BIM
Boletim Informativo Mensal
Comunicar para Educar
Agosto/2022 – Ano 3 – nº 31

Cuidados no Uso de Senhas

A senha é uma barreira para evitar que suas contas sejam invadidas por alguém não autorizado. Trate-a com cuidado e siga algumas recomendações importantes.

◈ Ao digitar uma senha, certifique-se de não estar sendo observado.

◈ Não deixe suas senhas escritas em local de fácil acesso. O conceito de “mesa limpa” é o melhor tratamento.

◈ Crie senhas fortes, elas são mais difíceis de serem quebradas por tentativas não autorizadas. Use caracteres especiais (Ex.: *, &, $, #).

◈ Ao criar uma senha, evite utilizar nome de pessoa, data de aniversário, número de telefone, placa de carro e algo óbvio do tipo “123senha”.

◈ Mantenha antivírus sempre atualizado.

◈ Não use a mesma senha para todos os serviços que acessa.

◈ Não compartilhe sua senha! Ela é de uso pessoal, intransferível e deve ser atualizada periodicamente.

◈ Ao acessar site que requeira senha, sempre feche a sessão utilizando a opção “sair” (*logout*).

Gestão de Continuidade de Negócios em Segurança da Informação

O processo de gestão de continuidade de negócios em segurança da informação deve ser baseado nas diretrizes institucionais sobre a continuidade do negócio do órgão ou da entidade como um todo, em especial quanto à continuidade das atividades críticas, e na avaliação dos riscos identificados previamente no processo de gestão de riscos.

A implementação desse processo tem o objetivo de minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades do órgão ou da entidade nessa área, além de recuperar em um nível aceitável perdas de ativos de informação, por intermédio de ações de resposta a incidentes e recuperação de desastres.

Esse processo deve ser composto por um plano de continuidade de negócios em segurança da informação, o qual observará o disposto no relatório de identificação, análise e avaliação de riscos de segurança da informação e a prioridade de recuperação dos processos de negócio.

O plano supracitado tem por objetivo definir como serão realizadas a gestão dos incidentes em caso de desastres ou de outras interrupções das operações de negócios e a maneira como deverão ser recuperadas as atividades nos prazos estabelecidos.

Para a implantação e a execução adequadas desse processo, é necessária a execução prévia dos processos de mapeamento de ativos de informação e de gestão de riscos de segurança da informação, pois fornecem elementos básicos essenciais.

Continua...

Finalmente, conforme consta na IN GSI/PR nº 3/2021, além desses processos mencionados, também são essenciais para a gestão de segurança da informação os processos de gestão de mudanças nos aspectos de segurança da informação e de avaliação de conformidade de segurança da informação, sobre os quais falaremos em futuras edições deste Boletim.

Principais Ações do Processo de Gestão de Continuidade de Negócios:

- designar um agente responsável pela gestão de continuidade de negócios;
- mapear as atividades críticas da organização;
- definir as estratégias de continuidade para essas atividades mapeadas;
- formalizar as diretrizes organizacionais sobre gestão de continuidade de negócios;
- elaborar um plano de continuidade de negócios;
- realizar testes de funcionamento desse plano; e
- avaliar e aprimorar o plano a partir dos resultados dos testes de funcionamento.

Transmissão de Informação Classificada por Meio do sei!

Você sabia que **não é permitido** tramitar documento classificado – Reservado, Secreto ou Ultrassecreto – pelo SEI (Sistema Eletrônico de Informações)?

É o que prevê o Decreto nº 7.845, de 14 de novembro de 2012, ao definir que a transmissão de informação classificada em grau de sigilo deve utilizar sistemas de informação e canais de comunicação seguros com diversos níveis de controle de acesso, bem como utilizar recursos criptográficos adequados aos graus de sigilo.

Sobre a utilização da criptografia, o decreto define que “a cifração e a decifração de informação classificada em qualquer grau de sigilo deverão utilizar recurso criptográfico baseado em algoritmo de Estado”, mas o SEI não possui esses recursos criptográficos.

Além disso, os níveis de acesso existentes no sistema (Sigiloso, Restrito e Público), apesar de permitirem a restrição do público que terá contato com determinado documento, não têm correlação com os graus de sigilo definidos na LAI (Lei de Acesso à Informação).

Portanto, você, **servidor do Poder Executivo federal**, que venha a produzir ou a receber algum documento classificado em qualquer grau de sigilo, não poderá, em nenhuma hipótese, incluir esse documento no SEI, e nem transmiti-lo pelo SEI, pois se assim o fizer incorrerá em quebra de segurança e estará sujeito às sanções previstas na LAI.

Para saber mais sobre esse assunto e sobre outros relacionados à segurança da informação, acesse: https://www.gov.br/gsi/pt-br/assuntos/dsi .

Fonte: https://www.gov.br/gsi/dsi/ https://www.gov.br/ctir
Editorial/redação/diagramação: AssESI Sugestões: asscom.dsi@presidencia.gov.br