Resumo Política de Segurança da Informação

SUMÁRIO

OBJETIVO

- Apresentar de maneira resumida a Política de segurança de Informação da Credipar.

PÚBLICO-ALVO

Público em geral.

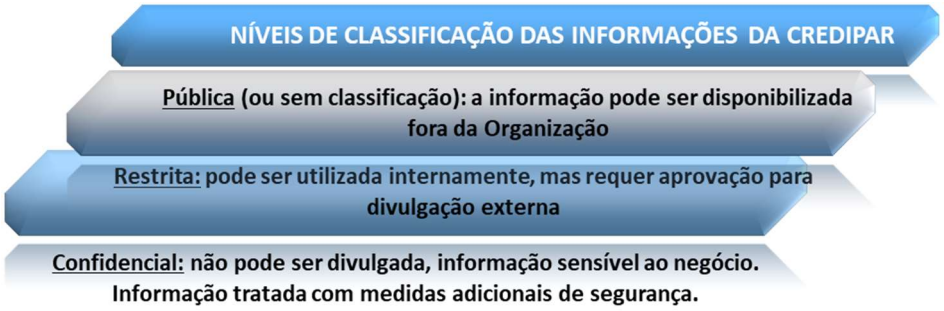
PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

Nosso compromisso com o tratamento adequado das informações com os nossos clientes e público em geral está fundamentado nos seguintes princípios:

a) **Confidencialidade**: garantir que a informação não estará disponível ou divulgada a indivíduos, entidades ou aplicativos sem autorização. Em outras palavras, é a garantia do resguardo das informações dadas pessoalmente em confiança e proteção contra a sua revelação não autorizada.
b) **Integridade**: garantir que a informação não tenha sido alterada em seu conteúdo e, portanto, é íntegra, autêntica, procedente e fidedigna. Uma informação íntegra é uma informação que não foi alterada de forma indevida ou não autorizada.
c) **Disponibilidade**: permite que a informação seja utilizada quando necessária, portanto, esteja ao alcance de seus usuários e destinatários e possa ser acessada no momento em que for necessário utilizá-lo.

CLASSIFICAÇÃO DA INFORMAÇÃO:

A informação é classificada de forma a indicar a prioridade e o nível esperado de proteção no tratamento de cada tipo de informação, conforme a classificação. A informação possui diferentes níveis de sensibilidade e criticidade. Determinadas informações poderão necessitar de um maior nível de proteção e tratativa



INCIDENTES DE SEGURANÇA DA INFORMAÇÃO:

Para efeito desta política, um incidente de segurança é definido como qualquer evento adverso, decorrente da ação de uma ameaça que explora uma ou mais vulnerabilidades, relacionado à segurança de um ativo que pode prejudicar quaisquer princípios da Segurança da Informação

DO GERENCIAMENTO DE SEGURANÇA CONTRA ATAQUES DIGITAIS

A TI da Credipar realiza o planejamento, controle, resposta e monitoramento dos mecanismos de proteção e segurança para prevenir, detectar e reduzir vulnerabilidades a ataques digitais à infraestrutura de TI que suporta os principais sistemas e dados de operação dos negócios da Credipar,

Os objetivos dos procedimentos de gerenciamento de segurança e proteção contra-ataques digitais são:

- Identificar e conhecer as principais vulnerabilidades que podem permitir que um atacante, ou seja, uma pessoa não autorizada, seja ela interna ou externa, acesse informações, dados ou sistemas de negócios da Credipar ou de seus clientes.
- Monitorar a eficácia dos processos e recursos de proteção contra os ataques digitais (Cyber Security), além de planejar e executar ações preventivas, sempre que necessário.
- Definir e executar ações corretivas de novas vulnerabilidades identificadas.
- Definir e executar ações de resposta a ataques digitais.

CRITÉRIOS BÁSICOS

- Os acessos às informações são realizados somente mediante autorização do responsável pela informação e são restritos a pessoas autorizadas.
- A organização tem controles para prevenir que vírus e outros tipos de softwares maliciosos entrem e se espalhem nos sistemas de informação por meio de arquivos e softwares não homologados cuja instalação e uso são proibidos.
- A organização conta com procedimentos específicos para garantir a recuperação de dados e informações quando necessário.
- A Credipar possui práticas em que apenas softwares e hardware homologados serão disponibilizados e podem ser usados pelos funcionários.
- A Credipar executa ações de resposta a ataques digitais.
- O Credipar conta com mecanismos para prevenção de ameaças de origem cibernética. Todo e qualquer incidente de segurança cibernética, passa por uma análise e é classificado de acordo com o impacto causado pelo incidente.
- A Credipar possui PCN (Plano de Continuidade de Negócios), identificando procedimentos e infraestrutura alternativa para proteger as pessoas, a reputação, os valores e os compromissos com os públicos relacionados.
- Caso um incidente de origem cibernética seja identificado pelo público geral, o mesmo deverá ser reportado pelo e-mail csirt@credipar.com.br.