BIM
Boletim Informativo Mensal
Comunicar para Educar
Março/2022 – Ano 3 – nº 26

QR Code

QR Code (*Quick Response Code*) é um código de resposta rápida, bidimensional, com símbolos horizontais e verticais, que pode ser decodificado, ou seja, lido pelas câmeras dos celulares.

Após a leitura, é possível realizar ações como: abrir uma página da *web*, baixar um arquivo, adicionar um contato, conectar-se a uma rede de *wi-fi*, efetuar pagamentos etc.

A tecnologia do *QR Code* não é recente, porém sua utilização cresceu muito nos últimos anos, devido a sua praticidade. Com isso, os golpistas, cada vez mais audaciosos e criativos, começaram a fazer uso dessa tecnologia para fins maliciosos.

Exemplos de golpes com a utilização do *QR Code*:

- ***phishing* (pescaria):**

O golpista envia campanhas, normalmente por *e-mail*, *SMS* ou anúncio com conteúdo bem estruturado e coerente, disponibilizando um *QR Code* que leva a vítima a um *site* falso. Nesse site são solicitados e "pescados" os dados pessoais da vítima, senhas de acessos e demais informações sensíveis que podem ser utilizadas para roubo, compras, empréstimos, entre outras.

- **com o Pix:**

O criminoso falsifica faturas de empresas, incluindo *QR Code* falso. E em alguns casos, a fatura falsa traz um código de barras e um *QR Code* e, ao realizar o pagamento por meio do aplicativo bancário, o cliente envia o dinheiro para a conta do golpista.

Como se prevenir?

1. Evite clicar em *pop-ups* e janelas. Para sair do anúncio, não clique em ícone escrito "Fechar", sempre use o pequeno símbolo "X" no canto.
2. Confirme os dados do destinatário antes de concluir pagamento via Pix. Apenas pagamento legítimo mostrará o nome correto da pessoa física ou da empresa (razão social).
3. Verifique se o endereço da página onde fará a compra começa com H**TT**PS e procure o ícone de cadeado 🔒 próximo ao endereço.
4. Se o uso do *QR Code* não for frequente, desative a opção de realizar leitura automática. Ative-a somente quando necessitar, nas configurações da câmera do seu celular ou no aplicativo baixado para esse fim.
5. Utilize um antivírus e o mantenha atualizado em todos os seus dispositivos.

Credenciamento de Segurança de Pessoas Naturais

O credenciamento de segurança de pessoa natural será concedido nos casos em que houver a necessidade de conhecer determinada informação classificada, em qualquer grau de sigilo (reservado, secreto e ultrassecreto). Releva mencionar que esta credencial estará associada **somente à informação classificada a qual a pessoa natural tenha a necessidade de conhecer.**

O processo de credenciamento de pessoas naturais segue as seguintes fases:

FASE DE INDICAÇÃO → **FASE DE INVESTIGAÇÃO DE SEGURANÇA** → **FASE DO CREDENCIAMENTO**

De maneira resumida, o processo se inicia a partir da solicitação formal ao Gestor de Segurança e Credenciamento do órgão de registro da autoridade solicitante, por qualquer autoridade referida no Art. 9º da IN GSI/PR nº 02/2013 ou § 2º do Art 30 do Dec. 7724/2012. Então, realiza-se o preenchimento do Formulário Individual de Dados para Credenciamento – FIDC. A investigação passa pela apreciação do órgão de registro com o qual o solicitante mantenha vínculo de qualquer natureza. Cumpridos os requisitos, a pessoa natural poderá receber credencial de segurança, que terá validade de, no máximo, dois anos.

Para saber mais sobre esse assunto acesse link:
https://www.gov.br/defesa/pt-br/arquivos/cartografia/divcar/2020/04nc01_in02_gsi_normacomplementar_27_06_2013.pdf

BIM
Boletim Informativo Mensal
Comunicar para Educar
Março/2022 – Ano 3 – nº 26

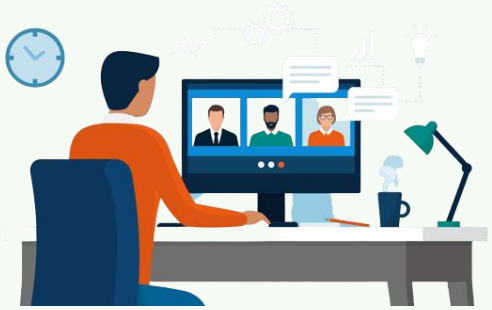
Gestão de Segurança da Informação na Administração Pública Federal

A crescente digitalização mundial acelerada pela pandemia de COVID-19 fez com que o trabalho remoto se tornasse uma realidade cada vez mais frequente na administração pública federal. Consequentemente, para fazer frente ao aumento dos riscos e dos incidentes associados a essa forma de trabalho, torna-se ainda mais importante que os órgãos e as entidades mantenham atualizadas a política de segurança da informação e as respectivas normas internas. É essencial também atribuir alta prioridade à destinação de recursos orçamentários para ações de conscientização e de capacitação de sua força de trabalho em temas relacionados à segurança da informação.

Com isso, deve-se atentar que a Política Nacional de Segurança da Informação (PNSI), instituída pelo Decreto nº 9.637, de 2018, lista como obrigação da alta administração "... observar as normas que estabelecem requisitos e procedimentos para a segurança da informação publicadas pelo [GSI/PR]". Todas essas normas estão disponíveis no site do Departamento de Segurança da Informação e podem ser acessadas por meio do link: https://www.gov.br/gsi/pt-br/assuntos/dsi/legislacao.

Vale destacar que essas normas são de cumprimento obrigatório para a administração pública federal, ratificado pelo Tribunal de Contas da União no item 9.8.2 do Acórdão nº 1233/2012 – TCU – Plenário: "... a implantação dos controles gerais de segurança da informação positivados nas normas do GSI/PR não é faculdade, mas obrigação da alta administração, e sua não implantação sem justificativa é passível [de] sanção ...".

Conforme a PNSI, a **alta administração deve** "incorporar padrões elevados de conduta para a garantia da segurança da informação" e "observar as normas e os procedimentos específicos aplicáveis, implementar e manter mecanismos, instâncias e práticas de governança". Assim, recomenda-se que os órgãos e as entidades assegurem em seu âmbito a adoção, entre outras, das seguintes práticas básicas:



1. **controle de acesso**: que inclui o credenciamento de usuário e a criação de senha segura ou outro método de acesso seguro a ativos de informação usados pela Administração;

- esse controle deve ser feito sempre, independentemente de quem seja o proprietário ou mantenedor desses ativos e do local físico onde estejam;
- é de alto risco a prática de compartilhar senha ou meio de acesso entre usuários, seja no exercício da função de administrador, mantenedor, desenvolvedor ou qualquer outra; e
- recomenda-se que norma interna considere como falta gravíssima e preveja sanção para o compartilhamento de senha ou meio de acesso a perfil com privilégio de administrador, mantenedor ou desenvolvedor, bem como a serviço digital essencial, a sistema estruturante, a informação classificada ou a dado pessoal.

2. **manutenção de *backup***: de dados e programas computacionais, com periodicidade, tempo de retenção e técnicas de segregação adequados à criticidade do serviço prestado e à classificação das informações e dos dados tratados, em conformidade com os processos de gestão de riscos e de gestão de continuidade de negócios do órgão ou da entidade, cuja realização é obrigatória.

Por fim, ressaltamos a necessidade de que todos tenham conhecimento dessas e de outras regras básicas de segurança da informação e da importância de cumpri-las.

Fonte: https://www.gov.br/gsi/dsi/ https://www.gov.br/ctir

Editorial/redação/diagramação: AssESI Sugestões: asscom.dsi@presidencia.gov.br