BIM
Boletim Informativo Mensal
Comunicar para Educar
Junho/2022 – Ano 3 – nº 29

Acordos Internacionais de Troca de Informação Classificada

Você sabia que a melhor maneira para trocar informação classificada com outros países ou organismos internacionais é um acordo de troca e proteção mútua da informação classificada? É o que está previsto na Lei de Acesso à Informação (LAI) e no Decreto nº 7.845, de 14 de novembro de 2012.

Tal acordo é conhecido como "acordo guarda-chuva", pois debaixo dele todos os outros atos internacionais que incluam troca de informação classificada, sejam eles tratados, acordos, memorandos de entendimento ou ajustes técnicos, podem ocorrer sem risco de quebra de segurança da informação.

Geralmente, estes acordos visam padronizar procedimentos e nomenclaturas que serão utilizados durante todo o processo. São estabelecidas as equivalências entre os graus de sigilo do Brasil e os do outro país, e como a informação classificada será tratada por ambas as partes.

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

Atenção Alta Administração, Assessorias e Chefias!!

Gestão de Riscos de Segurança da Informação

A **gestão de riscos de segurança da informação** é um processo de natureza permanente, estabelecido, direcionado e monitorado pela **alta administração**, que contempla as atividades de identificação, avaliação e gerenciamento de eventos que tenham o potencial de afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos.

Destaca-se que este processo de gestão tem por **objetivo** direcionar e controlar o risco de segurança da informação, a fim de adequá-lo aos níveis aceitáveis para o órgão ou entidade. E ele deve estar alinhado com o modelo de gestão de riscos institucional e ser compatível com a missão e os objetivos estratégicos do órgão ou da entidade.

É necessário ter em mente que ele fornece elementos básicos para a implantação e a execução adequadas do **processo de continuidade de negócios em segurança** da informação, que consta da IN GSI/PR nº 3/2021 e sobre o qual falaremos em futura edição deste Boletim. Fique atento!

Relembre conceitos importantes para o tema, de acordo com o Glossário de Segurança da Informação, Portaria GSI/PR Nº 93, de 18 de outubro de 2021.

- **ATIVOS DE INFORMAÇÃO** - meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização;
- **VULNERABILIDADE** - condição que, quando explorada por um criminoso cibernético, pode resultar em uma violação de segurança cibernética dos sistemas computacionais ou redes de computadores, e consiste na interseção de três fatores: suscetibilidade ou falha do sistema, acesso possível à falha e capacidade de explorar essa falha;
- **AMEAÇA** - conjunto de fatores externos com o potencial de causar dano para um sistema ou organização

BIM
Boletim Informativo Mensal
Comunicar para Educar
Junho/2022 – Ano 3 – nº 29

Cópias de Segurança – *Backup*

Backup é um termo em inglês que significa " cópia de segurança". Trata-se de uma cópia dos arquivos importantes de um aparelho, como celulares, *notebooks* ou computadores, para um outro dispositivo ou ambiente, como um serviço em nuvem, um HD externo ou um pen drive.

Segundo o Glossário de Segurança da Informação (Portaria GSI/PR Nº 93, de 18 de outubro de 2021), *backup* é conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Tem a fidelidade ao original assegurada.

Os dados ou informações armazenadas em um dispositivo computacional, estão sujeitos a perdas por diversas causas:

- exclusão acidental ou intencional;
- falha de armazenamento ;
- falha do sistema computacional;
- falha de equipamento;
- sinistro; e
- ataque de códigos maliciosos que façam a criptografia e/ou a exclusão dos dados originais.

Por estes motivos, é prudente realizar e manter pelo menos uma cópia de seus arquivos mais importantes em um ambiente seguro e separado do ambiente original.

Para realizar um *backup* você pode utilizar programas já integrados aos sistemas operacionais, aplicativos especializados em *backup*, repositórios externos (*google drive, one drive*) ou até mesmo cópias em mídias (*pen drives*, CDs, HDs externos).

Se você optar por serviço de *backup* em nuvem, onde os seus dados são salvos em um servidor remoto, é importante observar os seguintes aspectos:

- ✓ o custo do serviço (armazenamento);
- ✓ se o serviço oferece autenticação em duas etapas (segurança); e
- ✓ se o serviço oferece suporte ao aplicativo ou arquivos que se queira resguardar.

Se você escolher por *backup* armazenado localmente, ou seja, em alguma mídia física, é importante observar os tópicos abaixo:

- ✓ o tamanho dos arquivos x tamanho da mídia (capacidade de armazenamento);
- ✓ o local onde essa mídia será guardada (durabilidade e segurança); e
- ✓ se possível, realizar a criptografia dos dados armazenados.

Programe seus *backups* para serem executados de forma automática em horários específicos.

Confira regularmente se os seus *backups* estão sendo feitos e armazenados no local seguro.

O Gabinete de Segurança Institucional, por meio do Departamento de Segurança da Informação (DSI/GSI/PR), publicou uma instrução normativa de cumprimento **obrigatório** aos órgãos e entidades da administração pública federal, que dispõe sobre os requisitos mínimos de segurança da informação para a utilização de soluções de computação em nuvem, IN nº 05, de 30/08/2021.

Acesse no sítio eletrônico: https://in.gov.br/en/web/dou/-/instrucao-normativa-n-5-de-30-de-agosto-de-2021-341649684

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