Segurança da Informação

A

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;

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;

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;

AMEAÇA CIBERNÉTICA

Conjunto de fatores externos com o potencial de causar dano para um sistema ou organização;

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;

ANPD

sigla de Autoridade Nacional de Proteção de Dados que é o órgão da administração pública federal responsável por zelar, implementar e fiscalizar o cumprimento da Lei nº 13.709, de 14 de agosto de 2018;

ASSINATURA DIGITAL

tipo de assinatura eletrônica que usa operações matemáticas, 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

mecanismo que permite 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 CIBERNETICO

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

ATIVIDADE

ação ou conjunto de ações executadas 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 DE TI

recurso computacional ou a ele associado, usado no aproveitamento, produção, processamento, armazenamento, transmissão e recuperação da informação;

ATIVO DE REDE

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

ATIVO DE INFORMAÇÃO

qualquer informação produzida ou custodiada pelo PJSC, que tem valor para a instituição e consequentemente necessita ser adequadamente protegida e armazenada em base de dados específica ou arquivo eletrônico;

AUTENTICAÇÃO

processo que busca verificar a identidade digital de um usuário de um sistema, no momento em que ele requisita acesso a esse sistema. O processo é realizado por meio de regras preestabelecidas, geralmente pela comparação das credenciais apresentadas pelo usuário 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;

AUTENTICIDADE

atributo inerente à segurança da informação que assegura a correspondência entre o autor de determinada informação e a pessoa, processo ou sistema a quem se atribui a autoria;

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);

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 RISCOS

processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco.

B

BACKUP

o mesmo que cópia de segurança. O 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;

BIOMETRIA

verificação da identidade de um indivíduo por meio de uma característica física, como a digital ou o rosto;

BLOQUEIO

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

BLOQUEIO DE ACESSO

processo que tem por finalidade suspender temporariamente o acesso.

C

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;

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 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;

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;

COMITÊ DE GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO

vinculado à Presidência do Tribunal de Justiça, de natureza deliberativa e de caráter permanente, que atuará em nível estratégico, com o objetivo de promover a cultura e estabelecer diretrizes em segurança da informação;

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);

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;

CONFIDENCIALIDADE

princípio da segurança da informação do PJSC que assegura que a informação só seja acessada por pessoas, órgãos ou sistemas credenciados, ou seja, impede que a informação esteja disponível ou seja divulgada a indivíduos, entidades ou processos sem autorização específica;

CONFORMIDADE EM SEGURANÇA DA INFORMAÇÃO

cumprimento das legislações, normas e procedimentos relacionados à segurança da informação da organização;

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;

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;

CÓPIA DE SEGURANÇA – o mesmo que 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);

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;

CRITICIDADE

atributo inerente à segurança da informação que define a importância da informação para a continuidade das operações da instituição.

D

DADO PESSOAL

informação relacionada à pessoa natural identificada ou identificável;

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;

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;

DIREITO DE ACESSO

privilégio associado a um cargo, pessoa ou processo, para ter acesso a um ativo;

DISPONIBILIDADE

princípio da segurança da informação do PJSC que consiste em fazer com que a informação esteja acessível e utilizável, no momento escolhido por uma pessoa, órgão ou sistema, ou seja, garante o acesso à informação quando requisitado, de acordo com os seus requisitos de disponibilidade.;

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, USB drives, HD externo, e cartões de memória.

E

E-MAIL

sigla de correio eletrônico (electronic-mail);

EMISSÃO 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;

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;

ENSEC-PJ

Estratégia Nacional de Segurança Cibernética do Poder Judiciário, instituída por meio da Resolução CNJ n. 396/2021;

(ETIR) EQUIPE DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES DE SEGURANÇA CIBERNÉTICA

grupo de pessoas vinculado ao Comitê de Governança de Segurança da Informação, com o objetivo de atuar nos incidentes de segurança cibernética. Deve atuar em conjunto com a DTI-Diretoria de Tecnologia da Informação, com o NIS-Núcleo de Segurança Institucional, com o NSEC-Núcleo de Segurança Cibernética e com o CGPDP-Comitê Gestor de Proteção de Dados Pessoais, nos incidentes de segurança que tratarem de temas relacionados a competências desses órgãos;

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.

F

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.

G

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 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 DA INFORMAÇÃO

unidade ou responsável pela execução de projeto do PJSC que, no exercício de suas atribuições, produz informações ou obtém, de fonte externa ao PJSC, informações de propriedade de pessoa física ou jurídica;

GLOBAL PROTECT

software que faz a conexão do computador com a rede interna, por meio da rede privada virtual (VPN);

GOLPE

acesso aos dados de uma pessoa, órgão ou entidade por meio da exploração das fragilidades dos usuários, utilizando técnicas de engenharia social e por diferentes meios e discursos, visando enganar e persuadir potenciais vítimas a fornecerem informações sensíveis ou a realizarem ações, como executar códigos maliciosos e acessar páginas falsas. De posse dos dados das vítimas, os golpistas costumam efetuar transações financeiras, acessar sites, enviar mensagens eletrônicas, abrir empresas fantasmas e criar contas bancárias ilegítimas, entre outras atividades maliciosas. Muitos dos golpes aplicados na internet podem ser tipificados como estelionato e o golpista pode ser considerado um estelionatário.

H

HACKER

termo popularmente usado para definir especialistas em computação que utilizam o alto conhecimento para cometer crimes cibernéticos. Porém, essa definição não é totalmente correta, pois hackers são pessoas com um conhecimento profundo de computação e informática, que trabalham desenvolvendo e modificando softwares e hardwares de computadores, não necessariamente para cometer algum crime.

HARDWARE

conjunto dos equipamentos físicos que compõe um computador (dispositivos eletrônicos, monitor, placas, teclado etc.), juntamente com seus equipamentos periféricos (impressora, scanner etc.); equipamento utilizado no desenvolvimento de certa ação ou atividade;

HOST

qualquer computador ou máquina conectado a uma rede, que conta com número de IP e nome definidos. Essas máquinas são responsáveis por oferecer recursos, informações e serviços aos usuários ou clientes. Por essa abrangência, a palavra pode ser utilizada como designação para diversos casos que envolvam uma máquina e uma rede, desde computadores pessoais à roteadores.

I

ICP-Brasil

sigla de infraestrutura de chaves públicas brasileira que é a 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;

IDENTIDADE DIGITAL

representação unívoca de um indivíduo dentro do espaço cibernético;

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 DA INFORMAÇÃO

qualquer indício de fraude, sabotagem, desvio, falha ou evento indesejado ou inesperado que possa comprometer as operações do PJSC ou ameaçar a segurança da informação;

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;

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;

INTEGRIDADE

princípio da segurança da informação do PJSC que garante a não violação das informações para protegê-las contra alteração, gravação ou exclusão acidental ou proposital. A informação protegida deve ser íntegra, sem sofrer qualquer alteração indevida, não importa por quem e nem em qual etapa, se no processamento ou no envio;

INTERNET

rede global, composta pela interligação de inúmeras redes. Conecta 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;

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;

IP

sigla de INTERNET PROTOCOL protocolo que permite o endereçamento e o transporte de pacotes de dados (datagramas) na Internet, sem, contudo, assegurar que estes pacotes sejam entregues.

J

K

Keylogger

Programa malicioso que registra tudo que foi escrito no teclado.

L

LAI

sigla de Lei de Acesso à Informação;

LGPD

sigla de Lei Geral de Proteção de Dados Pessoais;

LOG

significa registro. Usado em auditorias, por exemplo, é o registro de eventos relevantes em um dispositivo ou sistema computacional.

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, spyware, adware e rootkits;

MEDIDAS DE SEGURANÇA

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

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.

N

NÍVEL DE MATURIDADE EM SI

identificado como inexistente, inicial, organizado, gerenciado ou otimizado, é obtido por meio de instrumento de avaliação específico e possibilita incentivar a execução de projetos e ações específicas para incrementar a maturidade, por meio de pesquisa do comportamento dos usuários de TI acerca da SI, campanhas de sensibilização ou conscientização, capacitação dos usuários e equipes técnicas da Diretoria de TI e implementação de melhorias nos processos do SGSI;

NÚCLEO DE SEGURANÇA CIBERNÉTICA

vinculado à Presidência do Tribunal de Justiça com o objetivo de aprimorar o nível de maturidade em segurança cibernética nos órgãos do Poder Judiciário do Estado de Santa Catarina, abrangendo os aspectos fundamentais da segurança da informação para o aperfeiçoamento necessário à consecução desse propósito. Deve atuar de forma articulada com o Comitê Gestor de Proteção de Dados Pessoais CGPDP, com o Núcleo de Inteligência e Segurança Institucional NIS e com a Diretoria de Tecnologia da Informação DTI para tratar de temas relacionados a competência desses órgãos;

NUVEM

é o fornecimento de serviços de computação, incluindo servidores, armazenamento, bancos de dados, rede, software, análise e inteligência, pela internet (“a nuvem”) para oferecer inovações mais rápidas, recursos flexíveis e economias de escala. Normalmente paga-se apenas pelos serviços de nuvem que usa, ajudando a reduzir os custos operacionais, a executar sua infraestrutura com mais eficiência e a escalonar conforme as necessidades da organização mudam. A computação em nuvem é uma grande mudança na forma tradicional de pensamento adotada pelas empresas sobre os recursos de TI, pois elimina o gasto de capital com a compra de hardware e software, configuração e execução de datacenters locais.

O

P

PERFIL DE ACESSO

conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;

PHISHING

é uma das técnicas mais utilizadas pelos golpistas para obter dados pessoais e financeiros de um usuário. É um tipo específico de golpe que envolve o redirecionamento da navegação do usuário para sites falsos. Normalmente vem em forma de mensagem de e-mail, combinando práticas de engenharia social, para que o receptor da mensagem aceite e execute as ações solicitadas por vontade própria;

PIN

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

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

documento que contém um conjunto de princípios que declara o comprometimento institucional com o provimento de diretrizes estratégicas, responsabilidades, competências e o apoio para implementar a gestão de segurança da informação a fim de garantir um ambiente tecnológico controlado e seguro de forma a oferecer todas as informações necessárias aos processos deste Tribunal com disponibilidade, integridade, confidencialidade e autenticidade. A Resolução TJ n. 15, de 4 de julho de 2018, instituiu a Política de Segurança da Informação do Poder Judiciário do Estado de Santa Catarina PSI/PJSC. As diretrizes estabelecidas nesta política determinam as linhas mestras que devem ser seguidas por todas as pessoas que tenham acesso a informações deste Poder Judiciário;

PROCESSOS DE SEGURANÇA DA INFORMAÇÃO – processos organizacionais componentes do Sistema de Gestão de Segurança da Informação

SGSI do PJSC, estabelecidos por meio da Resolução 15/2018-TJ. São eles: classificação da informação; gestão de riscos de segurança da informação; gestão de resposta a incidentes em segurança da informação; controle de acesso à informação; segurança da informação em recursos humanos e conscientização em segurança da informação; e segurança em recursos de tecnologia da informação e comunicações;

PROPRIETÁRIO DA INFORMAÇÃO

pessoa física, unidade ou responsável pela execução de projeto do PJSC que detém a posse, mesmo que transitória, de informação produzida ou recebida pelo PJSC;

PROTOCOLO

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

PROVEDOR DE SERVIÇOS DE NUVEM (PSN)

ente, público ou privado, que fornece uma plataforma, infraestrutura, aplicativo, serviços de armazenamento ou ambientes de tecnologia da informação baseados em nuvem.

Q

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;

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;

REDES SOCIAIS

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

RESPONSABILIDADE:

princípio da segurança da informação do PJSC que atribui obrigações e deveres a pessoa que ocupa determinada função em relação ao acervo de informações.

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.

S

SABOTAGEM CIBERNÉTICA

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

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

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;

SEGURANÇA DA INFORMAÇÃO

proteção da informação contra ameaças para garantir a continuidade dos serviços prestados pelo PJSC, minimizar os riscos e maximizar a eficiência e a efetividade das ações institucionais;

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

SERVIÇO DE TIC

conjunto de componentes relacionados que são utilizados no fornecimento de suporte a uma ou mais áreas de atuação do PJSC; também definido como a combinação de hardware, software, processos e pessoas com o objetivo de gerar um serviço que satisfaça uma ou mais necessidades;

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

conjunto de componentes relacionados que são utilizados no fornecimento de suporte a uma ou mais áreas de atuação do PJSC; também definido como a combinação de hardware, software, processos e pessoas com o objetivo de gerar um serviço que satisfaça uma ou mais necessidades;

SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO (SGSI)

é um sistema não necessariamente informatizado, que inclui toda a abordagem institucional usada para proteger a informação de acordo com seus princípios e atributos de confidencialidade, disponibilidade, integridade, responsabilidade, autenticidade e criticidade. Deve estabelecer políticas, objetivos, processos e procedimentos para a gestão de segurança da informação, por meio de processos específicos definidos em seu escopo. Foi criado no Capítulo II, art. 14 da Resolução 15/2018-TJ;

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 um personal 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;

SISTEMA BIOMÉTRICO

ver biometria 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 ACESSO

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

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;

SOFTWARE

reunião dos procedimentos e/ou instruções que determinam o funcionamento de um computador; conjunto dos elementos que, num computador, compõe o sistema de processamento de dados; todo programa que se encontra armazenado no disco rígido;

SPAM

é o termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas. Na prática, o Spam é uma mensagem eletrônica que chega ao usuário sem a sua permissão ou sem seu desejo em recebê-lo. Geralmente essas mensagens são recebidas por e-mail, mas também podem circular pelas redes sociais ou comentários de blogs. O Spam tem um fundo geralmente comercial, mas também pode assumir um viés criminoso ou para difundir histórias falsas;

SPYWARE

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

T

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;

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 ou de PENETRAÇÃO

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;

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;

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;

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 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 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;

TREND

marca do software antivírus oficial do PJSC, do fabricante Trend Micro Incorporated;

TROJAN

o mesmo que cavalo de Tróia.

U

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 entidade, formalizada por meio da assinatura de Termo de Responsabilidade.

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 dados low-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;

V

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 autoexecutável, ou seja, necessita que o seu programa hospedeiro seja executado para se tornar ativo;

VM

MÁQUINA VIRTUAL ou do inglês VIRTUAL MACHINE 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 do restante do sistema, o software dentro dela não pode adulterar o computador host. As máquinas virtuais também podem ser usadas para outras finalidades, como a virtualização de servidores;

VPN (REDE PRIVADA VIRTUAL)

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.

W

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.

X

Y

Z

ZUMBI

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