



PORTARIA Nº 139, DE 26 DE JUNHO DE 2023.

Estabelece diretrizes de segurança da informação para o uso seguro de computação em nuvem no Conselho Federal de Química.

O PRESIDENTE DO CONSELHO FEDERAL DE QUÍMICA (CFQ), no uso de suas atribuições conferidas pelo art. 8º da Lei nº 2.800, de 18 de junho de 1956;

Considerando a Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto no inciso XXXIII do art. 5º; e no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal;

Considerando a Lei nº 13.709, de 14 de agosto de 2018, que cria a Lei Geral de Proteção de Dados Pessoais;

Considerando a Instrução Normativa nº 01, de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

Considerando a Instrução Normativa nº 05, de 30 de agosto de 2021, do Gabinete de Segurança Institucional da Presidência da República, que dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal;

Considerando a Portaria nº 93, de 18 de outubro de 2021, do Gabinete de Segurança Institucional da Presidência da República, que aprova o glossário de segurança da informação;

Considerando a Portaria nº 182, de 6 de outubro de 2022, que dispõe sobre a institucionalização da Política de Segurança da Informação (POSIN) no âmbito do Conselho Federal de Química (CFQ);

Resolve:

Art. 1º Instituir os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelo Conselho Federal de Química.

CAPÍTULO I

DAS DISPOSIÇÕES INICIAIS

Seção I

Do Objeto e Âmbito de Aplicação

Art. 2º Esta Portaria dispõe sobre medidas técnicas e administrativas para utilização segura de soluções de computação em nuvem no âmbito do Conselho Federal de Química.

Art. 3º As medidas técnicas e administrativas têm como objetivo proteger as informações de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito e considerar a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, assim como os princípios previstos em Lei.

Art. 4º Fica autorizada a utilização e a migração de soluções de TIC para ambiente de computação em nuvem pelo CFQ.

Art. 5º A contratação de soluções de computação em nuvem busca garantir benefícios de capacidade, segurança e eficiência em tecnologia para o CFQ.

Seção II

Dos Objetivos



Art. 6º O objetivo desta Portaria é definir as diretrizes em relação à computação em nuvem, que são aplicáveis ao CFQ, para garantir a eficiência, o nível de segurança da informação, privacidade e proteção aos dados pessoais determinados pela Lei 13.709, de 14 de agosto de 2018 e pelas Instruções Normativas N° 01/2020 e 05/2021 emitidas pelo Gabinete de Segurança Institucional da Presidência da República.

§ 1º Deverão ser observados os requisitos constantes do capítulo II para que o CFQ adote soluções de computação em nuvem de forma segura, com o objetivo de elevar o nível de proteção das informações no uso dessa tecnologia.

§ 2º Esta norma atende ao disposto na Política de Segurança da Informação do CFQ e nas Instruções Normativas citadas no caput do artigo e define as medidas técnicas e administrativas que deverão ser observadas pelos integrantes da Governança, colaboradores, estagiários e prestadores de serviços, especialmente os fornecedores de computação em nuvem.

Seção III

Das Definições

Art. 7º Para efeitos desta Norma será considerado o Glossário de Segurança da Informação como conceitos básicos, estabelecido no Anexo Único desta Portaria.

I - *Cloud Broker*: indivíduo ou organização que oferece consultoria, medeia e facilita a seleção de soluções de computação em nuvem em nome de uma organização. Um cloud broker serve como um terceiro entre um provedor de serviço de nuvem (PSN) e uma organização que contrata serviços de computação em nuvem. Para as infraestruturas de multinuvm, o cloud broker proporciona uma visão mais centralizada de todos os fornecedores e soluções, o que auxilia no gerenciamento dos recursos disponíveis e também dos custos. Em geral, consideram-se quatro tipos de cloud broker:

- a) serviços de agregação, que garantem a interoperabilidade entre diversos provedores de serviço de nuvem, por meio da agregação de todos os serviços contratados em uma única interface;
- b) serviços de integração, que adicionam valor automatizando fluxos de trabalho em ambientes híbridos, por meio de uma única orquestração, para melhorar o desempenho e reduzir o risco de negócios;
- c) serviços de personalização (ou customização), que modificam os serviços de nuvem existentes, a fim de atender às necessidades dos negócios da contratante, podendo inclusive desenvolver recursos adicionais para executar corretamente os serviços desejados;
- d) serviços de arbitragem, fornecendo flexibilidade ao contratante por intermédio da oferta de vários serviços semelhantes para avaliação e seleção.

II - Computação em nuvem: modelo de fornecimento e entrega de tecnologia de informação que permite acesso conveniente e sob demanda a um conjunto de recursos computacionais configuráveis, sendo que tais recursos podem ser provisionados e liberados com mínimo gerenciamento ou interação com o provedor do serviço de nuvem (PSN) e é composta pelos:

III - modelos de implantação:

a) Nuvem privada (ou interna) - infraestrutura de nuvem dedicada para uso exclusivo do órgão e de suas unidades vinculadas, ou de entidade composta por múltiplos usuários, e sua propriedade e seu gerenciamento podem ser da própria organização, de terceiros ou de ambos.

b) Nuvem comunitária - infraestrutura de nuvem dedicada para uso exclusivo de uma comunidade, ou de um grupo de usuários de órgãos ou de entidades não vinculados, que compartilham a mesma natureza de trabalho e obrigações, e sua propriedade e seu gerenciamento podem ser de organizações da comunidade, de terceiros ou de ambos.



c) Nuvem pública (ou externa) - infraestrutura de nuvem dedicada para uso aberto de qualquer organização, e sua propriedade e seu gerenciamento podem ser de organizações públicas, privadas ou de ambas.

d) Nuvem híbrida - infraestrutura de nuvem composta por duas ou mais infraestruturas distintas (privadas, comunitárias ou públicas), que permanecem com suas próprias características, mas agrupadas por tecnologia padrão que permite interoperabilidade e portabilidade de dados, serviços e aplicações.

IV - tipos de serviço:

a) *Infraestrutura as a Service (IaaS):* tipo de serviço de computação em nuvem em que o provedor de serviço de nuvem oferece ao cliente a capacidade de criar redes virtuais em seu ambiente de computação, permitindo-lhe selecionar os sistemas operacionais a serem instalados em máquinas virtuais, bem como a estrutura da rede, incluindo o uso de switches virtuais, roteadores e *firewalls*. O IaaS também fornece total liberdade quanto ao software ou código personalizado executado nas máquinas virtuais.

b) *Plataforma as a Service (PaaS):* tipo de serviço de computação em nuvem, em que o provedor de serviço de nuvem oferece ao cliente a capacidade de operar códigos ou aplicativos personalizados, determinando previamente quais sistemas operacionais ou ambientes de execução são oferecidos, não sendo permitido ao cliente modificar os sistemas operacionais (mesmo patches de segurança) ou alterar o espaço da rede virtual.

c) *Software as a Service (SaaS):* tipo de serviço de computação em nuvem em que o provedor de serviço de nuvem oferece ao cliente a capacidade de usar um aplicativo fornecido, cabendo ao usuário tão somente usar o aplicativo oferecido e fazer pequenos ajustes de configuração e ao provedor a responsabilidade pela manutenção da aplicação.

V - Medida administrativa: controle organizacional, físico ou procedimental, obtido por processo que possibilite a conformidade legal e normativa e a confidencialidade, disponibilidade e integridade dos dados pessoais;

VI - Medida técnica: controle relacionado à segurança cibernética, obtido por processo que possibilite a conformidade legal e normativa e a confidencialidade, disponibilidade e integridade dos dados pessoais.

VII - Sistema estruturante: sistema com suporte de TIC fundamental e imprescindível para o planejamento, coordenação, execução, descentralização, delegação de competência, controle ou auditoria das ações de Estado, além de outras atividades auxiliares, desde que comum a dois ou mais órgãos ou entidades da Administração Pública Federal, direta ou indireta, e que necessitem de coordenação central.

CAPÍTULO II

DOS REQUISITOS PARA A ADOÇÃO DE COMPUTAÇÃO EM NUVEM

Art. 8º Deverão ser observados os requisitos mínimos dessas diretrizes para que o CFQ adote soluções de computação em nuvem de forma segura, com o objetivo de elevar o nível de proteção das informações no uso dessa tecnologia.

Seção I

Da Transferência de Serviços para um Provedor de Serviço de Nuvem

Art. 9º Antes de transferir serviços e/ou informações para um provedor de serviço de nuvem, a equipe responsável deverá, no mínimo:



I - verificar se estão alinhadas à legislação brasileira e aos direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas, especialmente, Lei 12.527/2011 - Lei de Acesso à Informação, Lei 12.965/2014 - Marco Civil da Internet, Lei 13.709/2018 - LGPD, Decreto 9.637/2018 e Instruções Normativas N° 01/2020 e N° 05/2021 emitidas pelo Gabinete de Segurança Institucional, e dos registros as seguintes operações:

a) de coleta, armazenamento, guarda e tratamento de registros de dados pessoais; e
b) de comunicações realizadas por provedores de conexão e de aplicações de internet, em que pelo menos um desses atos ocorra em território nacional;

II - realizar o gerenciamento de riscos, precedido por análise e relatório de impacto de dados pessoais, em conformidade com a legislação, dos seguintes itens:

a) o tipo de informação a ser migrada;
b) o fluxo de tratamento dos dados que podem ser afetados com a adoção da solução;
c) o valor dos ativos envolvidos; e
d) os benefícios da adoção de uma solução de computação em nuvem, em relação aos riscos de segurança e privacidade referentes à disponibilização de informações e serviços a um terceiro.

III - definir o modelo de serviço e de implementação de computação em nuvem que será adotado;

IV - utilizar, para os sistemas estruturantes, somente os modelos de implementação de nuvem privada ou de nuvem comunitária, desde que restritas às infraestruturas de órgãos ou de entidades;

V - avaliar quais informações serão hospedadas na nuvem, considerando:

a) o processo de classificação da informação de acordo com a legislação;
b) o valor do ativo de informação;
c) os controles de acessos físico e lógico relativos à segurança da informação; e
d) o modelo de serviço e de implementação de computação em nuvem.

VI - definir as medidas de mitigação de riscos e de custos para a implementação de solução de computação em nuvem e para possibilidade de crescimento dessa solução;

VII - planejar custos de migração das informações e dos serviços, nos casos de ingresso e de saída do serviço de computação em nuvem.

Seção II

Da Capacidade do Provedor de Serviço de Nuvem para Implementar Atualizações

Art. 10. Em função da capacidade de o provedor de serviço de nuvem implementar atualizações relacionadas à segurança da informação em seus produtos e serviços, o CFQ deverá, no mínimo:

I. definir os critérios e a periodicidade das atualizações dos procedimentos e dos recursos computacionais a serem observados pelo provedor de serviço de nuvem; e

II. revisar e atualizar periodicamente seus processos internos de gestão de riscos de segurança da informação.

Seção III

Do Gerenciamento de Identidades e de Registros (Logs)

Art. 11. Em relação ao gerenciamento de identidades e de registros, o CFQ deverá, no mínimo:

I - adotar um padrão de identidade federada para permitir, sempre que possível, o uso de tecnologia *single sign-on* no processo de autenticação de seus usuários no provedor de serviço de nuvem;



II - negar ao provedor de serviço de nuvem permissão de uso e acesso direto ao ambiente de autenticação do órgão ou da entidade;

III - adotar, de acordo com o nível de criticidade da informação, o uso da tecnologia *single sign-on*, o qual deve ser acompanhado:

a) de autenticação multifator; ou

b) de outra alternativa que aumente o grau de segurança no processo de autenticação de seus usuários no provedor de serviço de nuvem.

IV - exigir do provedor de serviço de nuvem que:

a) registre todos os acessos, incidentes e eventos cibernéticos, incluídas informações sobre sessões e transações; e

b) armazene, pelo período de um ano, todos os registros de que trata a alínea “a”.

V - armazenar os registros de todos os acessos, incidentes e eventos cibernéticos, incluindo informação sobre sessões e transações, por cinco anos, no ambiente do provedor de serviço de nuvem ou em ambiente próprio controlado, à critério do CFQ;

VI - manter, em ambiente próprio controlado, pelo período de cinco anos, os registros de todos os acessos, incidentes e eventos cibernéticos, incluindo informação sobre sessões e transações recebidos do provedor de serviço de nuvem; e

VII - capacitar a equipe de segurança para acessar e utilizar os registros gerados pelo provedor de serviço de nuvem.

Seção IV

Do Uso de Recursos Criptográficos

Art. 12. Em relação à necessidade do uso de recursos criptográficos, o CFQ deverá, no mínimo:

I. verificar se os dados da organização estão sendo tratados e armazenados de acordo com a legislação;

II. analisar a necessidade de criptografar dados com base nos requisitos legais, nos riscos, no nível de criticidade, nos custos e nos benefícios; e

III. utilizar, sempre que possível, chaves de encriptação baseadas em hardware.

Parágrafo único. As análises poderão ser realizadas pelo setor que utilizar o serviço podendo consultar os setores de Tecnologia da Informação (GTIC) e Assessoria Jurídica (AJUR), quando necessário.

Seção V

Da Segregação de Dados e Da Separação Lógica

Art. 13. Em relação à segregação de dados e à separação lógica em ambientes de computação em nuvem, o CFQ, em conjunto com o provedor de serviço de nuvem, deverá estabelecer, no mínimo, as seguintes ações:

I - garantir que o ambiente contratado seja protegido de usuários externos do serviço em nuvem e de pessoas não autorizadas e implementar controles de segurança da informação de forma a propiciar o isolamento adequado dos recursos utilizados pelo CFQ;

II - garantir que seja aplicada segregação lógica apropriada dos dados das aplicações virtualizadas, dos sistemas operacionais, do armazenamento e da rede a fim de estabelecer a separação de recursos utilizados;

III - garantir a separação de todos os recursos utilizados pelo Provedor de Serviço de Nuvem daqueles recursos utilizados pela administração interna do CFQ; e



IV - avaliar os riscos associados à execução de softwares proprietários a serem instalados no serviço de nuvem.

Seção VI

Do Gerenciamento da Nuvem

Art. 14. Em relação ao gerenciamento da nuvem, o CFQ deverá, no mínimo:

- I - capacitar a equipe responsável por esse gerenciamento nas tecnologias utilizadas pelo provedor de serviço de nuvem;
- II - exigir que o provedor de serviço de nuvem documente e comunique seus recursos, papéis e responsabilidades de segurança da informação para o uso de seus serviços em nuvem;
- III - elaborar uma matriz de responsabilidades que inclua obrigações e responsabilidades próprias; e
- IV - elaborar um processo de tratamento de incidentes junto ao provedor de serviço de nuvem e comunicá-lo à equipe responsável pelo gerenciamento da nuvem.

Seção VII

Do Tratamento da Informação

Art. 15. Em relação ao tratamento da informação em ambiente de computação em nuvem, o CFQ, além de cumprir as orientações contidas na legislação sobre proteção de dados pessoais, deve observar as seguintes diretrizes:

- I - informação sem restrição de acesso poderá ser tratada em ambiente de nuvem, considerada a legislação e os riscos de segurança da informação;
- II - informação classificada em grau de sigilo e documento preparatório que possa originar informação classificada não poderão ser tratados em ambiente de computação em nuvem; e
- III - poderão ser tratados em ambiente de computação em nuvem, observados os riscos de segurança da informação e a legislação vigente:
 - a) a informação com restrição de acesso prevista na legislação;
 - b) o material de acesso restrito regulado pelo CFQ;
 - c) a informação pessoal relativa à intimidade, vida privada, honra e imagem; e
 - d) o documento preparatório não previsto no inciso II do *caput*.

Art. 16. Os dados, metadados, informações e conhecimentos produzidos ou custodiados pelo CFQ, transferidos para o provedor de serviço de nuvem, devem estar hospedados em território brasileiro, observando-se as seguintes disposições:

- I - pelo menos uma cópia atualizada de segurança deve ser mantida em território brasileiro e, se possível, em infraestrutura própria do CFQ;
 - II - a informação sem restrição de acesso poderá possuir cópias atualizadas de segurança fora do território brasileiro, conforme legislação aplicável;
 - III - a informação com restrição de acesso prevista na legislação e o documento preparatório, bem como suas cópias atualizadas de segurança, não poderão ser tratados fora do território brasileiro, conforme legislação aplicável; e
 - IV - no caso de dados pessoais, deverão ser observadas as orientações previstas na Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais - LGPD, e demais legislações sobre o assunto.
-



Seção VIII

Das Cláusulas Contratuais Específicas

Art. 17. O instrumento contratual a ser firmado com um provedor de serviço de nuvem para a prestação do serviço de computação em nuvem deve conter dispositivos que tratem dos requisitos para a adoção segura de computação em nuvem além de, no mínimo, os seguintes procedimentos de segurança:

I - termo de confidencialidade que impeça o provedor de serviço de nuvem de usar, transferir e liberar dados, sistemas, processos e informações do CFQ para empresas nacionais, transnacionais, estrangeiras, países e governos estrangeiros;

II - garantia da exclusividade de direitos, por parte do CFQ, sobre todas as informações tratadas durante o período contratado, incluídas eventuais cópias disponíveis, tais como backups de segurança;

III - proibição do uso de informações do CFQ pelo provedor de serviço de nuvem para propaganda, otimização de mecanismos de inteligência artificial ou qualquer uso secundário não-autorizado;

IV - conformidade da política de segurança da informação do provedor de serviço de nuvem com a legislação brasileira;

V - devolução integral dos dados, informações e sistemas sob custódia do provedor de serviço de nuvem aos órgãos ou às entidades contratantes ao término do contrato;

VI - eliminação, por parte do provedor de serviço de nuvem, ao término do contrato, de qualquer dado, informação ou sistema do CFQ sob sua custódia, observada a legislação que trata da obrigatoriedade de retenção de dados; e

VII - garantia do direito à eliminação dos dados pessoais, conforme art. 16 da Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados.

CAPÍTULO III

DOS REQUISITOS DO PROVEDOR DE SERVIÇO DE NUVEM

Art. 18. Para que esteja habilitado a prestar serviço de computação em nuvem, o provedor de serviço de nuvem deverá cumprir, no mínimo os seguintes requisitos:

I - Possuir uma metodologia de riscos, elaborada e em conformidade com as melhores práticas da legislação vigente;

II - Implementar práticas de fortalecimento dos mecanismos de virtualização, que devem incluir, no mínimo, os seguintes procedimentos:

a) desabilitar ou remover todas as interfaces, portas, dispositivos ou serviços desnecessários executados pelo sistema operacional;

b) configurar com segurança todas as interfaces de rede e áreas de armazenamento virtuais;

c) estabelecer limites para a utilização dos recursos de máquina virtual (*Virtual Machine* - VM);

d) manter todos os sistemas operacionais e as aplicações em execução na máquina virtual em suas versões mais atuais;

e) validar a integridade das operações de gerenciamento de chaves criptográficas;



- f) possuir controles que permitam aos usuários autorizados do CFQ acessarem os registros de acesso administrativo do monitor de máquina virtual -*Hypervisor*;
 - g) habilitar o registro completo do *Hypervisor*; e
 - h) suportar o uso de máquinas virtuais confiáveis (*Trusted VM*) fornecidas pelo CFQ, que estejam em conformidade com as políticas e práticas de fortalecimento de redes exigidas ao provedor de serviço de nuvem.
- III - em relação ao gerenciamento de identidades e registros:
- a) possuir procedimentos de controle de acesso que abordem a transição entre as funções, os limites e controles dos privilégios dos usuários e os controles de utilização das contas de usuários;
 - b) impor mecanismo de autenticação que exija tamanho mínimo, complexidade, duração e histórico de senhas de acesso;
 - c) suportar tecnologia *single sign-on* para autenticação;
 - d) suportar mecanismos de autenticação multifator ou outra alternativa que aumente o grau de segurança no processo de autenticação de usuários do órgão ou da entidade no provedor de serviço de nuvem, de acordo com nível de criticidade da informação;
 - e) permitir ao CFQ gerenciar as próprias identidades, inclusive criação, atualização, exclusão e suspensão no ambiente fornecido pelo provedor de serviço de nuvem; e
 - f) atender aos requisitos legais, às melhores práticas de segurança e a outros critérios exigidos pelo CFQ em seus processos de autenticação, controle de acesso, contabilidade e de registro - formato, retenção e acesso.
- IV - em relação à segurança de aplicações web disponibilizadas no ambiente de nuvem:
- a) utilizar firewalls especializados na proteção de sistemas e aplicações;
 - b) desenvolver código web em conformidade com as melhores práticas de desenvolvimento seguro e com os normativos existentes;
 - c) utilizar melhores práticas de segurança de sistemas operacionais e de aplicações;
 - d) realizar periodicamente testes de penetração de redes e de aplicações; e
 - e) possuir um programa de correção de vulnerabilidades.
- V - possuir processos de gestão de continuidade de negócios e de gestão de mudanças, em conformidade com os normativos existentes e com as melhores práticas nessas áreas;
- VI - possuir um plano de recuperação de desastres que estabeleça procedimentos de recuperação e de restauração de plataforma, infraestrutura, aplicações e dados após incidentes de perda de dados;
- VII - estabelecer um canal de comunicação seguro utilizando, no mínimo, *Secure Sockets Layer/Transport Layer Security (SSL/TLS)*;
- VIII - utilizar um padrão de encriptação seguro, conforme padrão internacional reconhecidamente aceito, que possa ser implementado com chaves de encriptação geradas e armazenadas pelo CFQ;
- IX - disponibilizar facilidades que possibilitem a aplicação de uma proteção criptográfica própria do CFQ;
- X - em relação à segregação de dados:
- a) isolar, utilizando separação lógica, todos os dados e serviços do CFQ de outros clientes de serviço em nuvem;
-



- b) segregar o tráfego de gerenciamento do tráfego de dados do CFQ; e
- c) implementar dispositivos de segurança entre zonas.
- XI - possuir procedimentos em relação ao descarte de ativos de informação e de dados, que assegurem:
 - a) sanitizar ou destruir, de modo seguro, os dados existentes nos dispositivos descartados por meio da utilização de métodos que estejam em conformidade com os padrões estabelecidos para a conduta e as melhores práticas;
 - b) destruir, de modo seguro, ativo de informação no fim do ciclo de vida ou considerado inservível, com o fornecimento de um Certificado de Destruição de Equipamento Eletrônico (*Certificate of Electronic Equipment Destruction* - CEED) e discriminar os ativos que foram reciclados, bem como o peso e os tipos de materiais obtidos em virtude do processo de destruição; e
 - c) armazenar, de modo seguro, ativos de informação a serem descartados, em ambiente com acesso físico controlado, com registro de toda movimentação de entrada e de saída de dispositivos.
- XII - notificar, imediatamente, aos órgãos ou às entidades incidente cibernético contra os serviços ou dados sob sua custódia;
- XIII - possuir procedimentos necessários para preservação de evidências, conforme legislação; e
- XIV - demonstrar estar em conformidade com os padrões de segurança de nuvem, por meio de auditoria anual *Service and Organization Controls 2 (SOC 2)*, conduzida por um auditor independente, com a apresentação dos relatórios de tipo I e tipo II.

CAPÍTULO IV

DA UTILIZAÇÃO DE CLOUD BROKERS

Art. 19. O *cloud broker* deverá atuar como integrador dos serviços de computação em nuvem entre a entidade da administração pública federal e dois ou mais provedores de serviço de nuvem.

Art. 20. Caso o CFQ contrate por meio do cloud broker plataforma de gestão multinuvem para realizar procedimentos de provisionamento e orquestração do ambiente, é necessário que a ferramenta possua, no mínimo:

- I - em relação às funcionalidades de provisionamento e orquestração de multinuvem:
 - a) um único portal integrado de provisionamentos para o usuário final;
 - b) utilização de modelos de provisionamento;
 - c) automação segura de provisionamento simultâneo e utilização, no que couber, ferramentas de código aberto e interoperáveis;
 - d) fluxos de trabalho de orquestração baseada em eventos; e
 - e) soluções seguras integradas de criação de infraestrutura por código – IaC.
 - II - em relação às funcionalidades de monitoramento e análise em multinuvem:
 - a) relatórios de monitoramento de desempenho de recursos na nuvem;
 - b) coleta e monitoramento de registros; e
 - c) procedimentos de monitoramento de alertas.
 - III - em relação às funcionalidades de inventário e classificação em multinuvem:
 - a) inventário de recursos na nuvem;
-



b) procedimentos de segurança para configuração de recursos na plataforma de gestão multinuvem; e

c) detecção de recursos sem etiqueta.

IV - em relação às funcionalidades de gerenciamento de segurança, conformidade e identidade:

a) mecanismos de *single sign-one* de autenticação multifator das plataformas em nuvem;

b) gerenciamento seguro de usuários e de grupos de usuários;

c) gerenciamento de segurança dos recursos;

d) notificações de eventos de alerta multicanal;

e) gerenciamento de identidade e acesso - IAM; e

f) registros de atividade da plataforma em nuvem.

Parágrafo único. O *cloud broker* poderá utilizar ferramenta de *Software as a Service* (SaaS) comum de mercado, desde que não haja risco de dependência tecnológica para disponibilizar essa plataforma.

Art. 21. O *cloud broker* é o responsável por garantir que os provedores de serviço de nuvem que ele representa:

I - cumpram todos os requisitos previstos nesta Portaria e na legislação brasileira; e

II - operem de acordo com as melhores práticas de segurança.

Parágrafo único. O CFQ deverá prever no instrumento contratual que o *cloud broker* poderá ser responsabilizado, civil e administrativamente, por qualquer desconformidade nos provedores que ele representa.

CAPÍTULO V

DAS COMPETÊNCIAS

Art. 22. Compete ao Gestor de Segurança da Informação:

I - instituir e coordenar a equipe responsável pela elaboração e revisões do ato normativo sobre uso seguro de computação em nuvem;

II - supervisionar a aplicação do ato normativo sobre uso seguro de computação em nuvem;

III - assegurar a contínua efetividade da comunicação com o provedor de serviço de nuvem, que fornece tais serviços ao órgão ou à entidade, de forma a assegurar que os controles e os níveis de serviço acordados sejam cumpridos;

IV - supervisionar a aplicação das medidas de correção pelo provedor de serviço de nuvem, em casos de eventuais desvios;

V - comunicar incidentes cibernéticos informados pelo provedor de serviço de nuvem aos órgãos competentes para os seus tratamentos, conforme a relevância dos incidentes previamente estabelecida; e

VI - encaminhar para aprovação da alta administração as minutas de elaboração e de revisões do ato normativo sobre o uso seguro de computação em nuvem.

Art. 23. Compete ao Comitê de Governança Digital:

I - Recomendar os países nos quais dados e informações custodiados pelo CFQ poderão ser armazenados em soluções de computação em nuvem;



II - Definir e recomendar os requisitos criptográficos mínimos para o armazenamento de dados e informações, custodiados pela administração pública federal, em soluções de computação em nuvem; e

III - Propor políticas, diretrizes, normas e práticas relacionadas ao normativo sobre o uso seguro de computação em nuvem, bem como sua revisão.

Art. 24. Compete à Presidência aprovar as minutas de elaboração e de revisões do ato normativo sobre o uso seguro de computação em nuvem e divulgá-las às partes interessadas.

Art. 25. Compete à Equipe de Planejamento da Contratação, na avaliação sobre a possibilidade de contratação de solução de computação em nuvem:

I - durante a elaboração do Estudo Técnico Preliminar verificar se a solução pretendida está em conformidade com esta Portaria;

II - elaborar e atualizar o mapa de riscos; e

III - se após a conclusão do Estudo Técnico Preliminar a solução pretendida for baseada em computação em nuvem a Equipe de planejamento da contratação deverá:

a) prever a capacitação da equipe responsável pelo gerenciamento da solução nas tecnologias utilizadas pelo provedor de serviço de nuvem; e

b) enviar o processo de planejamento da contratação para conhecimento do Comitê de Governança Digital por meio de ofício contendo relatório de conformidade dos requisitos da presente Portaria.

Parágrafo único. A avaliação da solução de computação em nuvem será coordenada pelo integrante técnico da área de TIC.

Art. 26. Ao Fiscal Técnico dos contratos que possuam no seu objeto serviços envolvendo solução de computação em nuvem compete:

I - aplicar checklist de verificação de cumprimento dos requisitos da presente norma junto à contratada, pelo menos, uma vez a cada período de 12 meses de contrato;

II - atualizar o mapa de riscos do contrato, caso haja eventos relevantes, durante a fase de Gestão do Contrato;

III - comunicar incidentes cibernéticos informados pelo provedor de serviço de nuvem a Equipe de Tratamento e Resposta a Incidentes Cibernéticos -ETIR- CFQ;

IV - enviar relatório de conformidade dos requisitos da presente norma para conhecimento do Comitê de Governança Digital; e

V - monitorar e controlar os recursos de computação em nuvem de modo a garantir a continuidade dos serviços.

Parágrafo único. As competências acima farão parte das demais relacionadas na Portaria de nomeação da Equipe de Fiscalização de Contrato correspondente.

CAPÍTULO VI

DAS DISPOSIÇÕES FINAIS

Art. 27. Qualquer outra diretriz específica deve ser fixada em procedimentos internos.

Art. 28. A revisão deste ato normativo deverá ser realizada por equipe instituída para sua revisão e será ordinariamente realizada a cada dois anos.



Parágrafo único. A revisão poderá ocorrer a qualquer tempo, quando houver mudanças significativas nos requisitos de segurança da informação que influenciem o uso seguro de computação em nuvem, de forma a assegurar sua continuidade, sustentabilidade, adequação e efetividade.

Art. 29. Deverá ser instituída uma equipe para revisões do ato normativo sobre o uso seguro da computação em nuvem.

Art. 30. Esta Portaria entra em vigor nesta data.

Dê-se ciência.

Publique-se.

Brasília, 26 de junho de 2023.

JOSÉ DE RIBAMAR OLIVEIRA FILHO
Presidente



ANEXO ÚNICO

GLOSSÁRIO DE SEGURANÇA DA INFORMAÇÃO

Letra A

AAA - sigla de autenticação, autorização e auditoria;

AC - sigla de autoridade certificadora;

AC-RAIZ - sigla de autoridade certificadora raiz;

ACESSO - ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;

ACL - sigla de lista de controle de acesso (access control list);

ADMINISTRADOR DE PERFIL INSTITUCIONAL - agentes públicos que detenham autorização de responsável pela área interessada para administrar perfis institucionais de órgão ou entidade da administração pública federal, direta e indireta, nas redes sociais;

ADMINISTRADOR DE REDE - pessoa física que administra o segmento de rede correspondente à área de abrangência da respectiva unidade;

ADVANCED ENCRYPTION STANDARD(AES) - criado pelo Instituto Nacional de Padrões e Tecnologia (NIST), tornou-se o padrão efetivo do governo federal americano em 2002, após cinco anos de desenvolvimento. Esse desenvolvimento começou em 1997, quando se verificou que seu antecessor, o data encryption standard(criptografia de dados padrão - DES), não estava mais atendendo os critérios de segurança. O AES é construído a partir de três cifras de bloco: AES-128, AES-192 e AES-256. Cada uma dessas criptografia e de criptografa os dados em pedaços de 128 bits, usando chaves criptográficas de 128, 192 ou 256 bits. As chaves de 128 bits têm 10 rodadas de processamento, as chaves de 192 bits têm 12 e as de 256 bits 14 rodadas;

**SERVIÇO PÚBLICO FEDERAL**

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

ADVERTISING SOFTWARE (ADWARE)- tipo específico de spyware projetado especificamente para apresentar propagandas. Pode ser usado de forma legítima, quando incorporado a programas e serviços, como forma de patrocínio ou retorno financeiro, para quem desenvolve programas livres ou presta serviços gratuitos. Também pode ser usado para fins maliciosos, quando as propagandas apresentadas são direcionadas de acordo com a navegação do usuário e sem que este saiba que tal monitoramento está sendo realizado;

ADWARE- sigla de advertising software;

AES - sigla de advanced encryption standard;

AGENTE DEMANDANTE - servidor público, militar de carreira ou empregado público, ocupantes de cargo efetivo em órgão ou entidade da administração pública federal, direta ou indireta, responsável por uma demanda de serviço endereçada à área de segurança de informação, devidamente autorizada pela chefia superior;

AGENTE PÚBLICO - todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação, ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da administração pública federal, direta e indireta;

AGENTE PÚBLICO COM DISPOSITIVO MÓVEL CORPORATIVO - servidor público, militar de carreira ou empregado público, ocupantes de cargo efetivo em órgão ou entidade da administração pública federal, direta ou indireta, que utilize dispositivo móvel de computação de propriedade dos órgãos ou entidades a que pertence;

AGENTE PÚBLICO COM DISPOSITIVO MÓVEL PARTICULAR - servidor público, militar de carreira ou empregado público, ocupantes de cargo efetivo em órgão ou entidade da administração pública federal, direta ou indireta, que utilize dispositivo móvel de computação de sua propriedade. Os dispositivos particulares que se submetem aos padrões corporativos de software e controles de segurança e que são incorporados à rede de um órgão ou entidade são considerados como dispositivos corporativos;

AGENTE RESPONSÁVEL - servidor público, militar de carreira ou empregado público, ocupantes de cargo efetivo em órgão ou entidade da administração pública federal, direta e indireta, que se enquadre em qualquer das opções seguintes: a) execute o tratamento de informação classificada; b) possua credencial de segurança; c) seja responsável por um posto de controle de um órgão de registro; d) utilize dispositivos que tenham embarcado criptografia de Estado;



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

AGENTE RESPONSÁVEL PELA ETIR - servidor público, militar de carreira ou empregado público, ocupantes de cargo efetivo em órgão ou entidade da administração pública federal, direta ou indireta, incumbido de chefiar e gerenciar a equipe de prevenção, tratamento e resposta a incidentes cibernéticos (ETIR);

AGENTE RESPONSÁVEL PELA GESTÃO DE CONTINUIDADE DE NEGÓCIOS - servidor público, militar de carreira ou empregado público, ocupantes de cargo efetivo em órgão ou entidade da administração pública federal, direta e indireta, incumbido de gerenciar o processo de gestão de continuidade de negócios em segurança da informação;

AGENTE RESPONSÁVEL PELA GESTÃO DE MUDANÇA - servidor público, militar de carreira ou empregado público, ocupantes de cargo efetivo em órgão ou entidade da administração pública federal, direta e indireta, incumbido de gerenciar o processo de gestão de mudanças em aspectos de segurança da informação;

AGENTE RESPONSÁVEL PELO MAPEAMENTO DOS ATIVOS DE INFORMAÇÃO - servidor público, militar de carreira ou empregado público, ocupantes de cargo efetivo em órgão ou entidade da administração pública federal, direta e indireta, incumbido de gerenciar o processo de mapeamento de ativos de informação;

AGENTE RESPONSÁVEL PELA GESTÃO DE RISCOS - servidor público, militar de carreira ou empregado público, ocupantes de cargo efetivo em órgão ou entidade da administração pública federal, direta e indireta, incumbido de gerenciar o processo de gestão de riscos de segurança da informação;

AGENTE RESPONSÁVEL DE POSTO DE CONTROLE - representante do gestor de segurança e credenciamento de um órgão de registro em um posto de controle, a ele subordinado, podendo ser instituído a critério dos órgãos de registro;

AGENTE RESPONSÁVEL PELO USO SEGURO DE MÍDIAS SOCIAIS - servidor público, militar de carreira ou empregado público, ocupantes de cargo efetivo em órgão ou entidade da administração pública federal, direta e indireta, incumbido de gerenciar, de forma contínua, o uso seguro de mídias sociais de sua organização;

AGENTES DE TRATAMENTO - o controlador ou o operador;



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

ALERTA DE ETIR - informação descritiva de um incidente cibernético enviada, de forma reativa, para notificação de usuários;

ALGORITMO CRIPTOGRÁFICO - função matemática utilizada na cifração e na decifração de informações sigilosas, necessariamente nas informações classificadas;

ALGORÍTMO DE ESTADO - função matemática utilizada na cifração e na decifração, desenvolvida pelo Estado, para uso exclusivo em interesse do serviço de órgãos ou entidades do Poder Executivo federal;

AMBIENTAÇÃO - evento que oferece informações sobre a missão organizacional do órgão ou entidade da administração pública federal, direta e indireta, bem como sobre o papel do agente público nesse contexto;

AMBIENTE CIBERNÉTICO - inclui usuários, redes, dispositivos, software, processos, informação armazenada ou em trânsito, serviços e sistemas que possam ser conectados direta ou indiretamente a redes de computadores;

AMBIENTE DE INFORMAÇÃO - agregado de indivíduos, organizações ou sistemas que coletam, processam ou disseminam informação;

AMEAÇA - conjunto de fatores externos com o potencial de causar em dano para um sistema ou organização;

AMEAÇA PERSISTENTE AVANÇADA (APT) - operações de longo prazo, projetadas para infiltrar ou exfiltrar o máximo possível de dados, sem serem descobertas. Possui ciclo de vida mais longo e mais complexo que outros tipos de ataque, sendo mais elaboradas e necessitando de volume significativo de recursos para sua viabilização, o que exige forte coordenação. Em geral, são realizadas por grupos com intenção de espionagem ou sabotagem;

ANÁLISE DE IMPACTO NOS NEGÓCIOS (BIA) - visa estimar os impactos resultantes da interrupção de serviços e de cenários de desastres que possam afetar o desempenho dos órgãos ou entidades da administração pública federal, bem como as técnicas para qualificar e quantificar esses impactos. Define também a criticidade dos processos de negócio, suas prioridades de



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

recuperação, interdependências e os requisitos de segurança da informação, para que os objetivos de recuperação sejam atendidos nos prazos estabelecidos;

ANÁLISE DE INCIDENTES - consiste em examinar todas as informações disponíveis sobre o incidente, incluindo artefatos e outras evidências relacionadas ao evento. O propósito dessa análise é identificar o escopo do incidente, sua extensão, sua natureza e os prejuízos causados. Também faz parte da análise do incidente propor estratégias de contenção e recuperação;

ANÁLISE DE RISCOS - uso sistemático de informações para identificar fontes e estimar o risco;

ANÁLISE DE VULNERABILIDADES - verificação e exame técnico de vulnerabilidades, para determinar onde estão localizadas e como foram exploradas;

ANÁLISE DINÂMICA - tipo de teste de software que verifica seu comportamento externo em busca de anomalias ou vulnerabilidades. A análise dinâmica ocorre por meio de execução do software com dados de teste para examinar as saídas e o comportamento operacional. Ela opera como complemento da análise estática, considerando o código como uma caixa-preta. A principal vantagem da análise dinâmica é evidenciar defeitos sutis ou vulnerabilidades cujas origens são muito complexas para serem descobertas na análise estática. A análise dinâmica pode desempenhar um papel na garantia da segurança, mas seu principal objetivo é encontrar e eliminar erros (debug). Após o produto passar por um teste de análise dinâmica, ele tende a ficar mais limpo, o que traz consideráveis melhorias na performance;

ANÁLISE ESTÁTICA - tipo de teste de software que verifica a lógica interna em busca de falhas ou vulnerabilidades. A análise estática ocorre por meio de revisão, análise automatizada ou verificação formal do código-fonte ou dos binários, usando uma abordagem do tipo caixa-branca. Uma ferramenta que executa a análise estática de forma automatizada procura, essencialmente, por erros que possam impedir a execução (run-time errors), por erros comuns da linguagem alvo e por código potencialmente malicioso, sendo especialmente eficiente para encontrar erros como a corrupção de memória e estouros de buffer, vazamentos de memória, operações ilegais e inseguras, ponteiros nulos, loops infinitos, código incompleto, código redundante e código morto (absolutamente sem uso). Permite também identificar se está sendo chamada uma biblioteca incorretamente ou se a linguagem está sendo utilizada de forma incorreta ou de forma inconsistente;

ANONIMIZAÇÃO - utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

ANPD - sigla de Autoridade Nacional de Proteção de Dados;

APETITE AO RISCO - nível de risco que uma organização está disposta a aceitar;

API - sigla de interface de programação de aplicações (application programming interface);

APT - sigla de ameaça persistente avançada (advanced persistent threat);

AQUISIÇÃO DE EVIDÊNCIA - processo de coleta e cópia das evidências de incidente de segurança em redes computacionais;

AR - sigla de autoridade de registro;

ÁREA DE INFORMAÇÃO - esfera de atividade que envolve a criação, transformação e uso da informação, a infraestrutura de tecnologia da informação envolvida e a informação propriamente dita;

ÁREAS E INSTALAÇÕES DE ACESSO RESTRITO - áreas e instalações que contenham documento com Informação Classificada, ou que, por sua utilização ou finalidade, demandarem proteção, as quais tem seu acesso restrito às pessoas autorizadas pelo órgão ou entidade;

ÁREAS PRIORITÁRIAS - áreas definidas no Plano Nacional de Segurança de Infraestruturas Críticas para a aplicação da Política Nacional de Segurança de Infraestruturas Críticas, nos termos do disposto no art. 9º, inciso I, do Anexo ao Decreto nº 9.573, de 22 de novembro de 2018;

ARMA CIBERNÉTICA -software, hardware e firmware projetado ou aplicado especificamente para causar dano, por meio do domínio cibernético. Estão incluídas nessa categoria: ferramentas para acesso não-autorizado, vírus, worms, trojans, DoS, DDoS, botnets e rootkits. Além disso, atividades como a engenharia social também são consideradas armas cibernéticas. Armas cibernéticas podem ser utilizadas individualmente ou em conjunto para aumentar os efeitos desejados;



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

ARMA CIBERNÉTICA CINÉTICA -software, hardware e firmware projetado ou aplicado especificamente para causar danos físicos, direta ou indiretamente, tanto em pessoas como em equipamentos, somente por meio da exploração de vulnerabilidades dos sistemas e processos de informação;

ARP - sigla de address resolution protocol (protocolo de resolução de endereços);

ARQUITETURA AAA - arquitetura que define uma forma estruturada para integração das funcionalidades de autenticação, autorização e auditoria;

ARQUITETURA DE REDE - definição de alto nível do comportamento e das conexões entre os nós em uma rede, suficiente para possibilitar a avaliação das propriedades da rede;

ARTEFATO MALICIOSO - qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas ou redes de computadores;

ASSINATURA DIGITAL - tipo de assinatura eletrônica que usa operações matemáticas, com base em algoritmos criptográficos de criptografia assimétrica, para garantir segurança na autenticidade das documentações. É necessário possuir um certificado digital para assinar digitalmente um documento. Entre as principais vantagens do uso de assinatura digital estão o não repúdio, princípio em que não há dúvidas quanto ao remetente, e tempestividade, princípio pelo qual a autoridade certificadora pode verificar data e hora da assinatura de um documento;

ASSINATURA ELETRÔNICA - mecanismos que permitem a assinatura de documentos virtuais com validade jurídica. A legislação brasileira disciplinou a assinatura eletrônica, de forma ampla, por meio da Medida Provisória 2.200-2, de 24 de agosto de 2001;

ATAQUE - ação que constitui uma tentativa deliberada e não autorizada para acessar ou manipular informações, ou tornar um sistema inacessível, não íntegro, ou indisponível;

ATAQUESYBIL- estratégia baseada na saturação de uma rede blockchain, com diversos clones (sybils), dando apoio a uma determinada decisão, a fim de reverter o consenso obtido anteriormente, utilizando mecanismos proof of work ou proof of stake. Ataques sybil são uma extensão do conceito de gastos-duplos;



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

ATIVIDADE - ação ou conjunto de ações executados por um órgão ou entidade, ou em seu nome, que produzem ou suportem um ou mais produtos ou serviços;

ATIVIDADE CRÍTICA - atividade que deve ser executada visando garantir a consecução de produtos e serviços fundamentais do órgão ou entidade, de forma a atingir os objetivos mais importantes e sensíveis ao tempo;

ATIVIDADE MALICIOSA - qualquer atividade que infrinja a política de segurança de uma instituição ou que atente contra a segurança de um sistema;

ATIVO - tudo que tenha valor para a organização, material ou não;

ATIVO DE REDE - equipamento que centraliza, interliga, roteia, comuta, transmite ou concentra dados em uma rede de computadores;

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;

ATOS INTERNACIONAIS - vide tratados internacionais;

ATUALIZAÇÃO AUTOMÁTICA - atualizações que são feitas no dispositivo ou sistema, sem a interferência do usuário, inclusive, em alguns casos, sem notificação ao usuário;

ATUALIZAÇÃO AUTOMATIZADA - fornece aos usuários a habilidade de aprovar, autorizar e rejeitar uma atualização. Em alguns casos, o usuário pode necessitar ter o controle de como e quando as atualizações serão implementadas, em função de horário de funcionamento, limite de consumo de dados da conexão, padronização do ambiente, garantia de disponibilidade, entre outros aspectos;

AUDITORIA - processo de exame cuidadoso e sistemático das atividades desenvolvidas, cujo objetivo é averiguar se elas estão de acordo com as disposições planejadas e estabelecidas previamente, se foram implementadas com eficácia e se estão adequadas e em conformidade à consecução dos objetivos;



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

AUTENTICAÇÃO - processo que busca verificar a identidade digital de uma entidade de um sistema, no momento em que ela requisita acesso a esse sistema. O processo é realizado por meio de regras preestabelecidas, geralmente pela comparação das credenciais apresentadas pela entidade com outras já pré-definidas no sistema, reconhecendo como verdadeiras ou legítimas as partes envolvidas em um processo;

AUTENTICAÇÃO DE DOIS FATORES (2 FACTOR AUTHENTICATION) - processo de segurança que exige que os usuários forneçam dois meios de identificação antes de acessarem suas contas;

AUTENTICAÇÃO DE MULTIFATORES (MFA) - utilização de dois ou mais fatores de autenticação para concessão de acesso a um sistema. Os fatores de autenticação se dividem em: algo que o usuário conhece (senhas, frases de segurança, PIN, dentre outros); algo que o usuário possui (certificado digital, tokens, códigos enviados por SMS, dentre outros); algo que o usuário é (aferível por meios biométricos, tais como digitais, padrões de retina, reconhecimento facial, dentre outros); e onde o usuário está (quando o acesso só pode ser feito em uma máquina específica, cujo acesso é restrito);

AUTENTICAÇÃO MÚTUA - processo em que duas partes, tipicamente um cliente e um servidor, se autenticam mutuamente. Essa autenticação permite que ambos conheçam a identidade um do outro. Na autenticação mútua, o servidor solicita também um certificado do cliente. Também conhecida como autenticação bidirecional;

AUTENTICIDADE - propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;

AUTORIDADE CERTIFICADORA (AC) - entidade responsável por emitir e gerenciar certificados digitais;

AUTORIDADE CERTIFICADORA RAIZ (AC-RAIZ) - situa-se no topo da hierarquia da cadeia de certificação, portanto sendo a primeira autoridade. Sua função é executar as normas técnicas e operacionais e as políticas de certificados estabelecidas pelo Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira (ICP). Isso significa que a AC-Raiz pode emitir, distribuir, expedir, revogar e gerenciar os certificados das autoridades que estão abaixo de seu nível hierárquico, que são as autoridades certificadoras. A autoridade certificadora raiz da ICP Brasil é o Instituto Nacional de Tecnologia da Informação (ITI);



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

AUTORIDADE DE REGISTRO (AR) - estabelece a interface entre o usuário e a autoridade certificadora (AC). A AR vincula-se à AC e tem como principal objetivo ser o intermediário presencial entre a AC e o interessado pelo certificado digital, recebendo, validando e encaminhando as solicitações de emissão ou revogação dos certificados digitais, além de identificar os solicitantes de certificados digitais de forma presencial;

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) - órgão da administração pública federal responsável por zelar, implementar e fiscalizar o cumprimento da Lei nº 13.709, de 14 de agosto de 2018;

AUTORIZAÇÃO - processo que ocorre após a autenticação e que tem a função de diferenciar os privilégios atribuídos ao usuário que foi autenticado. Os atributos de autorização normalmente são definidos em grupos mantidos em uma base de dados centralizada, sendo que cada usuário herda as características do grupo a que ele pertence; portanto, autorização é o direito ou a permissão de acesso a um recurso de um sistema;

AValiação de CONFORMIDADE DE SEGURANÇA DA INFORMAÇÃO - exame sistemático do grau de atendimento dos requisitos relativos à segurança da informação com legislações específicas;

AValiação de RISCOS - processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco;

Letra B

BaaS - sigla de backend as a service;

BACKDOOR- qualquer mecanismo inserido no sistema, intencionalmente ou acidentalmente, com o objetivo de permitir o acesso não documentado ao sistema ou aos seus dados;

BACKEND AS A SERVICE(BaaS) - serviço de computação em nuvem que serve como middleware. Fornece aos desenvolvedores uma forma para conectar suas aplicações mobile e web a serviços na nuvem, a partir de interface de programação de aplicações (API) e de kit de desenvolvimento de software (SDK), abstraindo completamente a infraestrutura do lado do servidor;



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

BACKUP- conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada;

BANCO DE DADOS - coleção de dados inter-relacionados, representando informações sobre um domínio específico. São coleções organizadas de dados que se relacionam, a fim de criar algum sentido (informação) e de dar mais eficiência durante uma consulta ou a geração de informações ou conhecimento;

BANCO DE DADOS PESSOAIS - conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

BIA - sigla de business impact analysis (análise de impacto de negócios);

BIG DATA- conjuntos de dados extremamente amplos e que, por este motivo, necessitam de ferramentas especialmente preparadas para lidar com grandes volumes, de forma que toda e qualquer informação nesses meios possa ser encontrada, analisada e aproveitada em tempo hábil;

BIOMETRIA - verificação da identidade de um indivíduo por meio de uma característica física

o8BLACKLIST- lista de itens aos quais é negado o acesso a certos recursos, sistemas ou protocolos. Utilizar uma blacklist para controle de acesso significa garantir o acesso a todas entidades exceto àquelas incluídas na blacklist;

BLINDAGEM - também chamada de hardening, trata-se de um processo de mapeamento das ameaças, mitigação dos riscos e execução das atividades corretivas, com foco em infraestrutura, com o principal objetivo de torná-la preparada para enfrentar tentativas de ataque;

BLOCKCHAIN- base de dados que mantém um conjunto de registros que crescem continuamente. Novos registros são apenas adicionados à cadeia existente, sem que nenhum registro seja apagado;

BLOQUEIO - suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

BLOQUEIO DE ACESSO - processo que tem por finalidade suspender temporariamente o acesso;

BOT- tipo de malware que, além de incluir funcionalidades de worms, dispõe de mecanismos de comunicação com o invasor, os quais permitem que o computador infectado seja controlado remotamente. O processo de infecção e propagação do bot é similar ao do worm, ou seja, o bot é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados em computadores;

BOTNET- rede formada por diversos computadores zumbis (infectados com bots). Permite potencializar as ações danosas executadas pelos bots e ser usada em ataques de negação de serviço, esquemas de fraude, envio de spam, entre outros;

BRING YOUR OWN DEVICE(BYOD) - trata-se de uma política de segurança de uma organização, que permite que os dispositivos pessoais dos funcionários sejam usados nas atividades corporativas. Uma política BYOD estabelece limitações e restrições sobre se um dispositivo pessoal (como um notebook, smartphone ou tablet) pode ou não ser conectado pela rede corporativa;

BUILD- desenvolvimento de software, build é o termo usado para identificar uma versão compilada de um programa, ou seja, quando as linhas de código escritas em linguagem de alto nível são traduzidas para linguagem de máquina, que um computador é capaz de entender. A build pode ser completa (software inteiro) ou parcial (partes dele);

BYOD - sigla de bring your own device;

Letra C

CADEIA DE CUSTÓDIA - processo que acompanha o movimento de evidência, por meio de sua coleta, salvaguarda e ciclo de análise, documentando cada indivíduo que manuseou a evidência, o momento (data e hora) em que a evidência foi coletada ou transferida e o propósito de cada transferência. Contribui para a validação da prova pericial e do respectivo laudo gerado, porque garante a idoneidade e rastreabilidade dos vestígios, com a finalidade de preservar a confiabilidade e transparência até que o processo seja concluído;



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

CAVALO DE TRÓIA - tipo de malware que, além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário;

CERT DIVISION- vide computer emergency response team division;

CERTIFICAÇÃO - atesta a validade de um documento ou entidade;

CERTIFICAÇÃO DE POSTO DE CONTROLE - comprovação da conformidade dos requisitos técnicos mínimos, verificados por ocasião de uma inspeção de segurança;

CERTIFICAÇÃO PROFISSIONAL - processo acordado pelas representações dos setores especializados, pelo qual se identifica, avalia e valida formalmente os conhecimentos, saberes, competências, habilidades e aptidões profissionais desenvolvidos em programas educacionais ou por experiência de trabalho, com o objetivo de promover o acesso, a permanência e a progressão profissional;

CERTIFICADO - documento assinado de forma criptografada, destinado a assegurar para outros a identidade do terminal que utiliza o certificado. Um certificado é considerado confiável quando for assinado por outro certificado confiável, como uma autoridade de certificação, ou se ele próprio é um certificado confiável, pertence a uma cadeia de confiança reconhecida;

CERTIFICADO DE CONFORMIDADE - garantia formal de que um produto ou serviço, devidamente identificado, está em conformidade com uma norma legal;

CERTIFICADO DIGITAL - conjunto de dados de computador, gerados por uma autoridade certificadora, em observância à recomendação internacional ITU-T X.509 que se destina a registrar, de forma única, exclusiva e intransferível, a relação existente entre uma chave criptográfica e uma pessoa física, jurídica, máquina ou aplicação;

CHAVE CRIPTOGRÁFICA - valor que trabalha com um algoritmo criptográfico para cifração ou decifração;

CIDIC - sigla de código de indexação de documento com informação classificada;



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

CIFRAÇÃO - ato de codificar sinais de linguagem em claro, mediante uso de algoritmo criptográfico simétrico ou assimétrico, com o intuito de transformá-los em sinais ininteligíveis para pessoas não autorizadas a conhecê-la;

CLICKJACKING- técnica maliciosa em que uma vítima é induzida a clicar em URL, botão ou outro objeto de tela que ela não tenha percebido e nem pretendido clicar. O clickjacking pode ser realizado de muitas maneiras, uma delas seria carregar uma página web, de forma transparente, atrás de outra página visível, de forma que os links e objetos para clicar são apenas fachadas; ou seja, quando o usuário clicar em um link aparentemente óbvio, ele, na verdade, estará selecionando o link de uma página oculta;

CLOUD BROKER- indivíduo ou organização que oferece consultoria, medeia e facilita a seleção de soluções de computação em nuvem em nome de uma organização. Um cloud broker serve como um terceiro entre um provedor de serviço de nuvem (PSN) e uma organização que contrata serviços de computação em nuvem. Para as infraestruturas de multi-nuvem, o cloud broker proporciona uma visão mais centralizada de todos os fornecedores e soluções, o que auxilia no gerenciamento dos recursos disponíveis e também dos custos. Em geral, consideram-se quatro tipos de cloud broker: a) serviços de agregação, que garantem a interoperabilidade entre diversos provedores de serviço de nuvem, por meio da agregação de todos os serviços contratados em uma única interface; b) serviços de integração, que adicionam valor automatizando fluxos de trabalho em ambientes híbridos, por meio de uma única orquestração, para melhorar o desempenho e reduzir o risco de negócios; c) serviços de personalização (ou customização), que modificam os serviços de nuvem existentes, a fim de atender às necessidades dos negócios da contratante, podendo inclusive desenvolver recursos adicionais para executar corretamente os serviços desejados; d) serviços de arbitragem, fornecendo flexibilidade ao contratante por intermédio da oferta de vários serviços semelhantes para avaliação e seleção;

CLOUD JACKING- forma de ataque cibernético em que hackers infiltram-se nos programas e nos sistemas armazenados em ambiente de computação em nuvem, a fim de utilizar esses recursos para minerar criptomoedas;

CLOUD SECURITY ALLIANCE(CSA) - uma das principais organizações do mundo dedicada à definição e conscientização das melhores práticas, com a finalidade de ajudar a garantir um ambiente seguro de computação em nuvem, por meio de trabalhos de pesquisa, educação, eventos e produtos específicos para segurança em nuvem. Ela também opera um dos programas mais populares de certificação de provedor de segurança na nuvem, o CSA security, trust and assurance registry (STAR);



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

CÓDIGO DE INDEXAÇÃO - código alfanumérico que indexa documento com informação classificada em qualquer grau de sigilo;

CÓDIGO MALICIOSO - programa, ou parte de um programa de computador, projetado especificamente para atentar contra a segurança de um sistema computacional, normalmente por meio de exploração de alguma vulnerabilidade de sistema;

COLETA DE EVIDÊNCIAS DE SEGURANÇA EM REDES COMPUTACIONAIS - processo de obtenção de itens físicos que contém uma potencial evidência, mediante a utilização de metodologia e de ferramentas adequadas. Esse processo inclui a aquisição, ou seja, a geração das cópias das mídias ou a coleta de dados que contenham evidências do incidente;

COMITÊ DE SEGURANÇA DA INFORMAÇÃO - grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação no âmbito do órgão ou entidade da administração pública federal;

COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO - instituído pelo Decreto nº 9.637, de 26 de dezembro de 2018, com atribuição de assessorar o Gabinete de Segurança Institucional da Presidência da República (GSI/PR) nas atividades relacionadas à segurança da informação;

COMITÊ GESTOR DA ICP BRASIL - vinculado à Casa Civil da Presidência da República, possui como principal competência determinar as políticas que a AC-Raiz executará. É composto por cinco representantes da sociedade civil, integrantes de alguns setores afetos ao tema e representantes de órgãos da administração pública federal;

COMMON VULNERABILITIES AND EXPOSURES(CVE) - banco de dados on-line de ataques, explorações e comprometimento de segurança. É mantido pela MITRE Corporation em benefício do público. Ele inclui quaisquer ataques e abusos conhecidos, sobre qualquer tipo de sistema computacional ou produto de software. Muitas vezes, novos ataques e explorações são documentados em um CVE muito antes do fornecedor admitir o problema ou liberar uma atualização ou patch para resolver a situação. O link para o CVE é <https://cve.mitre.org/>;

COMPUTER EMERGENCY RESPONSE TEAM DIVISION(CERT DIVISION) - divisão do Software Engineering Institute(SEI), que se trata de um centro de pesquisa e desenvolvimento financiado pelo governo federal dos Estados Unidos sem fins lucrativos. O CERT pesquisa ameaças cibernéticas que impactam o desenvolvimento e utilização de software e a segurança na Internet, publica pesquisas e informações sobre suas descobertas e trabalha com empresas e governo para melhorar a segurança do software e da Internet como um todo;



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

COMPUTAÇÃO EM NUVEM - modelo de fornecimento e entrega de tecnologia de informação que permite acesso conveniente e sob demanda a um conjunto de recursos computacionais configuráveis, sendo que tais recursos podem ser provisionados e liberados com mínimo gerenciamento ou interação com o provedor do serviço de nuvem (PSN);

COMPROMETIMENTO - perda de segurança resultante do acesso não autorizado;

COMUNICAÇÃO DE DADOS - transmissão, emissão ou recepção de dados ou informações de qualquer natureza, por meios confinados, por radiofrequência ou por qualquer outro processo eletrônico ou eletromagnético ou ótico;

COMUNICAÇÃO DO RISCO - troca ou compartilhamento de informação sobre risco entre o tomador de decisão e outras partes interessadas;

COMUNIDADE OU PÚBLICO ALVO - conjunto de pessoas, setores, órgãos ou entidades atendidas por uma Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos;

CONFIANÇA ZERO - modelo de segurança criado em 2010, por John Kindervag, cujo principal conceito é não confiar em qualquer entidade interna ou externa à rede de infraestrutura de tecnologia da informação da organização. Atuando sempre com a suposição de que existem violações de segurança, esse modelo implica em alteração na postura, na política e no processo da organização, visando eliminar os problemas de estratégias, com foco apenas no perímetro, por meio da adoção de três princípios básicos: a) exigência de acesso seguro a todos os recursos, independentemente da origem da solicitação (interna ou externa) ou de quais recursos ela acesse; b) adoção de um modelo de privilégio mínimo, com a utilização de políticas adaptativas baseadas em risco e proteção de dados, em especial, pelo controle de permissões desnecessárias e usuários inativos; c) inspeção e registro de todos os eventos, com a aplicação de análises avançadas, para detectar e responder às anomalias em tempo real;

CONFIDENCIALIDADE - propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, ao sistema, ao órgão ou à entidade não autorizados nem credenciados;

CONFORMIDADE EM SEGURANÇA DA INFORMAÇÃO - cumprimento das legislações, normas e procedimentos relacionados à segurança da informação da organização;



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

CONSCIENTIZAÇÃO - atividade que tem por finalidade orientar sobre o que é segurança da informação, levando os participantes a obterem um nível adequado de conhecimento sobre segurança, além de um senso apropriado de responsabilidade. O objetivo dessa atividade é proteger o ativo de informações do órgão ou entidade, para garantir a continuidade dos negócios, minimizar os danos e reduzir eventuais prejuízos financeiros;

CONSENTIMENTO - manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

CONTA DE SERVIÇO - conta de acesso à rede corporativa de computadores, necessária a um procedimento automático (aplicação, script, entre outros) sem qualquer intervenção humana no seu uso;

CONTATO TÉCNICO DE SEGURANÇA - pessoa ou equipe a ser acionada em caso de incidente de segurança envolvendo a administração pública federal, com atribuições eminentemente técnicas sobre a questão;

CONTÊINER DOS ATIVOS DE INFORMAÇÃO - local onde se encontra o ativo de informação. Geralmente, um contêiner descreve algum tipo de ativo tecnológico -hardware, software ou sistema de informação (mas também pode se referir a pessoas ou mídias como papel, CD-ROM ou DVD-ROM). Um contêiner, portanto, é qualquer tipo de ativo dentro do qual um ativo de informação é armazenado, transportado ou processado. Ele pode ser um único ativo tecnológico (como um servidor), uma coleção de ativos tecnológicos (como uma rede) ou uma coletânea de mídias digitais, entre outros;

CONTINUIDADE DE NEGÓCIOS - capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, a fim de manter suas operações em um nível aceitável, previamente definido;

CONTRATO SIGILOSO - ajuste, convênio ou termo de cooperação, cujo objeto ou execução implique tratamento de informação classificada;

CONTROLADOR - pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

CONTROLE DE ACESSO - conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Via de regra, requer procedimentos de autenticação;

CONTROLE DE ACESSO À INFORMAÇÃO CLASSIFICADA - realizado por meio de credencial de segurança e da demonstração da necessidade de conhecer;

CONTROLE DE ACESSO BASEADO EM PAPÉIS (RBCA) - é uma abordagem para restringir o acesso a usuários autorizados. Definem os direitos e permissões baseados no papel que determinado usuário desempenha na organização. Esta estratégia simplifica o gerenciamento das permissões dadas aos usuários;

CONTROLES DE SEGURANÇA - certificado que autoriza uma pessoa natural para o tratamento de informação classificada;

CÓPIA DE SEGURANÇA – vide backup;

CREDENCIAL DE ACESSO - permissão concedida por autoridade competente, após o processo de credenciamento, que habilita determinada pessoa, sistema ou organização ao acesso de recursos. A credencial pode ser física (como por exemplo um crachá), ou lógica (como por exemplo a identificação de usuário e senha);

CREDENCIAL DE SEGURANÇA - certificado que autoriza pessoa para o tratamento de informação classificada;

CREDENCIAMENTO - processo pelo qual o usuário recebe credenciais de segurança que concederão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e definição de perfil de acesso, em função de autorização prévia e da necessidade de conhecer;

CREDENCIAMENTO DE SEGURANÇA - processo utilizado para habilitar órgão ou entidade, público ou privado, ou para credenciar pessoa natural para o tratamento de informação classificada;



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

CRIME CIBERNÉTICO - ato criminoso ou abusivo contra redes ou sistemas de informações, seja pelo uso de um ou mais computadores, utilizados como ferramentas para cometer o delito ou tendo como objetivo uma rede ou sistema de informações a fim de causar incidente, desastre cibernético ou obter lucro financeiro;

CRIPTOGRAFIA - arte de proteção da informação, por meio de sua transformação em um texto cifrado (criptografado), com o uso de uma chave de cifragem e de procedimentos computacionais previamente estabelecidos, a fim de que somente o(s) possuidor(es) da chave de decifragem possa(m) reverter o texto criptografado de volta ao original (texto pleno). A chave de decifragem pode ser igual (criptografia simétrica) ou diferente (criptografia assimétrica) da chave de cifragem;

CRIPTOGRAFIA ASSIMÉTICA - vide criptografia de chave pública;

CRIPTOGRAFIA BASEADA NA IDENTIDADE (IBE) - também conhecida por criptografia baseada em identidade (identity-based encryption), trata-se de um tipo de criptografia de chave pública, no qual um usuário pode gerar uma chave pública a partir de um identificador único conhecido (como por exemplo um endereço de e-mail), em que um servidor confiável de terceiros calcula a chave privada correspondente, a partir da chave pública. Dessa forma, não há necessidade de distribuir chaves públicas antes da troca de dados criptografados;

CRIPTOGRAFIA DE CHAVE PÚBLICA - também conhecida como criptografia assimétrica, é qualquer sistema criptográfico que usa pares de chaves: chaves públicas, que podem ser amplamente disseminadas, e chaves privadas, que são conhecidas apenas pelo proprietário. Isto realiza duas funções: autenticação, em que a chave pública verifica se um portador da chave privada aparelhada enviou a mensagem; e encriptação, em que apenas o portador da chave privada aparelhada pode decifrar a mensagem encriptada com a chave pública;

CROSS-SITE SCRIPTING(XSS) - método de ataque que explora vulnerabilidades de scripting entre sites, que visa contornar controles de acesso, como a política de mesma origem. Ao injetar um script malicioso em uma entrada desprotegida ou não validada do navegador, o invasor faz com que o script seja devolvido pelo aplicativo e executado no navegador. Um ataque XSS bem-sucedido pode permitir ao invasor assumir o controle das funcionalidades do aplicativo, manipular dados ou implantar códigos maliciosos adicionais. Os ataques XSS também permitem que os invasores injetem scripts do lado do cliente, em páginas da web visualizadas por outros usuários;

CSA - sigla de cloud security alliance;



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

CSIRT (COMPUTER SECURITY INCIDENT RESPONSE TEAM) - sigla internacional para designar um grupo de resposta a incidentes de segurança, responsável por tratar incidentes de segurança para um público alvo específico;

CTIR GOV - Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, subordinado ao Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República;

CUSTÓDIA - consiste na responsabilidade de guardar um ativo para terceiros. A custódia não permite automaticamente o acesso ao ativo e nem o direito de conceder acesso a outros;

CUSTODIANTE - aquele que, de alguma forma, total ou parcialmente, zela pelo armazenamento, operação, administração e preservação de um sistema estruturante, ou dos ativos de informação que compõem o sistema de informação, que não lhe pertence, mas que está sob sua custódia;

CUSTODIANTE DA INFORMAÇÃO - qualquer indivíduo ou estrutura de órgão ou entidade da administração pública federal, direta e indireta, que tenha responsabilidade formal de proteger a informação e aplicar os níveis de controles de segurança, em conformidade com as exigências de segurança da informação, comunicadas pelo proprietário da informação;

CVE - sigla de common vulnerabilities and exposures;

Letra D

DADO ANONIMIZADO - dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

DADO EM REPOUSO - informação armazenada. A proteção dos dados em repouso não deve ser subestimada, pois informações valiosas podem não ser transmitidas por canais de comunicação, mas apenas serem imóveis;

DADO PESSOAL - informação relacionada à pessoa natural identificada ou identificável;



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

DADO PESSOAL SENSÍVEL - dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

DADOS PROCESSADOS - dados submetidos a qualquer operação ou tratamento, por meio de processamento eletrônico ou por meio automatizado, com o emprego de tecnologia da informação;

DATAGRAMA (PACOTE DE DADOS) - trata-se de dados encapsulados, ou seja, dados aos quais são acrescentados cabeçalhos com informações sobre o seu transporte (como o endereço IP de destino). Os dados contidos nos datagramas são analisados e eventualmente alterados pelos switches (roteadores) que permitem o seu trânsito. Os dados circulam na Internet na forma de datagramas;

DC - sigla de documento controlado;

DDoS - sigla de negação de serviço distribuída (distributed denial of service);

DECIFRAÇÃO - ato de decifrar, mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para reverter processo de cifração original;

DEEPFAKE - forma de vídeo manipulado, utilizando técnicas de síntese de imagem humana, que criam renderizações artificiais hiper-realistas de um ser humano. Esses vídeos geralmente são criados pela mistura de um vídeo já existente com novas imagens, áudio e vídeo, para criar a ilusão da fala. Esse processo é realizado por meio de redes contraditórias generativas (GAN). A consequência mais perigosa da popularidade dos deepfakes é que eles podem facilmente convencer as pessoas a acreditarem em uma determinada história ou teoria, o que pode resultar em comportamentos com grande impacto na vida política, social ou financeira;

DEFESA CIBERNÉTICA - ações realizadas no espaço cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os ativos de informação de interesse da defesa nacional, obter dados para a produção de conhecimento de inteligência e buscar superioridade sobre os sistemas de informação do oponente;



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

DESASTRE - evento, ação ou omissão, repentino e não planejado, que tenha permitido acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica, gerando sérios impactos em sua capacidade de entregar serviços essenciais ou críticos por um período de tempo superior ao tempo objetivo de recuperação;

DESCARTE - eliminação correta de informações, documentos, mídias e acervos digitais;

DESCREDENCIAMENTO DE SEGURANÇA - processo utilizado para desabilitar órgão ou entidade, pública ou privada, ou para revogar a credencial de pessoal natural, para o tratamento da informação classificada;

DIREITO DE ACESSO - privilégio associado a um cargo, pessoa ou processo, para ter acesso a um ativo;

DISPONIBILIDADE - propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

DISPOSITIVOS MÓVEIS - equipamentos portáteis, dotados de capacidade de processamento, ou dispositivos removíveis de memória para armazenamento, entre os quais se incluem, não limitando a estes: e-books, notebooks, netbooks, smartphones, tablets, pendrives, USBdrives, HD externo, e cartões de memória;

DLT - sigla de livro razão distribuído (distributed ledger technology);

DLP - sigla de prevenção de perda de dados (data loss prevention);

DMZ - sigla de zona desmilitarizada (demilitarized zone);

DOCUMENTO - unidade de registro de informações, qualquer que seja o suporte ou o formato;



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

DOCUMENTOS CLASSIFICADOS - documentos que contenham informação classificada em qualquer grau de sigilo;

DOCUMENTO CONTROLADO - documento que contenha informação classificada em qualquer grau de sigilo ou previsto na legislação como sigiloso, que requeira medidas adicionais de controle;

DOCUMENTO PREPARATÓRIO - documento formal utilizado como fundamento da tomada de decisão ou de ato administrativo, a exemplo de pareceres e notas técnicas;

DOMÍNIO CIBERNÉTICO - domínio de processamento de informações (dados) eletrônicas, composto de uma ou mais infraestruturas de tecnologia da informação;

DoS - sigla de negação de serviço (denial of service);

Letra E

E-MAIL - sigla de correio eletrônico (electronic mail);

ECOSSISTEMA CIBERNÉTICO - infraestrutura de informação interconectada de interações entre pessoas, processos, dados e tecnologias da informação, juntamente com o ambiente e as condições que influenciam essas interações. Engloba diversos participantes - governo, firmas privadas, organizações não-governamentais, indivíduos, processos e dispositivos cibernéticos - que interagem com propósitos diversos;

ELIMINAÇÃO - exclusão de dado ou conjunto de dados, armazenados em banco de dados, independentemente do procedimento empregado;

EMIÇÃO DE ALERTAS E ADVERTÊNCIAS - serviço que consiste em divulgar alertas ou advertências imediatas, como uma reação diante de um incidente de segurança em redes de computadores, com o objetivo de advertir a comunidade ou dar orientações sobre como a comunidade deve agir diante do problema;



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

EMPRESA ESTRATÉGICA DE DEFESA (EED) DO SETOR DE TECNOLOGIA DE INFORMAÇÃO - toda pessoa jurídica do setor de tecnologia da informação, devidamente credenciada pelo Ministério da Defesa, mediante o atendimento cumulativo das condições previstas no art. 2º, inciso IV, da Lei nº 12.598, de 22 de março de 2012;

ENCARREGADO - pessoa indicada pelo controlador, para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

ENDEREÇO IP - conjunto de elementos numéricos ou alfanuméricos, que identifica um dispositivo eletrônico em uma rede de computadores. Sequência de números associada a cada computador conectado à Internet. No caso de IPv4, o endereço IP é dividido em quatro grupos, separados por "." e compostos por números entre 0 e 255. No caso de IPv6, o endereço IP é dividido em até oito grupos, separados por ":" e compostos por números hexadecimais (números e letras de "A" a "F") entre 0 e FFFF;

ENGENHARIA SOCIAL - técnica por meio da qual uma pessoa procura persuadir outra a executar determinadas ações. No contexto da segurança da informação, é considerada uma prática de má-fé para tentar explorar a boa-fé ou abusar da ingenuidade e da confiança de indivíduos, a fim de aplicar golpes, ludibriar ou obter informações sigilosas e importantes;

EQUIPE DE COORDENAÇÃO SETORIAL - equipe de prevenção, tratamento e resposta a incidentes cibernéticos das agências reguladoras, do Banco Central do Brasil ou da Comissão Nacional de Energia Nuclear ou das suas entidades reguladas responsáveis por coordenar as atividades de segurança cibernética e de centralizar as notificações de incidentes das demais equipes do setor regulado;

EQUIPE DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS (ETIR) - grupo de agentes públicos com a responsabilidade de prestar serviços relacionados à segurança cibernética para o órgão ou a entidade da administração pública federal, em observância à política de segurança da informação e aos processos de gestão de riscos de segurança da informação do órgão ou da entidade. Anteriormente era chamada de Equipe de Tratamento de Incidentes de Rede;

EQUIPE DE TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS (ETIR) - termo alterado pelo Decreto nº 10.641, de 2 de março de 2021, para denominação Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos;

**SERVIÇO PÚBLICO FEDERAL**

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

EQUIPES PRINCIPAIS - equipes de prevenção, tratamento e resposta a incidentes cibernéticos de entidades, públicas ou privadas, responsáveis por ativos de informação, em especial aqueles relativos a serviços essenciais, cuja interrupção ou destruição, total ou parcial, provoque sério impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade, nos termos do disposto no parágrafo único, inciso I, do art. 1º do Anexo ao Decreto nº 9.573, de 22 de novembro de 2018;

ESFERA DE INFORMAÇÃO - ambiente em que a informação existe e flui de forma estruturada ou randômica, e em que fatos ou conhecimentos residem e são representados ou transmitidos por uma sequência particular de símbolos, impulsos ou caracterizações;

ESPAÇO CIBERNÉTICO - espaço virtual composto por um conjunto de canais de comunicação da Internet e outras redes de comunicação, que garantem a interconexão de dispositivos de tecnologia da informação. Engloba todas as formas de atividades digitais em rede, incluindo o armazenamento, processamento e compartilhamento de conteúdo, além de todas as ações, humanas ou automatizadas, conduzidas por meio desse ambiente;

ESPAÇO DE INFORMAÇÃO - qualquer meio em que a informação possa ser criada, transmitida, recebida, armazenada, processada ou descartada;

ESPALHAMENTO (HASHING) - tabela de espalhamento (hashing) que associa uma chave a um endereço. Esse endereço é usado como base para armazenamento e para recuperação de registros, sendo bastante similar à indexação, pois associa a chave ao endereço relativo a um registro. No espalhamento, os endereços parecem aleatórios, não existindo conexão óbvia entre a chave e o endereço;

ESPIONAGEM CIBERNÉTICA - atividade que consiste em ataques cibernéticos dirigidos contra a confidencialidade de sistemas de tecnologia da informação, com o objetivo de obter dados e informações sensíveis a respeito de planos e atividades de um governo, instituição, empresa ou pessoa física, sendo geralmente lançados e gerenciados por serviços de inteligência estrangeiros ou por empresas concorrentes;

ESTIMATIVA DE RISCOS - processo utilizado para atribuir valores à probabilidade e às consequências de um risco;

ESTRATÉGIA DE CONTINUIDADE DE NEGÓCIOS - abordagem de um órgão ou entidade que garante a recuperação dos ativos da informação e a continuidade das atividades críticas ao se confrontar com um desastre, uma interrupção ou com outro incidente maior;



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

ETIR - sigla de Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos;

EVENTO - qualquer mudança de estado que tem importância para a gestão de um item de configuração ou serviço de tecnologia da informação. Em outras palavras, qualquer ocorrência dentro do escopo de tecnologia da informação que tenha relevância para a gestão dos serviços entregues ao cliente;

EVENTO DE SEGURANÇA - qualquer ocorrência identificada em um sistema, serviço ou rede, que indique uma possível falha da política de segurança, falha das salvaguardas ou mesmo uma situação até então desconhecida, que possa se tornar relevante em termos de segurança;

EVIDÊNCIA DIGITAL - informação ou dado, armazenado ou transmitido eletronicamente, em modo binário, que pode ser reconhecida como parte de um evento;

EVITAR O RISCO - forma de tratamento de risco, na qual a alta administração decide não realizar a atividade, não se envolver ou não agir, a fim de se retirar de uma situação de risco;

EXCLUSÃO DE ACESSO - processo que tem por finalidade suspender definitivamente o acesso, incluindo o cancelamento do código de identificação e de perfil de acesso;

EXFILTRAÇÃO DE DADOS - movimento não autorizado de dados, também chamado de dataexfil, exportação de dados, extrusão de dados, vazamento de dados e roubo de dados;

EXFIL- vide exfiltração de dados;

EXPLOIT- técnicas, programas ou parte de programas maliciosos, projetados para explorar uma vulnerabilidade existente em um programa de computador. Entre os tipos mais comuns de exploits estão o SQL injection, o cross-site scripting, o abuso de configuração de autenticação fraca e o abuso de falhas de configuração de segurança;

EXPLORAÇÃO DE DIA ZERO - ataque digital que faz uso das "Vulnerabilidades de Dia Zero" para instalar software malicioso em um aparelho. É considerada uma ameaça grave, pois é impossível reconhecê-la, uma vez que a falha não é conhecida. Ela pode ser mitigada e algumas vezes



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

evitada por meio de ferramentas de segurança que monitorem o comportamento do tráfego e o acesso aos equipamentos para identificar atividades suspeitas ou maliciosas;

Letra F

FEDERAL INFORMATION PROCESSING STANDARD 140-2(FIPS 140-2) - norma do governo dos Estados Unidos que especifica a criptografia e os requisitos de segurança necessários para produtos de tecnologia da informação para uso de caráter sensível. Também especifica como indivíduos ou outros processos devem ser autorizados para utilizar o produto, e como módulos ou componentes devem ser concebidos para interagir de forma segura com outros sistemas. Essa padronização garante que um produto utilize sólidas práticas de segurança, como métodos e algoritmos de criptografia fortes e aprovados;

FIDC - sigla de formulário individual de dados para credenciamento;

FIPS 140-2 - sigla de federal information processing standard140-2;

FIREWALL- ferramenta para evitar acesso não autorizado, tanto na origem quanto no destino, a uma ou mais redes. Podem ser implementados por meio de hardware ou software, ou por meio de ambos. Cada mensagem que entra ou sai da rede passa pelo firewall, que a examina a fim de determinar se atende ou não os critérios de segurança especificados;

FORENSE DIGITAL - aplicação de procedimentos digitais investigativos para a identificação, exame e análise de dados, com a devida preservação da integridade da informação e mantendo uma estrita cadeia de custódia para os dados;

FORMULÁRIO INDIVIDUAL DE DADOS PARA CREDENCIAMENTO (FDIC) - formulário de preenchimento obrigatório para que pessoa natural seja submetida a processo de credenciamento de segurança;

FUNÇÃO DE RESUMO CRIPTOGRÁFICO - vide resumo criptográfico;

Letra G



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

GAN - sigla de redes contraditórias generativas (generative adversarial networks);

GASTOS-DUPLOS - ato de usar o mesmo dado mais de uma vez em diferentes transações em uma rede blockchain;

GESTÃO DE CONTINUIDADE DE NEGÓCIOS EM SEGURANÇA DA INFORMAÇÃO - processo que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Esse processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação, a marca da organização e suas atividades de valor agregado;

GESTÃO DE INCIDENTES CIBERNÉTICOS - processo que realiza ações sobre qualquer evento adverso relacionado à segurança cibernética dos sistemas ou da infraestrutura de computação;

GESTÃO DE MUDANÇAS NOS ASPECTOS RELATIVOS À SEGURANÇA DA INFORMAÇÃO - processo estruturado que visa aumentar a probabilidade de sucesso em mudanças, com mínimos impactos, e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação;

GESTÃO DE RISCOS EM SEGURANÇA DA INFORMAÇÃO - processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificação, avaliação e gerenciamento de potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos;

GESTÃO DE SEGURANÇA DA INFORMAÇÃO - processo que visa integrar atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e organizacional, aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação;

GESTOR DE MUDANÇAS - responsável pelo planejamento e implementação do processo de gestão de mudanças no âmbito do órgão ou entidade da administração pública federal;

GESTOR DE SEGURANÇA DA INFORMAÇÃO - responsável pelas ações de segurança da informação no âmbito do órgão ou entidade da administração pública federal;



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

GESTOR DE SEGURANÇA E CREDENCIAMENTO (GSC) - responsável pela segurança da informação classificada, em qualquer grau de sigilo, nos órgãos de registro e postos de controle;

GSI/PR - sigla de Gabinete de Segurança Institucional da Presidência da República;

GSC - sigla de gestor de segurança e credenciamento;

GUERRA CIBERNÉTICA - atos de guerra, utilizando predominantemente elementos de tecnologia da informação em escala suficiente, por um período específico de tempo e em alta velocidade, em apoio às operações militares, por meio de ações tomadas exclusivamente no espaço cibernético, com a finalidade de abalar ou de incapacitar as atividades de uma nação inimiga, especialmente pelo ataque aos sistemas de comunicação, visando obter vantagem operacional militar significativa. Tais ações são consideradas uma ameaça à Segurança Nacional do Estado;

Letra H

HABILITAÇÃO DE SEGURANÇA - condição atribuída a um órgão ou a uma entidade, pública ou privada, que lhe confere a aptidão para o tratamento da informação classificada em determinado grau de sigilo;

HARDENING- vide blindagem;

HASH- resultado único e de tamanho fixo, gerado por uma função de resumo. O hash pode ser utilizado, entre outras possibilidades, para verificar a integridade de arquivos e gerar assinaturas digitais. Ele é gerado de forma que não é possível realizar o processamento inverso para recuperação da informação original. Além disso, qualquer alteração na informação original produzirá um hash distinto. Apesar de ser teoricamente possível que informações diferentes gerem hashes iguais, a probabilidade de isso ocorrer é bastante baixa;

HIPÓTESE LEGAL DE SIGILO - quando uma informação sigilosa é definida por lei específica, diversa da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação);

HONEYNET- ferramenta de pesquisa, que consiste em uma rede projetada especificamente para ser comprometida, e que contém mecanismos de controle para prevenir que seja utilizada como



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

base de ataques contra outras redes. Trata-se de um tipo de honeypot de alta interatividade, projetado para pesquisa e obtenção de informações dos invasores, também conhecido como honeypot de pesquisa;

HONEYPOT- recurso computacional de segurança dedicado a ser sondado, atacado ou comprometido. Existem dois tipos de honeypots: os de baixa interatividade e os de alta interatividade. Em um honeypot de baixa interatividade são instaladas ferramentas para emular sistemas operacionais e serviços com os quais os atacantes irão interagir; desta forma, o sistema operacional real deste tipo de honeypot deve ser instalado e configurado de modo seguro, para minimizar o risco de comprometimento. Nos honeypots de alta interatividade, os atacantes interagem com sistemas operacionais, aplicações e serviços reais;

HSM - sigla de módulo de segurança em hardware (hardware security module);

HSTS - sigla de HTTP strict transport security;

HTTP - sigla de hypertext transfer protocol;

HTTPS - sigla de hypertext transfer protocol secure;

HTTPSTRICT TRANSPORT SECURITY(HSTS) - mecanismo de política de segurança web que ajuda a proteger websites contra os ataques do tipo degradação de protocolo e sequestro de cookies. Ele permite que os servidores web determinem que os browsers (ou outros mecanismos de acesso) devem interagir com eles, utilizando apenas conexões seguras HTTPS. O HSTS é um padrão IETF e está especificado na RFC 6797;

HYPERTEXT TRANSFER PROTOCOL(HTTP) - protocolo de comunicação entre sistemas de informação, o qual permite a transferência de dados entre redes de computadores, principalmente na World Wide Web (Internet). Para que esta transferência de dados ocorra, o protocolo HTTP necessita estar agregado a outros dois protocolos de rede, TCP e IP, os quais possibilitam a comunicação entre a URL e o servidor web que armazenará os dados, a fim de que a página HTML solicitada pelo usuário seja enviada;

HYPERTEXT TRANSFER PROTOCOL SECURE(HTTPS) - extensão do HTTP, utilizado para comunicação segura pela rede de computadores. No HTTPS o protocolo de comunicação é criptografado usando o TLS ou o seu predecessor, o SSL. A principal motivação para o uso do



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

HTTPS é a autenticação do site acessado e a proteção da privacidade e integridade dos dados trocados durante o tráfego de informações;

HYPERVISOR- também conhecido como monitor de máquina virtual, é um software, firmware ou hardware que cria e roda máquinas virtuais;

Letra I

IaaS - sigla de infraestrutura como código (infrastructure as a code);

IaaS - sigla de infraestrutura como serviço (infrastructure as a service);

IaC-sigla de infraestrutura como código (infrastructure as code);

IBE - sigla de criptografia baseada em identidade (identity-based encryption);

ICP-Brasil - sigla de infraestrutura de chaves públicas brasileira;

IDENTIDADE DIGITAL - representação unívoca de um indivíduo dentro do espaço cibernético;

IDENTIDADE FEDERADA - modelo federado está fundamentado sobre a distribuição da tarefa de autenticação dos usuários por múltiplos provedores de identidade, estando esses dispostos em diferentes domínios administrativos, tais como empresas, governos e academia. Em cada domínio administrativo há diversos usuários, um único provedor de identidade e vários provedores de serviços, sendo que os provedores de identidade estabelecem relações de confiança, de forma que uma identidade emitida por um provedor de identidade de um determinado domínio seja reconhecida por provedores de serviços de outros domínios;

IDENTIDADE SINTÉTICA - tipo de fraude de identidade na qual os golpistas usam uma mistura de credenciais reais e fabricadas, para criar a ilusão de uma pessoa real. É bastante popular, pois os criminosos podem facilmente criar identidades sintéticas com apenas alguns dados verdadeiros (como nome e número de um documento de identificação), sendo normalmente utilizada com o objetivo de abrir contas fraudulentas e realizar aquisições;



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

IDENTIFICAÇÃO DE RISCOS - processo de localizar, listar e caracterizar elementos de risco;

IDENTITY-BASED ENCRYPTION(IBE) - vide criptografia baseada na identidade;

IDS - sigla de sistema de detecção de intrusão (intrusion detection system);

IMAGEM DE MÁQUINA VIRTUAL - abrange a definição completa do armazenamento de uma máquina virtual, contendo o disco do sistema operacional e todos os discos de dados, capturando as propriedades do disco (como cache de host) necessárias para implantar uma Virtual Machine em uma unidade reutilizável;

INCIDENTE - interrupção não planejada ou redução da qualidade de um serviço, ou seja, ocorrência, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

INCIDENTE CIBERNÉTICO - ocorrência que pode comprometer, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema. Poderá também ser caracterizada pela tentativa de exploração de vulnerabilidade de sistema de informação que caracterize violação de norma, política de segurança, procedimento de segurança ou política de uso. De maneira geral, os tipos de atividade comumente reconhecidas como incidentes cibernéticos são: a) tentativas de obter acesso não-autorizado a um sistema ou a dados armazenados; b) tentativa de utilização não-autorizada de sistemas para a realização de atividades de processamento ou armazenamento de dados; c) mudanças não-autorizadas de firmware, hardware ou software em um ambiente computacional; d) ataques de negação de serviço (DoS); e e) demais ações que visem afetar a disponibilidade ou integridade dos dados. Um incidente de segurança cibernética não significa necessariamente que as informações já estão comprometidas; significa apenas que a informação está ameaçada;

INCIDENTE DE SEGURANÇA - qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

INFORMAÇÃO - dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

INFORMAÇÃO ATUALIZADA - informação que reúne os dados mais recentes sobre o tema, de acordo com sua natureza, com os prazos previstos em normas específicas ou conforme a periodicidade estabelecida nos sistemas informatizados que a organizam;

INFORMAÇÃO CLASSIFICADA EM GRAU DE SIGILO: informação sigilosa em poder dos órgãos e entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, a qual é classificada como ultrassecreta, secreta ou reservada;

INFORMAÇÃO PESSOAL - informação relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem;

INFORMAÇÃO SIGILOSA - informação submetida temporariamente à restrição de acesso público, em razão de sua imprescindibilidade para a segurança da sociedade e do Estado; e aquela abrangida pelas demais hipóteses legais de sigilo;

INFORMAÇÃO SIGILOSA CLASSIFICADA - vide informação classificada;

INFORMAÇÃO SIGILOSA PROTEGIDA POR LEGISLAÇÃO ESPECÍFICA - informação amparada pelo sigilo bancário, fiscal, comercial, profissional ou segredo de justiça (lista com exemplos encontra-se no ANEXO A do Glossário);

INFRAESTRUTURA CIBERNÉTICA - sistemas e serviços de informação compostos por todo hardware e software necessários para processar, armazenar e transmitir a informação, ou qualquer combinação desses elementos. O processamento inclui criação, acesso, modificação e destruição da informação. O armazenamento engloba qualquer tipo de mídia na qual a informação esteja armazenada. A transmissão é composta tanto pela distribuição como pelo compartilhamento da informação, por qualquer meio;

INFRAESTRUTURA COMO CÓDIGO (IaC) - processo de gerenciamento e provisionamento de data centers de computador, por meio de arquivos de definição legíveis por máquina, em vez de configuração física de hardware ou ferramentas de configuração interativas;

INFRAESTRUTURA COMO SERVIÇO (IaaS) - tipo de serviço de computação em nuvem onde o provedor de serviço de nuvem oferece ao cliente a capacidade de criar redes virtuais em seu ambiente de computação. Uma solução IaaS permite que o cliente selecione quais sistemas

**SERVIÇO PÚBLICO FEDERAL**

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

operacionais instalar em máquinas virtuais, bem como a estrutura da rede, incluindo o uso de switches virtuais, roteadores e firewalls. O IaaS também fornece total liberdade quanto ao software ou código personalizado executado nas máquinas virtuais. Uma solução IaaS é a mais flexível de todos os serviços de computação em nuvem; permite uma redução significativa do hardware pelo cliente em sua própria instalação local. Geralmente, é a forma mais cara de serviço de computação em nuvem;

INFRAESTRUTURA CRÍTICA - instalações, serviços, bens e sistemas, virtuais ou físicos, que se forem incapacitados, destruídos ou tiverem desempenho extremamente degradado, provocarão sério impacto social, econômico, político, internacional ou à segurança;

INFRAESTRUTURA CRÍTICA DE INFORMAÇÃO - sistemas de tecnologia da informação que suportam ativos e serviços chaves da infraestrutura nacional crítica;

INFRAESTRUTURA DE CHAVE PÚBLICA (PKI) - sistema de recursos, políticas e serviços que suportam a utilização de criptografia de chave pública para autenticar as partes envolvidas na transação. Não há um único padrão que define os componentes de uma infraestrutura de chave pública, mas uma infraestrutura de chave pública geralmente inclui autoridades certificadoras e autoridades de registro. O padrão ITU-T X.509 fornece a base para a infraestrutura de chave pública padrão de mercado;

INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA (ICP-BRASIL) - cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais, para identificação virtual do cidadão. Essa infraestrutura é um conjunto elaborado de práticas, técnicas e procedimentos, que serve para suportar um sistema criptográfico baseado em certificados digitais. O modelo adotado no Brasil para a infraestrutura de chaves públicas é chamado de certificação com raiz única, em que existe uma autoridade certificadora raiz (AC-Raiz). Além de desempenhar esse papel, a AC-Raiz credencia os demais participantes da cadeia, além de supervisionar e auditar os processos. Foi criada pela Medida Provisória Nº 2.200-2, de 24 de agosto de 2001, e está regulamentada pelas resoluções do Comitê-Gestor da ICP-Brasil;

INFRAESTRUTURA NACIONAL CRÍTICA - ativos, virtuais ou físicos, que são essenciais para o devido funcionamento da sociedade e da economia nacional (como energia, transporte, saúde, telecomunicações, entre outros);

INSPEÇÃO PARA HABILITAÇÃO DE SEGURANÇA - verificação da existência dos requisitos indispensáveis à habilitação de segurança de órgãos e entidades para o tratamento de informação classificada;



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

INTEGRIDADE - propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

INTERFACE DE PROGRAMAÇÃO DE APLICAÇÕES (API) - tem por objetivo disponibilizar recursos de uma aplicação para serem usados por outra aplicação, abstraindo os detalhes da implementação e, muitas vezes, restringindo o acesso a esses recursos com regras específicas para tal;

INTERNET - rede global, composta pela interligação de inúmeras redes. Conecta mais de 500 milhões de usuários, provendo comunicação e informações das mais variadas áreas de conhecimento;

INTERNET DAS COISAS (IoT) - infraestrutura que integra a prestação de serviços de valor adicionado com capacidades de conexão física ou virtual de coisas, com dispositivos baseados em tecnologias da informação existentes e nas suas evoluções, com interoperabilidade, conforme disposto no Decreto nº 9.854, de 25 de junho de 2019, que institui o Plano Nacional de Internet das Coisas;

INTERNETPROTOCOL(IP) - protocolo que permite o endereçamento e o transporte de pacotes de dados (datagramas) na Internet, sem, contudo, assegurar que estes pacotes sejam entregues;

INTEROPERABILIDADE - característica que se refere à capacidade de diversos sistemas e organizações trabalharem em conjunto (interoperar), de modo a garantir que pessoas, organizações e sistemas computacionais interajam para trocar informações de maneira eficaz e eficiente;

INTRANET - rede privada, acessível apenas aos membros da organização a que atende. Utiliza os mesmos recursos e protocolos da Internet, mas é comumente separada desta, por meio de firewalls;

INVASÃO - incidente de segurança no qual o ataque foi bem-sucedido, resultando no acesso, na manipulação ou na destruição de informações em um computador ou em um sistema da organização;



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

INVESTIGAÇÃO PARA CREDENCIAMENTO DE SEGURANÇA - verificação da existência dos requisitos indispensáveis para a concessão da credencial de segurança a uma pessoa natural, a fim de realizar o tratamento de informação classificada;

IoT - sigla de Internet das coisas (Internet of things);

IP - sigla de Internet protocol;

Letra J

JAILBREAK- processo que modifica o sistema operacional original de um dispositivo, permitindo que ele execute aplicativos não-autorizados pelo fabricante. Um aparelho com um software do tipo jailbreak é capaz de instalar aplicativos anteriormente indisponíveis nos sites oficiais do fabricante, por meio de instaladores não-oficiais, assim como aplicações adquiridas de forma ilegal. O uso de técnicas jailbreak não é recomendado pelos fabricantes, já que permitem a execução de aplicativos não certificados, que podem inclusive conter malware embutidos;

Letra K

KEYLOGGER- tipo específico de spyware, com a capacidade de capturar e de armazenar as teclas digitadas pelo usuário no teclado do computador. Normalmente, a ativação do keylogger é condicionada a uma ação prévia do usuário, como o acesso a um site específico de comércio eletrônico ou de Internet banking;

KIT DE DESENVOLVIMENTO DE SOFTWARE (SDK) - conjunto de ferramentas de desenvolvimento e de códigos pré-gravados, que podem ser usados pelos desenvolvedores para criar aplicativos. Geralmente, ajudam a reduzir a quantidade de esforço e de tempo que seria necessário para os profissionais escreverem seus próprios códigos;

Letra L

LAI - sigla de Lei de Acesso a Informação;

LGPD - sigla de Lei Geral de Proteção de Dados Pessoais;



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

LISTA DE CONTROLE DE ACESSO (ACL) - mecanismo que implementa o controle de acesso para um recurso, enumerando as entidades do sistema que possuem permissão para acessar o recurso e definindo, explicita ou implicitamente, os modos de acesso concedidos à cada entidade;

LIVRO RAZÃO DISTRIBUÍDO (DLT) - banco de dados distribuído por vários nós ou dispositivos de computação. Cada nó replica e salva uma cópia idêntica do livro-razão. Cada nó participante da rede atualiza-se de forma independente. O recurso inovador da tecnologia de contabilidade distribuída é que a planilha não é mantida por nenhuma autoridade central. Atualizações para o livro-razão são independentemente construídas e registradas por cada nó. Os nós então votam nessas atualizações, para garantir que a maioria concorde com a conclusão alcançada. Um sistema blockchain é uma forma de tecnologia de contabilidade distribuída. No entanto, a estrutura do sistema blockchain é distinta de outros tipos de livro-razão distribuídos, pois os dados em um sistema blockchain são agrupados e organizados em blocos, que são então ligados entre si e protegidos usando criptografia;

LISTA DE BLOQUEIO – vide blacklist;

LOG (REGISTRO DE AUDITORIA) - registro de eventos relevantes em um dispositivo ou sistema computacional;

Letra M

MALWARE-software malicioso, projetado para infiltrar um sistema computacional, com a intenção de roubar dados ou danificar aplicativos ou o sistema operacional. Esse tipo de software costuma entrar em uma rede por meio de diversas atividades aprovadas pela empresa, como e-mail ou sites. Entre os exemplos de malware estão os vírus, worms, trojans (ou cavalos de Troia), spyware, adware e rootkits;

MÁQUINA VIRTUAL (VM) - as máquinas virtuais são computadores de software, com a mesma funcionalidade que os computadores físicos. Assim como os computadores físicos, elas executam aplicativos e um sistema operacional. No entanto, as máquinas virtuais são arquivos de computador, executados em um computador físico, e se comportam como um computador físico. Geralmente, são criadas para tarefas específicas, cujas execuções são arriscadas em um ambiente host, como por exemplo, o acesso a dados infectados por vírus e a testes de sistemas operacionais. Como a máquina virtual é separada por sandbox do restante do sistema, o



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

software dentro dela não pode adulterar o computador host. As máquinas virtuais também podem ser usadas para outras finalidades, como a virtualização de servidores;

MÁQUINA VIRTUAL CONFIÁVEL (TVM) - instância de uma máquina virtual (VM), que apresenta as seguintes características: a) máquinas virtuais devem ser lançadas em servidores com integridade de inicialização comprovável; b) imagens de máquinas virtuais devem ser criptografadas em trânsito, em repouso e durante a execução. Isso é essencial para preservar a confidencialidade e o sigilo. As chaves estão sob o controle do cliente e só são disponibilizadas (política de gerenciamento de chaves) para o provedor de serviços, quando ele atesta que as imagens da máquina virtual estão sendo lançadas em servidores confiáveis; c) apenas imagens de máquinas virtuais qualificadas e atestadas podem ser lançadas e provisionadas, sendo o provedor de serviço responsável por atestar a integridade de lançamento na infraestrutura;

MARCAÇÃO - aposição de marca que indica o grau de sigilo da informação classificada;

MATERIAL DE ACESSO RESTRITO - qualquer matéria, produto, substância ou sistema que contenha, utilize ou veicule conhecimento ou informação classificada, em qualquer grau de sigilo, informação econômica ou informação científico-tecnológica, cuja divulgação implique risco ou dano aos interesses da sociedade e do Estado, tendo seu acesso restrito às pessoas autorizadas pelo órgão ou entidade;

MATRIZ RACI - também conhecida como tabela RACI, trata-se de uma ferramenta visual, que define com clareza as atribuições, papéis e responsabilidades de cada colaborador nas atividades de um processo. A sigla RACI representa responsible (responsável), accountable (aprovador), consulted (consultado) e informed (informado);

MEDIDAS DE SEGURANÇA - medidas destinadas a garantir sigilo, inviolabilidade, integridade, autenticidade e disponibilidade da informação classificada em qualquer grau de sigilo;

METADADOS - representam "dados sobre dados", fornecendo os recursos necessários para entender os dados no decorrer do tempo, ou seja, são dados estruturados que fornecem uma descrição concisa a respeito dos dados armazenados e que permitem encontrar, gerenciar, compreender ou preservar informações a respeito dos dados ao longo do tempo. Possuem um papel importante na gestão de dados, pois, a partir deles, as informações são processadas, atualizadas e consultadas. As informações de como os dados foram criados ou derivados, do ambiente em que residem ou residiram, das alterações realizadas, dentre outras, são obtidas de metadados;



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

MFA - sigla de autenticação de multifatores (multifactor authentication);

MÍDIA - mecanismos em que dados podem ser armazenados. Além da forma e da tecnologia utilizada para a comunicação, inclui discos ópticos, magnéticos, compact disk(CD), fitas, papel, entre outros. Um recurso multimídia combina sons, imagens e vídeos;

MODELO DE CONSENSO - componente primário de sistemas distribuídos de blockchain e, definitivamente, um dos mais importantes para a sua funcionalidade. Trata-se da base sobre a qual os usuários podem interagir uns com os outros de maneira trustless. A maioria dos sistemas blockchain públicos utiliza o Consenso de Nakamoto;

MODELO DE IMPLEMENTAÇÃO DE NUVEM PRÓPRIA - solução compartilhada de recursos computacionais configuráveis, cuja infraestrutura de nuvem pertence apenas a uma organização e suas subsidiárias;

MODELO DE IMPLEMENTAÇÃO DE NUVEM COMUNITÁRIA - solução compartilhada de recursos computacionais configuráveis, cuja infraestrutura de nuvem é compartilhada entre diversas organizações que possuem necessidades comuns, tais como missão, valores, requisitos de segurança, política e requisitos legais, entre outras;

MÓDULO DE SEGURANÇA EM HARDWARE (HSM) - criptoprocessador dedicado, especificamente projetado para a proteção do ciclo de vida de uma chave criptográfica. Um HSM age como âncora segura, que protege a infraestrutura criptográfica gerenciando, processando e armazenando chaves criptográficas em um ambiente seguro e resistente a adulterações;

MULTI-NUVEM - estratégia de utilização dos serviços de computação em nuvem por meio de dois ou mais provedor de serviço de nuvem;

Letra N

NECESSIDADE DE CONHECER - condição segundo a qual o conhecimento da informação classificada é indispensável para o adequado exercício de cargo, função, emprego ou atividade. O termo "necessidade de conhecer" descreve a restrição de dados que sejam considerados extremamente sigilosos. Sob restrições do tipo necessidade de conhecer, mesmo que um indivíduo tenha as credenciais necessárias para acessar uma determinada informação, ele só

**SERVIÇO PÚBLICO FEDERAL**

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

terá acesso a essa informação caso ela seja estritamente necessária para a condução de suas atividades oficiais;

NEGAÇÃO DE SERVIÇO (DoS) - bloqueio de acesso devidamente autorizado a um recurso ou a geração de atraso nas operações e funções normais de um sistema, com a resultante perda da disponibilidade aos usuários autorizados. O objetivo do ataque DoS é interromper atividades legítimas de um computador ou de um sistema. Uma forma de provocar o ataque é aproveitando-se de falhas ou de vulnerabilidades presentes na máquina vítima, ou enviar um grande número de mensagens que esgotem algum dos recursos da vítima, como CPU, memória, banda, entre outros. Para isto, é necessária uma única máquina poderosa, com bom processamento e bastante banda disponível, capaz de gerar o número de mensagens suficiente para causar a interrupção do serviço;

NEGAÇÃO DE SERVIÇO DISTRIBUÍDA (DDoS) - atividade maliciosa, coordenada e distribuída, em que um conjunto de computadores ou de dispositivos móveis é utilizado para tirar de operação um serviço, um computador ou uma rede conectada à Internet. Embora os ataques do tipo DoS sejam, em geral, perigosos para os serviços de Internet, a forma distribuída é ainda mais perigosa, justamente por se tratar de um ataque feito por várias máquinas, que podem estar espalhadas geograficamente e não terem nenhuma relação entre si, exceto o fato de estarem parcial ou totalmente sob controle do atacante. Além disso, mensagens DDoS podem ser difíceis de identificar por conseguirem facilmente se passar por mensagens de tráfego legítimo, pois enquanto é pouco natural que uma mesma máquina envie várias mensagens semelhantes a um servidor em períodos muito curtos de tempo, como no caso do ataque DoS, é perfeitamente natural que várias máquinas enviem mensagens semelhantes de requisição de serviço regularmente a um mesmo servidor, o que disfarça o ataque DDoS;

NÍVEIS DE ACESSO - especificam quanto de cada recurso ou sistema o usuário pode utilizar;

NOTIFICAÇÃO DE INCIDENTE - ato de informar eventos ou incidentes para uma Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) ou grupo de segurança;

NSC - sigla de Núcleo de Segurança e Credenciamento;

NÚCLEO DE SEGURANÇA E CREDENCIAMENTO (NSC) - órgão de registro central, instituído no Gabinete de Segurança Institucional da Presidência da República;

**SERVIÇO PÚBLICO FEDERAL**

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

NÚMERO DE IDENTIFICAÇÃO PESSOAL (PIN) - número exclusivo, conhecido somente pelo usuário e pelo sistema, para a autenticação do usuário no sistema. PINs comuns são usados em caixas automáticos para realização de transações bancárias e em chips telefônicos;

NUVEM COMUNITÁRIA - infraestrutura de nuvem dedicada para uso exclusivo de uma comunidade, ou de um grupo de usuários de órgãos ou de entidades não vinculados, que compartilham a mesma natureza de trabalho e obrigações, e sua propriedade e seu gerenciamento podem ser de organizações da comunidade, de terceiros ou de ambos;

NUVEM HÍBRIDA - infraestrutura de nuvem composta por duas ou mais infraestruturas distintas (privadas, comunitárias ou públicas), que permanecem com suas próprias características, mas agrupadas por tecnologia padrão que permite interoperabilidade e portabilidade de dados, serviços e aplicações;

NUVEM PRIVADA (OU INTERNA) - infraestrutura de nuvem dedicada para uso exclusivo do órgão e de suas unidades vinculadas, ou de entidade composta por múltiplos usuários, e sua propriedade e seu gerenciamento podem ser da própria organização, de terceiros ou de ambos;

NUVEM PÚBLICA (OU EXTERNA) - infraestrutura de nuvem dedicada para uso aberto de qualquer organização, e sua propriedade e seu gerenciamento podem ser de organizações públicas, privadas ou de ambas;

Letra O

OBSOLESCÊNCIA TECNOLÓGICA - ciclo de vida do software ou de equipamento, definido pelo fabricante ou causado pelo desenvolvimento de novas tecnologias;

ONE-TIME PASSWORD- vide senha descartável;

OPEN WEB APPLICATION SECURITY PROJECT(OWASP) - trata-se de uma comunidade on-line que cria e disponibiliza, de forma gratuita, artigos, metodologias, documentação, ferramentas e tecnologias no campo da segurança de aplicações web, a todos os interessados em aperfeiçoar a segurança em aplicações;



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

OPERADOR - pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

OPT-IN- processo em que o usuário autoriza uma determinada ação por parte de uma empresa. Geralmente, a coleta de dados e o seu compartilhamento com empresas parceiras ou o recebimento de mensagens enviadas por empresas;

OPT-OUT- processo em que o usuário desautoriza uma empresa a continuar com uma determinada ação previamente permitida;

ÓRGÃO DE PESQUISA - órgão ou entidade da administração pública, direta ou indireta, ou pessoa jurídica de direito privado sem fins lucrativos, legalmente constituída sob as leis brasileiras, com sede e foro no país, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico;

ÓRGÃOS DE REGISTRO - órgão ou entidade pública da administração pública federal habilitada para o tratamento de informação classificada;

ÓRGÃOS DE REGISTRO NÍVEL 1 - os Ministérios e os órgãos e entidades públicas de nível equivalente, habilitados pelo Núcleo de Segurança e Credenciamento (NSC);

ÓRGÃOS DE REGISTRO NÍVEL 2 - os órgãos ou entidade pública vinculada a um órgão de Registro Nível 1 e por este habilitado;

ÓRGÃO GESTOR DE SEGURANÇA DA INFORMAÇÃO - órgão ao qual foi atribuída a competência legal para atuar no planejamento das ações de segurança da informação a serem implementadas, considerando requisitos ou pressupostos estabelecidos pela administração pública federal, bem como o acompanhamento da evolução da maturidade de segurança da informação;

ORN1 - sigla de órgão de registro nível 1;

ORN2 - sigla de órgão de registro nível 2;



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

OWASP - sigla de open web application security project;

Letra P

PaaS - sigla de plataforma como serviço (platform as a service);

PADRÕES CORPORATIVOS DE SISTEMAS E DE CONTROLE - conjunto de regras e de procedimentos que compõem os normativos internos das corporações;

PC - sigla de posto de controle;

PENTEST- acrônimo de teste de penetração (penetration test);

PERFIL DE ACESSO - conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;

PERFIL INSTITUCIONAL - cadastro do órgão ou entidade da administração pública federal como usuário em redes sociais, alinhado ao planejamento estratégico e à Política de Segurança da Informação da instituição, com observância de sua correlata atribuição e competência;

PIN - sigla de número de identificação pessoal (personal identification number);

PKI - sigla de infraestrutura de chave pública (public key infrastructure);

PLANO DE CONTINUIDADE DE NEGÓCIOS EM SEGURANÇA DA INFORMAÇÃO - documentação dos procedimentos e das informações necessárias para que os órgãos ou entidades da administração pública federal mantenham seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo, em um nível previamente definido, em caso de incidente;

PLANO DE GESTÃO DE INCIDENTES - plano de ação claramente definido e documentado, para ser usado em caso de incidente que basicamente englobe os principais recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de incidentes;

**SERVIÇO PÚBLICO FEDERAL**

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

PLANO DE GESTÃO DE INCIDENTES CIBERNÉTICOS PARA A ADMINISTRAÇÃO PÚBLICA FEDERAL - plano que orienta as equipes dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional, exceto das agências reguladoras, do Banco Central do Brasil e da Comissão Nacional de Energia Nuclear, sobre a coordenação de atividades referentes à prevenção, ao tratamento e à resposta a incidentes cibernéticos;

PLANO DE GESTÃO DE RISCOS EM SEGURANÇA DA INFORMAÇÃO - documentação que compõe o processo de gestão de riscos de segurança da informação, que deve conter, pelo menos, a abrangência da aplicação da gestão de riscos, delimitando seu âmbito de atuação e os ativos de informação que serão objeto de tratamento; a metodologia a ser utilizada que deverá contemplar, no mínimo, critérios de avaliação e de aceitação de riscos; os tipos de riscos; o nível de severidade dos riscos; um modelo do relatório de identificação, análise e avaliação dos riscos de segurança da informação com as orientações necessárias para sua elaboração; e um modelo do relatório de tratamento de riscos de segurança da informação com as orientações necessárias para sua elaboração;

PLANO DE RECUPERAÇÃO DE NEGÓCIOS - documentação dos procedimentos e de informações necessárias para que o órgão ou entidade da administração pública federal operacionalize o retorno das atividades críticas à normalidade;

PLANO DE VERIFICAÇÃO DE CONFORMIDADE - documentação que compõe o processo de avaliação de conformidade nos aspectos de segurança da informação, que deve conter, pelo menos, as unidades a serem abrangidas; os aspectos a serem observados para verificação da conformidade; as ações e atividades a serem realizadas; os documentos necessários para fundamentar a verificação de conformidade; e as responsabilidades;

PLANOS SETORIAIS DE GESTÃO DE INCIDENTES CIBERNÉTICOS - planos que orientam as equipes nas agências reguladoras, no Banco Central do Brasil, na Comissão Nacional de Energia Nuclear ou nas suas entidades reguladas sobre a coordenação de atividades referentes à prevenção, ao tratamento e à resposta a incidentes cibernéticos inerentes ao setor específico;

PLATAFORMA COMO SERVIÇO (PaaS) - tipo de serviço de computação em nuvem, em que o provedor de serviço de nuvem oferece ao cliente a capacidade de operar códigos ou aplicativos personalizados. Um provedor PaaS determina quais sistemas operacionais ou ambientes de execução são oferecidos, não sendo permitido ao cliente modificar os sistemas operacionais (mesmo patches de segurança) ou alterar o espaço da rede virtual. A principal vantagem do PaaS é permitir ao cliente reduzir a implantação de hardware em sua própria instalação local e



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

aproveitar um modelo de computação sob demanda (no qual o cliente pagará apenas pelos recursos utilizados);

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - documento aprovado pela autoridade responsável pelo órgão ou entidade da administração pública federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação. Este termo substituiu o termo Política de Segurança da Informação e Comunicação;

POSIC - sigla de Política de Segurança da Informação e Comunicação. Substituído pela sigla **POSIN**;

POSIN - sigla de Política de Segurança da Informação. Substituiu a sigla **POSIC**;

PoS - sigla de Prova de Participação (proof of stake);

PoW - sigla de Prova de Trabalho (proof of work);

POSTO DE CONTROLE - unidade de órgão ou entidade pública ou privada, habilitada, responsável pelo armazenamento de informação classificada em qualquer grau de sigilo;

PRESERVAÇÃO DE EVIDÊNCIA DE INCIDENTES CIBERNÉTICOS - processo que compreende a salvaguarda das evidências e dos dispositivos, de modo a garantir que os dados ou metadados não sofram alteração, preservando-se a integridade e a confidencialidade das informações;

PRESTADOR DE SERVIÇO - pessoa envolvida com o desenvolvimento de atividades, de caráter temporário ou eventual, exclusivamente para o interesse do serviço, que poderão receber credencial especial de acesso;

PREVENÇÃO DE PERDA DE DADOS (DLP) - prática de detectar e prevenir vazamentos de dados, exfiltração de dados ou a destruição de dados sensíveis de uma organização. O termo DLP refere-se tanto a ações contra a perda de dados (evento no qual os dados são definitivamente perdidos pela organização), quanto a ações contra vazamentos de dados (transferência indevida de dados para fora da fronteira da organização);



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

PRIMARIEDADE - qualidade da informação coletada na fonte, com o máximo de detalhamento possível, sem modificações;

PROOF OF STAKE (PoS) - algoritmo com os mesmos objetivos do PoW (proof of work). Entretanto, no PoW, o algoritmo recompensa mineiros, que resolvem problemas matemáticos, com o objetivo de validar transações e criar novos blocos. Já no PoS, o criador de um novo bloco, definido como stake, é escolhido, de forma determinística, baseado no seu grau de participação. Nesse sistema, o potencial criador já deve contar com uma participação na rede (por meio de moedas, em caso de criptomoedas). Quanto maior a participação de um usuário no sistema, maior a chance de ele ser o criador escolhido. Além disso, o usuário selecionado deverá alocar uma quantidade de ativos para este processo e, caso tente comprometer ou alterar o bloco, perderá suas ativos. Isto em teoria garante a integridade dos participantes;

PROOF OF WORK (PoW) - requisito da operação de mineração que precisa ser realizada, visando a criação um novo bloco num blockchain. Trata-se de um protocolo que tem por principal objetivo deter ataques cibernéticos como DDoS, por ser um mecanismo de resistência a ataques sybil. Possui a função de esgotar os recursos de um sistema computacional pelo envio de múltiplas requisições falsas. Uma das principais desvantagens do PoW, no modelo público, reside no controle da geração de tokens de recompensa; todos os nós competem para ser o primeiro a solucionar o enigma matemático vinculado ao bloco de transações. Esse modelo implica em emprego de força bruta, o qual utiliza grande quantidade de recursos computacionais e de energia. O primeiro usuário a resolver o problema ganha o direito de criar o próximo bloco, recebendo o token de recompensa;

PROPRIETÁRIO DA INFORMAÇÃO - parte interessada do órgão ou entidade da administração pública federal, direta e indireta, ou indivíduo legalmente instituído por sua posição ou cargo, que é responsável primário pela viabilidade e sobrevivência da informação;

PROTOCOLO - conjunto de parâmetros que definem a forma e como a transferência de informação deve ser efetuada;

PROVA DE PARTICIPAÇÃO – vide proof of stake;

PROVA DE TRABALHO – vide proof of work;

PROVEDOR DE SERVIÇOS DE NUVEM - ente, público ou privado, que fornece uma plataforma, infraestrutura, aplicativo, serviços de armazenamento ou ambientes de tecnologia da informação baseados em nuvem;

**SERVIÇO PÚBLICO FEDERAL**

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

PROVISIONAMENTO - processo de definição da infraestrutura de tecnologia da informação. Também se refere às etapas necessárias para gerenciar o acesso aos dados e recursos, e para disponibilizá-los aos usuários e sistemas. O provisionamento e a configuração são diferentes, mas ambos são etapas do processo de implantação. A configuração é feita após o provisionamento;

PROVISIONAMENTO DE REDES - processo de definição de uma rede, para que usuários, servidores, containers, dispositivos de Internet of things (IoT), entre outros, possam acessá-la;

PROVISIONAMENTO DE SERVIÇOS - processo de definição de um serviço e do gerenciamento dos dados relacionados, sendo comum em prestação de serviços de computação em nuvem;

PROVISIONAMENTO DE SERVIDORES - processo de definição de todas as operações necessárias para criar uma nova máquina e colocá-la em funcionamento, incluindo a definição do estado desejado do sistema;

PROVISIONAMENTO DE USUÁRIOS - processo de gestão das identidades o qual monitora privilégios de autorização e direitos de acesso. Costuma ser realizado pela área de tecnologia da informação e de recursos humanos;

PSEUDONIMIZAÇÃO - tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional, mantida separadamente pelo controlador, em ambiente controlado e seguro;

PSN - sigla de provedor de serviço de nuvem;

PÚBLICO ALVO DA ETIR - conjunto de pessoas, setores, órgãos ou entidades atendidas por uma Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR). Também chamado de comunidade da ETIR;

Letra Q

QUEBRA DE SEGURANÇA - ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação;



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

Letra R

RANSOMWARE - tipo de malware, que, por meio de criptografia, impede o acesso a dados computacionais. Para recuperar o acesso, exige-se pagamento de um valor de resgate. Caso o pagamento do resgate não seja realizado, pode-se perder definitivamente o acesso aos dados sequestrados;

RBAC - sigla de controle de acesso baseado em papéis (role-based access control);

RECOMENDAÇÃO DE ETIR - informação, com ações de curto prazo, enviadas aos usuários, com orientações sobre como lidar com os impactos resultantes de um incidente cibernético e as atividades que devem ser realizadas para proteger ou recuperar os sistemas que foram afetados;

RECURSO CRIPTOGRÁFICO - sistema, programa, processo, equipamento isolado ou em rede, que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração;

REDE DE COMPUTADORES - conjunto de computadores, interligados por ativos de rede, capazes de trocar informações e de compartilhar recursos, por meio de um sistema de comunicação;

REDE DE TELECOMUNICAÇÕES - conjunto operacional contínuo de enlaces e equipamentos, incluindo funções de transmissão, comutação ou quaisquer outras indispensáveis à operação de serviço de telecomunicações;

REDE PRIVADA VIRTUAL (VPN) - refere-se à construção de uma rede privada, utilizando redes públicas (por exemplo, a Internet) como infraestrutura. Esses sistemas utilizam criptografia e outros mecanismos de segurança para garantir que somente usuários autorizados possam ter acesso à rede privada e que nenhum dado será interceptado enquanto estiver passando pela rede pública;

REDES CONTRADITÓRIAS GENERATIVAS (GAN) - criadas por Ian Goodfellow, em 2014, durante seus estudos de doutorado, na Universidade de Montreal, um dos principais institutos de pesquisa em Inteligência Artificial. Trata-se de uma classe de estruturas de aprendizado de máquina, sendo usadas duas redes neurais separadas (geradora e discriminadora), as quais são colocadas umas contra as outras. Começando com um determinado conjunto de dados (por exemplo, uma coleção de fotos de rostos humanos), a geradora começa a criar novas imagens



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

que, em termos de pixels, são matematicamente semelhantes às imagens existentes. Enquanto isso, a discriminadora recebe as imagens, sem saber se elas são do conjunto de dados original ou da saída do gerador, tendo-se como tarefa identificar quais imagens são sintéticas. À medida que as duas redes trabalham interativamente uma contra a outra: a geradora, tentando gerar imagens capazes de enganar a discriminadora, e a discriminadora, tentando descobrir as criações da geradora; elas aprimoram as suas capacidades. Eventualmente, a taxa de sucesso da classificação da discriminadora cai para 50% (pouco melhor do que suposições aleatórias), o que significa que as imagens geradas sinteticamente se tornaram indistinguíveis das imagens originais;

REDES DE NÚCLEO - redes pertencentes às próprias prestadoras de serviços de telecomunicações;

REDES SOCIAIS - estruturas sociais digitais, compostas por pessoas ou organizações, conectadas por um ou vários tipos de relações, que partilham valores e objetivos comuns;

REDUZIR RISCO - forma de tratamento de risco, na qual a alta administração decide realizar a atividade, adotando ações para reduzir a probabilidade, as consequências negativas, ou ambas, associadas a um risco;

REGIÃO DE NUVEM - agrupamento de localizações geográficas específicas, em que recursos computacionais encontram-se hospedados. Considera-se, para efeito deste Glossário, que o território brasileiro está localizado em uma única região;

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS - documentação do controlador, no qual são descritos os processos de tratamento de dados pessoais, que identificam os riscos às liberdades civis e aos direitos fundamentais, as medidas de salvaguarda, bem como mecanismos de mitigação dos riscos;

REMETENTES CONFIÁVEIS – vide whitelist;

REQUISITOS DE SEGURANÇA DE SOFTWARE - conjunto de necessidades de segurança que um software deve atender. Essas necessidades são determinadas pela política de segurança da informação da organização, compreendendo aspectos funcionais e não funcionais. Os aspectos funcionais descrevem comportamentos que viabilizam a criação ou a manutenção da segurança e, geralmente, podem ser testados diretamente. São exemplos de requisitos funcionais o controle de acesso, baseado em papéis de usuários (administradores, usuários comuns, entre outros) e a autenticação com o uso de credenciais (usuário e senha, certificados digitais, entre



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

outros). Os aspectos não funcionais descrevem procedimentos necessários para que o software permaneça executando suas funções adequadamente, mesmo quando sob uso indevido. São exemplos de requisitos não funcionais a validação das entradas de dados e o registro de logs de auditoria com informações suficientes para análise forense;

RESILIÊNCIA - capacidade de uma organização ou de uma infraestrutura de resistir aos efeitos de um incidente, ataque ou desastre, e retornar à normalidade das operações;

RESUMO CRIPTOGRÁFICO - resultado da ação de algoritmos que fazem o mapeamento de bits de tamanho arbitrário para uma sequência de bits de tamanho fixo menor, conhecido como resultado hash. Dessa forma, torna-se difícil encontrar duas mensagens que produzam o mesmo resultado hash (resistência à colisão), e também realizar o processo reverso (utilizando-se apenas o hash não é possível recuperar a mensagem que o gerou);

RETER RISCO - tipo de tratamento de risco, em que a alta administração decide realizar a atividade, assumindo as responsabilidades, caso ocorra o risco identificado;

RISCO - no sentido amplo, trata-se da possibilidade de ocorrência de um evento que pode impactar o cumprimento dos objetivos. Pode ser mensurado em termos de impacto e de probabilidade;

RISCO DE SEGURANÇA DA INFORMAÇÃO - risco potencial associado à exploração de uma ou mais vulnerabilidades de um ou mais ativos de informação, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

ROAMING- capacidade de enviar e de receber dados em telefonia móvel, por intermédio de redes móveis, em uma zona onde o serviço é provido por outra operadora;

ROLE-BASED ACCESS CONTROL(RBAC) - vide controle de acesso baseado em papéis;

ROOT OF TRUST(RoT) - fonte considerada sempre confiável em um sistema criptográfico. Como a segurança criptográfica é dependente de chaves para a encriptação e decriptação de dados e para a execução de funções, como a geração de assinaturas digitais, esquemas RoT geralmente incluem módulos de hardware reforçados (sendo o principal exemplo o HSM -hardware security module), que geram e protegem chaves, e executam funções criptográficas em um ambiente seguro. O RoT é um componente crítico de public key infrastructure (PKI) para a geração e



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

proteção de chaves de autoridade certificadora e de raiz; para a assinatura de código, visando garantir que o software permaneça seguro, inalterado e autêntico; e para a criação de certificados digitais para o credenciamento e autenticação de dispositivos proprietários para aplicações do tipo Internet of things (IoT) e para outros componentes de rede;

ROOTKIT- conjunto de programas e de técnicas que permitem esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido. É importante ressaltar que o nome rootkit não indica que as ferramentas que o compõem são usadas para obter acesso privilegiado em um computador (root ou administrator), mas, sim, para manter o acesso privilegiado em um computador previamente comprometido;

RoT - sigla de root of trust;

Letra S

SaaS - sigla de software como Serviço (software-as-a-service);

SABOTAGEM CIBERNÉTICA - ataques cibernéticos contra a integridade e disponibilidade de sistemas e de serviços de tecnologia da informação;

SANITIZAÇÃO DE DADOS - eliminação efetiva de informação armazenada em qualquer meio eletrônico, garantindo que os dados não possam ser reconstruídos ou recuperados;

SCREENLOGGER- tipo específico de spyware. Programa similar ao keylogger, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou a região que circunda a posição onde o mouse é clicado. É bastante utilizado por atacantes para capturar as teclas digitadas pelos usuários em teclados virtuais, disponíveis principalmente em sites de Internet banking;

SDK - sigla de kit de desenvolvimento de software (software development kit);

SECURITY BY DESIGN- significa pensar em segurança desde o escopo de desenvolvimento de um novo software, prevendo toda possibilidade de riscos aos quais aquela aplicação pode estar sujeita. É um conceito de grande importância para a indústria de segurança da informação;

**SERVIÇO PÚBLICO FEDERAL**

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

SECURITY TRUST AND ASSURANCE REGISTRY(STAR) - programa de garantia de segurança de provedor de serviço de nuvem, da cloud security alliance (CSA), em três níveis (autoavaliação, auditoria de terceiros e monitoramento contínuo), abrangendo os princípios de chave de transparência, de auditoria rigorosa e de harmonização de padrões. Um provedor de serviço de nuvem com certificação STAR utiliza as melhores práticas de segurança em suas ofertas de serviços de nuvem. Os níveis de certificação podem ser encontrados em <https://cloudsecurityalliance.org/star/levels/>;

SEGURANÇA CIBERNÉTICA - ações voltadas para a segurança de operações, visando garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético, capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis;

SEGURANÇA CORPORATIVA - vide segurança orgânica;

SEGURANÇA DA INFORMAÇÃO - ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

SEGURANÇA FEDERADA - tem por objetivo fornecer um mecanismo para estabelecer relações de confiança entre domínios, para que os usuários possam autenticar para o seu próprio domínio ao mesmo tempo em que está sendo concedido acesso aos aplicativos e serviços que pertencem a outro domínio. Isso possibilita que as técnicas de autenticação, como o serviço single sign-on, eliminem a necessidade de provisionar e gerenciar contas duplicadas para os usuários em domínios e de aplicativos, e reduz significativamente o custo para estender os aplicativos de terceiros confiáveis;

SEGURANÇA ORGÂNICA - conjunto de medidas passivas, com o objetivo de prevenir e, até mesmo, obstruir as ações que visem o comprometimento ou a quebra de segurança de uma organização. Inclui os processos relacionados às áreas: de pessoal, de documentação, das comunicações, da tecnologia da informação, dos materiais e das instalações de uma organização, dentre outros;

SENHA DESCARTÁVEL (one-time password) - senha que é válida somente para uma sessão de login ou transação, em um sistema de computadores ou outros dispositivos digitais;

SENSIBILIZAÇÃO - atividade que tem por objetivo atingir uma predisposição dos participantes para uma mudança de atitude sobre a SI, de tal forma que eles possam perceber em sua rotina,



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

peçoal e profissional, ações que devem ser corrigidas. É uma etapa inicial da educação em segurança da informação;

SERVIÇOS - meio de fornecimento de valor a clientes, com vistas a entregar os resultados que eles desejam, sem que tenham que arcar com a propriedade de determinados custos e riscos;

SERVIÇO DA ETIR - conjunto de procedimentos, estruturados em um processo bem definido, oferecido à comunidade da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos;

SERVIÇOS DE REDE DE TELECOMUNICAÇÕES - provimento de serviços de telecomunicações, de tecnologia da informação e de infraestrutura para redes de comunicação de dados;

SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO - provimento de serviços de desenvolvimento, de implantação, de manutenção, de armazenamento e de recuperação de dados e de operação de sistemas de informação, projeto de infraestrutura de redes de comunicação de dados, modelagem de processos e assessoramento técnico necessários à gestão da informação;

SI - sigla de segurança da informação;

SINGLE SIGN-ON(SSO) - é uma solução tecnológica que permite que diversos aplicativos com senhas de acesso diferentes possam ser acessados de forma transparente e segura pela utilização de uma única senha principal ou meio de identificação pessoal (como a biometria ou umpersonal identification number- PIN, por exemplo). Ou seja, com o SSO, o usuário digita apenas uma senha quando faz o primeiro acesso e depois vai abrindo os demais aplicativos sem necessidade de digitar a senha específica do aplicativo;

SÍNTESE DE IMAGEM HUMANA - técnica que pode ser aplicada para fazer interpretações críveis e, até mesmo, para criar foto realista de pessoas reais, em movimento ou parados. A construção de uma imagem humana sintetizada é iniciada pelo mapeamento da pessoa desejada, por meio da digitalização e fotografia 3D, seguida da criação de um modelo 3D, baseado nas amostras, por intermédio da aplicação de informações estatísticas e aproximações. A aplicação da síntese com um ator e com algoritmos adequados é então aplicada sobre o modelo 3D. O papel do ator na síntese é imitar as expressões humanas na síntese de imagens paradas e em vídeos com movimentação. Diversos algoritmos são necessários para simular leis da física e da fisiologia, além de mapear corretamente o modelo, sua aparência e sua movimentação;



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

SISTEMA DE ACESSO - conjunto de ferramentas que se destina a controlar e a dar a uma pessoa permissão de acesso a um recurso;

SISTEMA BIOMÉTRICO - conjunto de ferramentas que se utiliza das características de uma pessoa, levando em consideração fatores comportamentais e fisiológicos, a fim de identificá-la de forma unívoca;

SISTEMA DE DETECÇÃO DE INTRUSÃO (IDS) - refere-se a um mecanismo que, sigilosamente, ouve o tráfego na rede para detectar atividades anormais ou suspeitas e, deste modo, reduz os riscos de intrusão. Existem duas famílias distintas de IDS: os N-IDS (network based intrusion detection system ou sistema de detecção de intrusões de rede), que garantem a segurança dentro da rede e os H-IDS (host based intrusion detection system ou sistema de detecção de intrusões no host), que asseguram a segurança no host;

SISTEMA DE INFORMAÇÃO - conjunto de elementos materiais ou intelectuais, colocados à disposição dos usuários, em forma de serviços ou bens, que possibilitam a agregação dos recursos de tecnologia, informação e comunicações de forma integrada;

SISTEMA DE PROTEÇÃO FÍSICA - sistema composto por pessoas, equipamentos e procedimentos, para a proteção de ativos contra danos, roubo, sabotagem e outros prejuízos causados por ação humana não autorizada, conforme gestão da segurança física e ambiental;

SISTEMA ESTRUTURANTE - sistema com suporte de tecnologia da informação, fundamental e imprescindível para o planejamento, coordenação, execução, descentralização, delegação de competência, controle ou auditoria das ações de Estado, além de outras atividades auxiliares, desde que comum a dois ou mais órgãos ou entidades da administração pública federal, direta ou indireta, e que necessitem de coordenação central;

SOC 2 - desenvolvido pelo American Institute of CPAs (AICPA), define critérios para gerenciamento de dados dos usuários, baseados nos cinco princípios de confiança do serviço - disponibilidade, integridade, confidencialidade, segurança e privacidade - sendo considerado um requisito mínimo a ser atendido pelo provedor de serviço de nuvem. O relatório tipo I informa se o projeto dos sistemas do provedor de serviço de nuvem é adequado para atender os princípios de confiança relevantes. O relatório tipo II detalha a efetividade operacional dos sistemas do provedor de serviço de nuvem;

SOFTWARE COMO SERVIÇO (SaaS) - tipo de serviço de computação em nuvem em que o provedor de serviço de nuvem oferece ao cliente a capacidade de usar um aplicativo fornecido. São



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

exemplos de SaaS serviços de e-mail on-line e sistemas de edição de documentos on-line. Um usuário de uma solução SaaS só é capaz de usar o aplicativo oferecido e de fazer pequenos ajustes de configuração. O provedor SaaS é responsável pela manutenção da aplicação;

SOLUÇÃO DE IoT (Internet of things) - conjunto de dispositivos, softwares ou serviços desenvolvidos para operar no ambiente de Internet das coisas;

SOLUÇÃO END-TO-END- solução que busca controlar um processo do seu início até o seu término;

SPOOFING- ato de falsificar a identidade da fonte de uma comunicação ou interação. É possível falsificar endereço IP, ARP, DNS (conhecido com envenenamento do cache de DNS), endereço MAC, site da web, endereço de e-mail, id de chamador, entre outros;

SPYWARE- tipo de malware. Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros. Keylogger, screenlogger e adware são alguns tipos específicos de spyware;

SSL - sigla de secure sockets layer;

SSO - sigla de single sign-on;

STAR - sigla de security trust and assurance registry.

Letra T

TCG - sigla de trusted computing group;

TCMS - sigla de termo de compromisso de manutenção de sigilo;

TCP - sigla de transmission control protocol;



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

TCP/IP - trata-se de um conjunto de protocolos. Esse grupo é dividido em quatro camadas: aplicação, transporte, rede e interface. Cada uma delas é responsável pela execução de tarefas distintas. Essa divisão em camadas é uma forma de garantir a integridade dos dados que trafegam pela rede;

TECNOLOGIA DA INFORMAÇÃO - ativo estratégico que apoia processos de negócios institucionais, mediante a conjugação de recursos, processos e técnicas, utilizados para obter, processar, armazenar, disseminar e fazer uso de informações;

TELECOMUNICAÇÕES - transmissão, emissão ou recepção, por fio, radioeletricidade, meios ópticos ou qualquer outro processo eletromagnético, de símbolos, caracteres, sinais, escritos, imagens, sons ou informações de qualquer natureza;

TEMPO OBJETIVO DE RECUPERAÇÃO - tempo pré-definido no qual uma atividade deverá estar disponível após uma interrupção ou incidente;

TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO - termo utilizado para garantir o sigilo de uma informação classificada em grau de sigilo em caráter excepcional, mediante assinatura de pessoa natural não credenciada ou não autorizada por legislação;

TERMO DE RESPONSABILIDADE - termo assinado pelo usuário, concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações a que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso;

TERRORISMO CIBERNÉTICO - crime cibernético perpetrado por razões políticas, religiosas ou ideológicas, contra qualquer elemento da infraestrutura cibernética com os objetivos de: provocar perturbação severa ou de longa duração na vida pública; causar danos severos à atividade econômica, com a intenção de intimidar a população; forçar as autoridades públicas ou uma organização a executar, tolerar, revogar ou a omitir um ato; ou abalar ou destruir as bases políticas, constitucionais, econômicas ou sociais de um Estado, organização ou empresa. É principalmente realizado por atos de sabotagem cibernética, organizados e gerenciados por indivíduos, grupos político-fundamentalistas, ou serviços de inteligência estrangeiros;

TESTE DE INTRUSÃO - vide teste de penetração;



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

TESTE DE PENETRAÇÃO (PENTEST) - também chamado de teste de intrusão, é fundamental para a análise de vulnerabilidades e consiste em testar todos os sistemas em busca de, além das já verificadas na fase anterior, vulnerabilidades conhecidas e disponibilizadas por especialistas ou pelas instituições detentoras dos softwares que estão sendo utilizados pela instituição;

TIC - sigla de tecnologia da informação e comunicação;

TITULAR DO DADO - pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

TOKEN - algo que o usuário possui e controla (tipicamente uma chave, senha e/ou módulo criptográfico) e que é utilizado para autenticar a identidade do requerente e/ou a requisição em si;

TLS - sigla de transport layer security;

TPM - sigla de trusted platform module;

TRANSFERIR RISCO - forma de tratamento de risco na qual a alta administração decide realizar a atividade, compartilhando com outra entidade o ônus associado a um risco;

TRANSMISSION CONTROL PROTOCOL(TCP) - protocolo da camada de transporte do modelo TCP/IP, que permite gerenciar os dados originados ou destinados ao protocolo IP. Trata-se de um protocolo orientado à conexão, o qual permite a comunicação entre duas máquinas e o controle do estado da transmissão;

TRANSFERÊNCIA INTERNACIONAL DE DADOS - transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

TRATAMENTO - toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

TRATAMENTO DA INFORMAÇÃO - conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;

TRATAMENTO DA INFORMAÇÃO CLASSIFICADA - conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle de informação classificada, independente do meio, suporte ou formato;

TRATAMENTO DE ARTEFATOS MALICIOSOS - serviço que prevê o recebimento de informações ou cópia do artefato malicioso que foi utilizado no ataque, ou de qualquer outra atividade desautorizada ou maliciosa. Uma vez recebido o artefato, este deve ser analisado, ou seja, deve-se buscar a natureza do artefato, seu mecanismo, versão e objetivo, para que seja desenvolvida, ou sugerida, uma estratégia de detecção, remoção e defesa contra esses artefatos;

TRATAMENTO DE INCIDENTES CIBERNÉTICOS - consiste nas ações e procedimentos tomados imediatamente após a identificação do incidente, visando garantir a continuidade de operações, preservar evidências e emitir as notificações necessárias;

TRATAMENTO DE INCIDENTES DE SEGURANÇA EM REDES COMPUTACIONAIS - vide tratamento de incidentes cibernéticos;

TRATAMENTO DE RISCOS - processo de implementação de ações de Segurança da Informação para evitar, reduzir, reter ou transferir um risco;

TRATAMENTO DE VULNERABILIDADES - serviço que prevê o recebimento de informações sobre vulnerabilidades, em hardware ou software, objetivando analisar sua natureza, mecanismo e suas consequências, e desenvolver estratégias para detecção e correção dessas vulnerabilidades;

TRILHA DE AUDITORIA - registro ou conjunto de registros gravados em arquivos de log ou outro tipo de documento ou mídia, que possam indicar, de forma cronológica e inequívoca, o autor e a ação realizada em determinada operação, procedimento ou evento;

TROJAN- vide cavalo de Tróia;



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

TRUSTED COMPUTING GROUP(TCG) - organização sem fins lucrativos, formada para desenvolver, definir e promover padrões abertos e neutros do setor global, apoiando uma raiz de confiança baseada em hardware, para plataformas de computação confiáveis interoperáveis;

TRUSTED PLATFORM MODULE(TPM) – um chip TPM é um processador de criptografia seguro, projetado para desempenhar as operações de criptografia. Ele inclui vários mecanismos de segurança física, para torná-lo resistente a adulterações por software mal-intencionado nas funções de segurança do TPM. Suas funções mais comuns são medições de integridade do sistema e uso e criação de chaves. Versões diferentes do TPM estão definidas nas especificações do TCG (trusted computing group);

TRUSTED VIRTUAL MACHINE(TVM) - vide máquina virtual confiável;

TRUSTLESS- em sistemas blockchain é a forma pela qual ocorre a validação dos processos, conforme as regras definidas pelo protocolo em execução por meio da distribuição do esforço computacional entre os membros componentes do sistema, sem a existência de um único membro ou órgão central;

TVM - sigla de máquina virtual confiável (trusted virtual machine);

Letra U

UID - sigla de identificador único (unique identifier) em sistemas de computadores. Baseados nessa definição, também temos o GUID (identificador global único ou global unique identifier) e UUID (identificador universal único ou universal unique identifier). Ressalta-se que, no sistema UNIX, UID significa identificador do usuário (user identifier);

USO COMPARTILHADO DE DADOS - comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais, por órgãos e entidades públicos, no cumprimento de suas competências legais, ou entre esses entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

USUÁRIO DE INFORMAÇÃO - pessoa física, seja servidor ou equiparado, empregado ou prestador de serviços, habilitada pela administração para acessar os ativos de informação de um órgão ou



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

entidade da administração pública federal, formalizada por meio da assinatura de Termo de Responsabilidade;

USUÁRIO VISITANTE COM DISPOSITIVO MÓVEL - agentes públicos ou não, que utilizem dispositivos móveis, de sua propriedade ou do órgão ou entidade a que pertencem, dentro dos ambientes físicos de órgãos ou entidades da administração pública federal dos quais não fazem parte;

URL - sigla de uniform resource locator;

Letra V

VAZAMENTO DE DADOS - transmissão não autorizada de dados de dentro de uma organização para um destino ou recipiente externo. O termo pode ser usado para descrever dados que são transferidos eletronicamente ou fisicamente. Pode ocorrer de forma acidental ou intencional (pela ação de agentes internos, pela ação de agentes externos ou pelo uso de software malicioso). É conhecido também como roubo de dado slow-and-slow(rasteiro-e-lento), pois a exfiltração de dados para fora da organização é feita usando técnicas do tipo low-and-slow, a fim de evitar detecção;

VENDOR LOCK-IN- também conhecido como lock-in proprietário ou lock-in do cliente, usado para designar a situação em que há um alto custo de troca para o consumidor em um ou mais serviços. Isso faz com que um cliente fique dependente de um fornecedor de produtos e serviços, pois a mudança de fornecedor implica em substanciais custos de mudança;

VERIFICAÇÃO DE CONFORMIDADE EM SEGURANÇA DA INFORMAÇÃO - procedimentos que fazem parte da avaliação de conformidade, que visam identificar o cumprimento das legislações, normas e procedimentos relacionados à segurança da informação da organização;

VÍRUS - seção oculta e autorreplicante de um software de computador, geralmente utilizando lógica maliciosa, que se propaga pela infecção (inserindo uma cópia sua e tornando-se parte) de outro programa. Não é auto executável, ou seja, necessita que o seu programa hospedeiro seja executado para se tornar ativo;

VIRTUAL MACHINE(VM) - vide máquina virtual;



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

VIRTUAL MACHINE IMAGE(VMI) - vide imagem de máquina virtual;

VISHING- uma forma de ataque de phishing que ocorre em VoIP, sendo que as vítimas não precisam estar utilizando VoIP. O atacante usa sistemas VoIP para efetuar ligações para qualquer número de telefone, sem cobrança de taxas, e, geralmente, falsifica (spoofing) sua identificação de chamada, a fim de levar a vítima a acreditar que está recebendo um telefonema de uma fonte legítima ou confiável (como um banco, uma loja de varejo, entre outros);

VM - sigla de máquina virtual (virtual machine);

VMI - sigla de imagem de máquina virtual (virtual machine image);

VPN - sigla de rede privada virtual (virtual private network);

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;

VULNERABILIDADE DE DIA ZERO - falha na segurança de um software, que ainda não é conhecida por seus desenvolvedores, pelos fabricantes de soluções de segurança e pelo público em geral. Também é considerada uma vulnerabilidade de dia zero a falha de segurança que já é conhecida pelo fornecedor do produto, mas para a qual ainda não existe um pacote de segurança para corrigi-la. Por não ser conhecida ou por não haver ainda um patch de segurança para essa falha, ela pode ser explorada por hacker sem explorações de dia zero. A correção de uma vulnerabilidade de dia zero geralmente é tarefa do fabricante do software, que precisará lançar um pacote de segurança para consertar a falha;

Letra W

WHITELIST- lista de itens aos quais é garantido o acesso a certos recursos, sistemas ou protocolos. Utilizar uma whitelist para controle de acesso significa negar o acesso a todas as entidades, exceto àquelas incluídas na whitelist;

**SERVIÇO PÚBLICO FEDERAL**

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

WORM- programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o worm não embute cópias de si mesmo em outros programas ou arquivos, e não necessita ser explicitamente executado para se propagar. Sua propagação se dá por meio da exploração de vulnerabilidades existentes ou de falhas na configuração de programas instalados em computadores;

Letra X

XSS - sigla de cross-site scripting;

Letra Z

ZERO-DAY EXPLOIT- vide exploração de dia zero;

ZERO-DAY VULNERABILITY- vide vulnerabilidade de dia zero;

ZERO TRUST- vide confiança zero;

ZONA DE NUVEM - locais isolados dentro de cada região, dos quais os serviços de computação em nuvem pública se originam e operam;

ZONA DESMILITARIZADA (DMZ) - também conhecida como rede de perímetro, trata-se de uma sub-rede (física ou lógica) que se situa entre uma rede privada confiável e uma rede não confiável, e onde recursos computacionais são hospedados para serem acessados a partir da rede não confiável (em geral, a Internet), evitando o acesso à rede interna da organização. A DMZ garante o isolamento entre a rede confiável e não confiável por uma série de regras de conectividade mantidas em um firewall;

ZUMBI - nome dado a um computador infectado por bot, pois pode ser controlado remotamente, sem o conhecimento do seu proprietário; e

Número 2



SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE QUÍMICA

SCS QD 09 – BL A – TORRE B – 9º ANDAR – ED. PARQUE CIDADE CORPORATE

70308-200 – BRASÍLIA/DF – (61) 2099-3300 – e-mail: cfq@cfq.org.br

2FA - sigla de autenticação de dois fatores (2factor authentication).

Este conteúdo não substitui o publicado na versão certificada.