Comunicar para Educar
Fevereiro/2023 - Ano 4 - nº 36

BIM

Boletim Informativo Mensal

O DSI, agora, se chama Departamento de Segurança da Informação e Cibernética

Com a entrada em vigor, em 24 de janeiro deste ano, do Decreto nº 11.331, de 1º de janeiro de 2023, o Departamento de Segurança da Informação passou a se chamar Departamento de Segurança da Informação e Cibernética. Ele agora integra a nova Secretaria de Segurança da Informação e Cibernética do Gabinete de Segurança Institucional da Presidência da República.

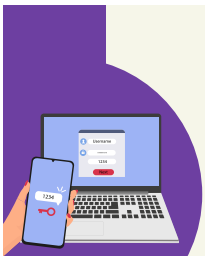
Vamos falar de autenticação de 2 fatores?

Você está familiarizado com a autenticação de dois fatores (2FA)?

Caso responda sim, tem certeza que está completamente seguro?
E caso a resposta seja não, já passou da hora de conhecer essa tecnologia.

O que é autenticação de dois fatores ou 2FA?

Originária do termo em inglês "*two-factor authentication*", a 2FA, ou autenticação de dois fatores, é um recurso de segurança oferecido pelos prestadores de serviços *on-line* em que é exigido que o usuário forneça duas formas de autenticação no processo de *login* de sua conta.



Como funciona?

Ao acessar uma conta, será solicitado o primeiro fator de autenticação: nome de usuário e senha. Em seguida, você irá informar o segundo fator disponibilizado pelo prestador do serviço *on-line*, que pode ser o número variável de um *token*, um código de acesso único enviado por *e-mail*, ou uma mensagem de texto com o código de verificação enviada ao seu número de telefone ou ao seu dispositivo móvel pessoal cadastrado, sempre disponibilizado em um meio ao qual apenas você possui acesso. Somente após a entrega desses dois itens, seu acesso ao serviço será liberado.

Quem disponibiliza a autenticação de dois fatores?

Atualmente, a maioria dos serviços comerciais *on-line*, redes sociais e aplicações bancárias e de governo, como o sou.gov, tem a possibilidade de autenticação de dois fatores. No caso do aplicativo MEU GOV.BR no celular, é necessário ativar a autenticação de dois fatores para a sua utilização.

Empregar a autenticação de dois fatores é muito importante e, apesar de não ser 100% à prova de falhas, evita muitos golpes, invasões de conta e fraudes na internet. Ainda assim, não podemos afirmar que estamos totalmente seguros. Para mitigar possíveis brechas e aumentar a resiliência cibernética, é recomendado que:

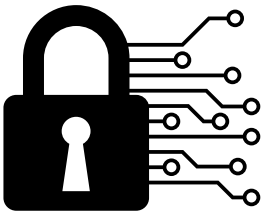
- sempre que possível, utilize um fator biométrico como autenticação; e
- nunca compartilhe com outras pessoas os códigos recebidos, seja por SMS ou por meio de um de seus *softwares* geradores de códigos aleatórios.

Memorando de Entendimento

O Gabinete de Segurança Institucional e o Ministério das Relações Exteriores, *Commonwealth* e Desenvolvimento (*Foreign*, *Commonwealth & Development Office* – FCDO) do Reino Unido celebraram em 21 de novembro de 2022, o Memorando de Entendimento sobre cooperação na área de Segurança Cibernética.

O Memorando de Entendimento é um importante instrumento na relação entre países, pois, por meio dele, podem ser definidos mecanismos que possibilitam uma cooperação mais efetiva entre os participantes.

Com isso, os dois países pretendem facilitar a cooperação, trocando informações sobre incidentes cibernéticos e compartilhando as melhores práticas de segurança, de modo a promoverem interesses mútuos e um espaço cibernético mais seguro e resiliente para as instituições de Estado e para suas populações.



Acesso à informação

O acesso à informação está consolidado como direito fundamental para todo cidadão brasileiro, com sua previsão descrita no inciso XXXIII, do art. 5º da Constituição Federal de 1988 (CF/88), o qual fala:

Todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado.

Garantido desde 1988 pela Constituição, o direito do cidadão de ter acesso à informação foi regulamentado, em 2011, pela Lei de Acesso à Informação – LAI (Lei nº 12.527/2011), que tem como preceito geral a máxima divulgação, porém nem toda informação é de acesso público.

A LAI prevê restrição de acesso ao público em geral para alguns tipos de informações. Segundo a Lei, informações pessoais, informações sigilosas protegidas por lei específica e informações classificadas em grau de sigilo não podem ser tornadas públicas.

Terá acesso a esse tipo de informação quem necessitar delas para executar seu trabalho. Podemos citar, como exemplo, o encarregado de pessoal de determinado órgão que precisa acessar os dados pessoais de funcionários para processar o pagamento do mês; ou o funcionário de determinado tribunal que lida com processos em segredo de justiça; ou ainda um gerente de banco que tem acesso aos dados financeiros de seu cliente.

A exceção, à regra mencionada acima, é o acesso à informação classificada em grau de sigilo (reservada, secreta e ultrassecreta). Além da necessidade de conhecer esse tipo de informação para executar o seu trabalho, o indivíduo deverá possuir uma credencial de segurança que o permita acessar esse tipo de informação.

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

Recomendações

- O nosso site foi reformulado e encontra-se disponível em: https://www.gov.br/gsi/dsic. nele encontramos notícias, todas as edições deste Boletim, as Orientações de Segurança da Informação e Cibernética (OSIC), informações institucionais, portarias, instruções normativas, normas complementares e resoluções elaboradas por este Departamento, além de legislação correlata e de outros documentos importantes como o Plano de Gestão de Incidentes Cibernéticos e a Cartilha de Gestão de Segurança da Informação, publicados recentemente.

- Recomendamos que a Cartilha de Gestão de Segurança da Informação seja lida integralmente pelos gestores de segurança da informação dos órgãos e das entidades e demais servidores que executam atividades de segurança da informação e cibernética, pois serve de guia para a execução dos processos de segurança da informação e apresenta a legislação aplicável.

- No nosso *site*, encontramos também o *link* para o *site* específico do CTIR Gov – Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, de responsabilidade nacional, para a proteção cibernética, mantido por este departamento (https://www.gov.br/ctir/pt-br). Lá, estão publicados, em sua página principal, os Alertas e as Recomendações elaboradas pelo Centro, além de notícias de outras informações importantes.

- Recomendamos fortemente às equipes de prevenção, tratamento e resposta a incidentes cibernéticos (ETIRs) dos órgãos e das entidades que consultem, diariamente, os Alertas e as Recomendações do CTIR Gov e que façam a comunicação de incidentes de segurança em seus ativos, seguindo o procedimento que consta no menu “Comunicação de Incidentes de Rede” do *site*.

- O DSIC é o órgão do Governo Federal responsável por elaborar normativos e requisitos metodológicos relativos à atividade nacional de segurança da informação, no âmbito da administração pública federal, incluídos a segurança cibernética, a gestão de incidentes cibernéticos, a proteção de dados, o credenciamento de segurança e o tratamento de informações sigilosas. Estão vigentes atualmente nove instruções normativas e nove normas complementares do DSIC/GSI/PR sobre segurança da informação e cibernética, sendo que algumas delas estão em revisão, o que reforça a importância de consultar com frequência a nossa página de legislação.

- O cumprimento das normas do DSIC/GSI é obrigatório para toda a administração pública federal, conforme dispõe o Decreto nº 9.637, de 26 de dezembro de 2018, art. 17, VI.

- Zelar pela segurança da informação e cibernética é um dever de todos. Acompanhem nosso site e procurem conhecer mais sobre o tema.

Fonte: https://www.gov.br/gsi/dsi/
Editorial/redação/diagramação: SSIC Sugestões: educa.si@presidencia.gov.br