BIM
Boletim Informativo Mensal
Comunicar para Educar
Setembro/2022 – Ano 3 – nº 32

A Importância de Manter os Sistemas e Dispositivos Atualizados

Atualmente, muitos dispositivos computacionais (*smartphones*, *tablets*, computadores, e *Smart* TVs, por exemplo) funcionam utilizando sistemas operacionais embarcados. Estes sistemas são responsáveis por executar um conjunto de tarefas específicas e predefinidas, que variam de acordo com a natureza e a finalidade dos aparelhos em que são instalados. Todavia, uma característica torna-se comum a todos eles: a necessidade de atualização.

Destacamos quatro motivos que fazem da atualização dos sistemas, uma boa prática:

A Correção de falhas: Os sistemas podem apresentar falhas em determinadas situações. Tais falhas, quando acontecem, facilitam o corrompimento de dados, o comportamento não desejado de aplicativos e até mesmo a interrupção da atividade do equipamento. Desenvolvedores estão sempre em busca de descobrir eventuais falhas e corrigi-las, para entregar atualizações aprimoradas e mais seguras. Mantenha os sistemas operacionais de seus dispositivos sempre atualizados para evitar panes e exposições.

O Aumento da performance: Outra vantagem das atualizações é proporcionar maior estabilidade e otimizar o tempo de execução e processamento das tarefas que um aparelho realiza.

A adição de novos recursos: É bastante frequente a inclusão de novas funcionalidades e ferramentas quando os sistemas operacionais são atualizados. Isto pode tornar a atividade dos usuários mais produtiva.

O aprimoramento da segurança: Algumas falhas podem permitir a execução de códigos, a elevação de privilégios nos sistemas e a interrupção de operações, dentre outras possibilidades. Essas vulnerabilidades podem ser exploradas por agentes maliciosos ou por grupos de ameaças avançadas persistentes, como os grupos de *Ransomwares*.

Aplicando as correções disponibilizadas pelos fabricantes nessas atualizações, o usuário diminui o risco de se tornar vítima de um ataque cibernético, uma vez que o equipamento estará mais seguro.

Como exemplo, cabe relembrar o ataque de *ransomware "WannaCry,"* de 2017. Se as empresas e demais usuários tivessem aplicado as atualizações disponíveis para o sistema operacional Windows, à época, provavelmente o ataque não teria sido tão eficaz e agressivo.

Portanto, manter os dispositivos computacionais atualizados significa mantê-los eficientes e mais protegidos.

BIM
Boletim Informativo Mensal
Comunicar para Educar
Setembro/2022 – Ano 3 – nº 32

Gestão de Mudanças nos Aspectos de Segurança da Informação (SI)

A implementação do processo de gestão de mudanças nos aspectos de SI tem por objetivo preparar e adaptar os órgãos e as entidades da administração pública federal para as transformações decorrentes da evolução de seu ambiente computacional, seja em processos ou em tecnologias da informação, visando à obtenção de modificações eficazes e eficientes e à mitigação de eventuais resistências.

Além de promover o planejamento e o controle das mudanças e a participação dos atores afetados por elas, esse processo deve considerar a análise crítica das consequências adversas inerentes às transformações e prever ações para amenizar seus efeitos.

Importante observar que ele deve ser respaldado pelas informações contidas no relatório de identificação, análise e avaliação de riscos de SI e no relatório de tratamento de riscos de SI - produtos da implementação do processo de gestão de riscos de SI, conforme escrevemos em edição anterior deste Boletim.

O processo de gestão de mudanças de SI deve ser constituído, no mínimo, pelos seguintes instrumentos:

- documento de descrição de mudança — visa identificar o tipo de alteração pretendida, de forma a adequar a organização às transformações no contexto interno e no externo; e
- documento de avaliação e aprovação de mudança — tem o objetivo de analisar as mudanças demandadas, recomendar quais alterações devem ser aprovadas e sugerir as alternativas para a implementação das modificações.

Finalmente, vale destacar que este é mais um dos importantes processos relacionados à gestão de SI nos órgãos e nas entidades da administração pública federal, conforme consta na IN GSI/PR nº 3/2021. Além dos já mencionados nesta edição do Boletim e em anteriores, essa norma define também o processo de avaliação de conformidade de SI, sobre o qual escreveremos em edição futura.

Qual a Diferença Entre Informação Classificada e Informação Sigilosa?

Você já sabe?! Muita gente confunde uma coisa com a outra!

Para acabar de vez com essa dúvida é bem simples!

Podemos dizer que a **informação classificada é um subconjunto do grande conjunto das informações sigilosas**. Ou seja: uma é parte da outra.

Segundo a LAI, a **informação** é considerada **sigilosa** quando submetida temporariamente à restrição de acesso público - em razão de sua importância para a segurança da sociedade e do Estado.

Já a informação sigilosa que precisar de um nível maior de proteção, deverá ser **classificada** - de acordo com o seu grau de sensibilidade - como **reservada**, **secreta** ou **ultrassecreta,** tratada apenas por pessoas devidamente credenciadas, e armazenada em local que atenda aos requisitos mínimos de segurança.

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