1. **Introdução**
   1. A Norma de segurança da informação **N-SI-010** complementa Política Geral de Segurança da Informação, definindo as diretrizes para responder eventos ou incidentes de segurança estejam impactando ou possam vir a impactar ativos/serviços de informação ou recursos computacionais da SOLUS METAL DO BRASIL.
2. **Propósito**
   1. Estabelecer diretrizes para garantir a resposta e tratamento adequados a incidentes de segurança da informação que possam impactar ativos/serviços de informação ou recursos computacionais da SOLUS METAL DO BRASIL.
3. **Escopo**
   1. Esta norma obedece ao escopo definido na Política Geral de Segurança da Informação.
4. **Diretrizes**
   1. **Incidentes de segurança da informação**
      1. Todas as ocorrências que possam vir a ter impacto negativo sobre a confidencialidade, integridade ou disponibilidade dos ativos/serviços de informação ou recursos computacionais da SOLUS METAL DO BRASIL serão caracterizadas como um incidente de segurança da informação, devendo as referidas ocorrências serem tratadas de maneira a minimizar qualquer tipo de impacto e recuperar as características de segurança da informação dos itens afetados;
      2. Incidentes de segurança devem ser priorizados com base na criticidade dos ativos/serviços de informação ou recursos computacionais afetados, combinada com a estimativa de impacto prevista;
      3. Todos os incidentes de segurança da informação ou suspeitas de incidentes de segurança da informação devem ser imediatamente comunicados a área de segurança da informação;
      4. A área de segurança da informação deverá determinar a criticidade do incidente e, quando pertinente, comunicar as partes interessadas como, por exemplo, membros do time de resposta a incidentes de segurança da informação;
      5. Na ocorrência de um incidente de segurança da informação, ativos/serviços de informação ou recursos computacionais com suspeita de ter sua segurança comprometida, devem ser isolados do ambiente corporativo, de forma a garantir a contenção do incidente;
      6. A extensão dos danos do incidente de segurança deve ser avaliada para, em seguida, ser identificado o melhor curso de ação para erradicação completa do incidente e restauração dos ativos de informação afetados;
      7. Após a erradicação completa do incidente, deve ser realizada uma revisão completa da ocorrência, identificando o nível real de impacto, vulnerabilidades exploradas, a efetividade do tratamento aplicado e a necessidade de maiores ações para evitar a recorrência do incidente.
   2. **Time de resposta a incidentes de segurança da informação**
      1. O time de resposta a incidentes de segurança da informação da SOLUS METAL DO BRASIL deverá ser composto por, no mínimo, representantes das seguintes áreas:
         1. Gerência de tecnologia da informação;
         2. Gerência de segurança da informação;
         3. Gerência de recursos humanos;
         4. Gerência jurídica.
      2. Conforme a natureza do incidente, colaboradores de qualquer setor da SOLUS podem ser convocados a participar do time de resposta a incidentes de segurança da informação.
   3. **Disseminação de informação sobre incidentes de segurança da informação**
      1. Nenhum tipo de informação sobre incidentes e ocorrências de segurança da informação poderá ser divulgado para entidades ou pessoas externas a SOLUS METAL DO BRASIL sem aprovação expressa e formal da diretoria.
5. **Papéis e Responsabilidades**
   1. **GERÊNCIA DE SEGURANÇA DA INFORMAÇÃO**
      1. É responsabilidade da GERÊNCIA DE SEGURANÇA DA INFORMAÇÃO:
         1. Atuar como responsável por ocorrências e eventos de segurança e garantir a existência de recursos identificar, escalar, mitigar, conter, e erradicar incidentes de segurança, bem como ações efetivas para recuperar o estado anterior de ativos/serviços de informação ou recursos computacionais afetados pelo incidente;
         2. Comunicar prontamente o time de resposta a incidentes de segurança da informação da SOLUS sobre eventos e incidentes de segurança.
   2. **TIME DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO**
      1. É responsabilidade do TIME DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO:
         1. Apoiar a equipe de segurança da informação no tratamento de ocorrências e incidentes de segurança da informação, fornecendo orientação e direcionamento estratégico dentro da área de especialidade de cada um dos participantes do time de resposta a incidentes de segurança da informação;
         2. Aconselhar a diretoria da SOLUS METAL DO BRASIL sobre quais informações sobre eventos e incidentes de segurança da informação podem ser divulgadas para públicos internos e externos.
   3. **COMUNICAÇÃO**
      1. É responsabilidade da GERÊNCIA DE COMUNICAÇÃO:
         1. Aprovar qualquer tipo de comunicação ou disseminação total ou parcial de informações sobre ocorrências e incidentes de segurança da informação para qualquer parte ou público.
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-010** 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 27/01/2017

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