corporativos podem ser limitadas a pastas ou arquivos específicos, de modo a evitar o comprometimento do desempenho de recursos computacionais críticos;
         4. As funções de proteção em tempo real e detecção com base no comportamento devem estar habilitadas para todas as estações de usuários e dispositivos móveis;
         5. Sites, serviços e arquivos baixados da internet detectados como possíveis ameaças serão automaticamente bloqueados em estações de usuários, dispositivos móveis e servidores corporativos;
      4. Caso uma estação de usuário ou dispositivo móvel esteja infectado ou com suspeita de infecção de código malicioso, a mesma deverá ser imediatamente isolada da rede corporativa da SOLUS e de qualquer comunicação com a internet;
      5. Caso um servidor corporativo esteja infectado ou com suspeita de infecção de código malicioso, deverão ser adotadas medidas para garantir o isolamento do mesmo da rede corporativa e da internet, levando em consideração o impacto da desativação dos serviços publicados no referido servidor;
   2. **Prevenção dos usuários contra códigos maliciosos**
      1. Mesmo com a existência de ferramentas para proteção contra códigos maliciosos, os usuários da SOLUS METAL DO BRASIL devem adotar um comportamento seguro, reduzindo a probabilidade de infecção ou propagação de códigos maliciosos;
      2. Os usuários da SOLUS devem seguir as seguintes regras para proteção contra códigos maliciosos:
         1. Não tentar efetuar o tratamento e correção de códigos maliciosos por iniciativa própria;
         2. Reportar imediatamente a área de tecnologias da informação qualquer infecção ou suspeita de infecção por código malicioso;
         3. Não desenvolver, testar ou armazenar qualquer parte de um código malicioso de qualquer tipo, a menos que expressamente autorizado;
         4. Efetuar uma varredura com a ferramenta de proteção contra códigos maliciosos fornecida pela SOLUS antes de utilizar arquivos armazenados em mídias removíveis, baixados da internet ou recebidos nos serviços de e-mail ou comunicadores instantâneos;
         5. Não habilitar MACROS para arquivos recebidos de fontes suspeitas, baixados da internet ou recebidos nos serviços de e-mail ou comunicadores instantâneos. Caso necessário, poderá ser solicitado o apoio da equipe de segurança da informação para validar se o arquivo representa ou não uma ameaça.
5. **Papéis e Responsabilidades**
   1. **GERENCIA DE TECNOLOGIA DA INFORMAÇÃO**
      1. É responsabilidade da gerencia de tecnologia da informação:
         1. Tratar casos de infecção ou suspeita de infecção por códigos maliciosos, reportando os mesmos a equipe de segurança da informação, caso necessário.
   2. **GERENCIA DE SEGURANÇA DA INFORMAÇÃO**
      1. É responsabilidade da gerencia de segurança da informação:
         1. Garantir que novas modalidades de códigos maliciosos são adequadamente investigados, tratados e protegidos pela ferramenta corporativa adotada pela SOLUS;
         2. Garantir a existência de iniciativas para divulgação sobre informações de ameaças, códigos maliciosos e medidas de proteção para os usuários da SOLUS.
6. **Sanções e Punições**
   1. Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação.
7. **Revisões**
   1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.
8. **Gestão da Norma**
   1. A norma **N-SI-006** é aprovada pelo Comitê Gestor de Segurança da Informação, em conjunto com a Diretoria da SOLUS METAL DO BRASIL.
   2. A presente norma foi aprovada no dia 26/01/2017

|  |  |  |
| --- | --- | --- |
| signaturedimage |  | signaturedimage |
| Albert Solus – Presidente |  | Alfredo Solus – Vice-Presidente |