**ANEXO I - CONCEITOS E DEFINIÇÕES**

Para os fins dessa Política, considera-se:

* Acesso Lógico – acesso a redes de computadores, sistemas e estações de trabalho por meio de autenticação;
* Acesso Remoto – ingresso, por meio de uma rede, aos dados de um computador fisicamente distante da máquina do usuário;
* Agente responsável: Servidor Público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da Administração Pública Federal (APF), direta ou indireta incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;
* ADSL (Asymmetric Digital Subscriber Line) – (Linha Digital Assimétrica para Assinante) tecnologia de transmissão que possibilita o transporte de voz e dados a alta velocidade através da rede telefônica convencional, analógica ou digital;
* Ameaça - conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;
* Análise/avaliação de riscos – processo completo de análise e avaliação de riscos;
* Ativo - qualquer bem, tangível ou intangível, que tenha valor para a organização;
* Ativo da Informação – os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;
* Ativo Sigiloso – qualquer bem tangível ou intangível que possa conter informações sigilosas que, se acessadas por pessoas não autorizadas, podem causar danos significativos à organização;
* Auditoria – verificação e avaliação dos sistemas e procedimentos internos com o objetivo de reduzir fraudes, erros, práticas ineficientes ou ineficazes;
* Autenticação – é o ato de confirmar que algo ou alguém é autêntico, ou seja, uma garantia de que qualquer alegação de ou sobre um objeto é verdadeira;
* Autenticidade – propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;
* Banco de Dados (ou Base de Dados) – é um sistema de armazenamento de dados, ou seja, um conjunto de registros que tem como objetivo organizar e guardar as informações.
* Biometria – uso de mecanismos de identificação para restringir o acesso a determinados lugares ou serviços. Exemplos de identificação biométrica: através da íris (parte colorida do olho), da retina (membrana interna do globo ocular), da impressão digital, da voz, do formato do rosto e da geometria da mão;
* Bloqueio de acesso: processo que tem por finalidade suspender temporariamente o acesso;
* Bluetooth - tecnologia de transmissão de dados via sinais de rádio de alta frequência, entre dispositivos eletrônicos próximos;
* Classificação da informação - atribuição, pela autoridade competente, de grau de sigilo dado à informação, documento, material, área ou instalação;
* Confidencialidade – propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;
* Contingência - descrição de medidas a serem tomadas por uma empresa, incluindo a ativação de processos manuais, para fazer com que seus processos vitais voltem a funcionar plenamente, ou num estado minimamente aceitável, o mais rápido possível, evitando assim uma paralisação prolongada que possa gerar maiores prejuízos à corporação;
* Controle de Acesso - conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;
* Cópia de Segurança (Backup) – copiar dados em um meio separado do original, de forma a protegê-los de qualquer eventualidade. Essencial para dados importantes;
* Correio Eletrônico - é um método que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação;
* Credenciais ou contas de acesso - permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física como crachá, cartão e selo ou lógica como identificação de usuário e senha;
* Criptografia – é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário (detentor da "chave secreta");
* CTIF – Comitê estratégico de tecnologia da informação da Fundação Nacional do Índio;
* Dado – representação de uma informação, instrução, ou conceito, de modo que possa ser armazenado e processado por um computador;
* COGETI – Coordenação de Gestão em Tecnologia da Informação
* Diretriz - descrição que orienta o que deve ser feito, e como, para se alcançar os objetivos estabelecidos nas políticas;
* Disponibilidade - propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;
* Download - (Baixar) copiar arquivos de um servidor (site) na internet para um computador pessoal;
* Espelhamento – Sistema de proteção de dados onde o conteúdo é espelhado em tempo real. Todos os dados são duplicados entre as áreas de armazenamento disponíveis.
* FTP (File Transfer Protocol) – (Protocolo de Transferência de Arquivo) é um protocolo da Internet para transferência de arquivos;
* Gestão de Continuidade de Negócios - Processo de gestão global que identifica as potenciais ameaças para uma organização e os impactos nas operações da instituição que essas ameaças, se concretizando, poderiam causar, e fornecendo e mantendo um nível aceitável de serviço face a rupturas e desafios à operação normal do dia-a-dia;
* Gestão de Risco – conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;
* Gestão de Segurança da Informação e Comunicações - conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;
* Hardware – É a parte física do computador, conjunto de componentes eletrônicos, circuitos integrados e periféricos, como a máquina em si, placas, impressora, teclado e outros;
* HTTP (Hyper Text Transfer Protocol) - (Protocolo de Transferência de Hipertexto) é uma linguagem para troca de informação entre servidores e clientes da rede;
* HTTPS (HyperText Transfer Protocol Secure) – (Protocolo de Transferência de Hipertexto Seguro) é uma linguagem para troca de informação entre servidores e clientes da rede, com recursos de criptografia, autenticação e integridade;
* Incidente de Segurança - é 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 transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
* Informações Críticas - são as informações de extrema importância para a sobrevivência da instituição;
* Informação sigilosa - informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo;
* Instant Messenger – (Mensageiro instantâneo) é uma aplicação que permite o envio e o recebimento de mensagens em tempo real;
* Integridade – propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
* Internet – rede mundial de computadores;
* Internet Protocol – (Protocolo de Internet) é um protocolo de comunicação usado entre duas ou mais máquinas em rede para encaminhamento dos dados;
* Intranet – rede de computadores privada que faz uso dos mesmos protocolos da Internet. Pode ser entendida como rede interna de alguma instituição em que geralmente o acesso ao seu conteúdo é restrito;
* Log - é o termo utilizado para descrever o processo de registro de eventos relevantes num sistema computacional. Esse registro pode ser utilizado para reestabelecer o estado original de um sistema ou para que um administrador conheça o seu comportamento no passado. Um arquivo de log pode ser utilizado para auditoria e diagnóstico de problemas em sistemas computacionais;
* Logon - Procedimento de identificação e autenticação do usuário nos Recursos de Tecnologia da Informação. É pessoal e intransferível;
* On line – (Estar disponível ao vivo) no contexto da Internet significa estar disponível para acesso imediato, em tempo real;
* Perfil de acesso - conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;
* Plano de Contingência - Descrever as medidas a serem tomadas por uma empresa, incluindo a ativação de processos manuais, para fazer com que seus processos críticos voltem a funcionar plenamente, ou num estado minimamente aceitável, o mais rápido possível, evitando assim uma paralisação prolongada;
* Plano de Continuidade de Negócios - documentação dos procedimentos e informações necessárias para que os órgãos ou entidades da APF mantenham seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo num nível previamente definido, em casos de incidentes;
* Peer-to-peer (P2P) – (Ponto a ponto) permite conectar o computador de um usuário a outro, para compartilhar ou transferir dados, como MP3, jogos, vídeos, imagens, entre outros;
* Política de Segurança da Informação e das Comunicações (POSIC) - 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 e comunicações;
* Protocolo - convenção ou padrão que controla e possibilita uma conexão, comunicação, transferência de dados entre dois sistemas computacionais. Método padrão que permite a comunicação entre processos, conjunto de regras e procedimentos para emitir e receber dados numa rede;
* Proxy - é um serviço intermediário entre as estações de trabalho de uma rede e a
* Internet. O servidor de rede proxy serve para compartilhar a conexão com aInternet, melhorar o desempenho do acesso, bloquear acesso a determinadas páginas;
* Quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;
* Recursos Computacionais - recursos que processam, armazenam e/ou transmitem informações, tais como aplicações, sistemas de informação, estações de trabalho, notebooks, servidores de rede, equipamentos de conectividade e infraestrutura;
* Rede Corporativa - conjunto de todas as redes locais sob a gestão da instituição;
* Rede Pública – rede de acesso a todos;
* Replicação - é a manutenção de cópias idênticas de dados em locais diferentes. O objetivo de um mecanismo de replicação de dados é permitir a manutenção de várias cópias idênticas de um mesmo dado em vários sistemas de armazenamento;
* Roteador – equipamento responsável pela troca de informações entre redes;
* Sala Cofre – é uma sala fortificada que pode ser instalada em uma instituição, provendo um local seguro de invasões e outras ameaças. São ambientes projetados para resistir a vários tipos de catástrofes. Suportam, por exemplo, temperaturas de até 1.200 graus Celsius, inundações, cortes bruscos de energia, gases corrosivos, explosões e até ataques nucleares;
* Sala Segura - sala que proporciona um ambiente seguro no Datacenter, oferecendo maior garantia no armazenamento de informações eletrônicas. Uma Sala Segura possui gerador próprio, instalação elétrica independente, paredes especiais, piso elevado, ar-condicionado, detecção e combate a incêndios, iluminação, sinalização de emergência e monitoração do ambiente;
* Segurança da Informação e Comunicações: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;
* Servidor de Rede - recurso de TI com a finalidade de disponibilizar ou gerenciar serviços ou sistemas informáticos;
* Servidor - pessoa legalmente investida em cargo público;
* Sistemas de Informação – conjunto de meios de comunicação, computadores e redes de computadores, assim como dados e informações que podem ser armazenados, processados, recuperados ou transmitidos por serviços de telecomunicações, inclusive aplicativos, especificações e procedimentos para sua operação, uso e manutenção;
* Sistema de Segurança da Informação - proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São características básicas da segurança da informação os atributos de confidencialidade, integridade, disponibilidade e autenticidade, não estando esta segurança restrita somente a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento;
* Software - são todos os programas existentes em um computador, como sistema operacional, aplicativos, entre outros;
* Site - Conjunto de páginas virtuais dinâmicas ou estáticas, que tem como principal objetivo fazer a divulgação da instituição;
* Streaming - transferência de dados (normalmente áudio e vídeo) em fluxo contínuo por meio da Internet;
* Switches – Um switch de rede é um equipamento eletrônico de comutação que funciona como um nó central numa rede no formato estrela, armazenando em memória o endereço físico de todos os computadores conectados a ele, relacionando cada endereço físico a uma de suas portas e permitindo assim a interligação entre os dispositivos conectados;
* Termo de Responsabilidade - termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso;
* Tratamento da informação - recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;
* Tratamento de Incidentes de Segurança em Redes Computacionais - serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;
* Trilhas de Auditoria - são rotinas específicas programadas nos sistemas para fornecerem informações de interesse da auditoria. São entendidas como o conjunto cronológico de registros (logs) que proporcionam evidências do funcionamento do sistema. Esses registros podem ser utilizados para reconstruir, rever/revisar e examinar transações desde a entrada de dados até a saída dos resultados finais, bem como para avaliar/rastrear o uso do sistema, detectando e identificando usuários não autorizados;
* Usuário - servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da APF, formalizada por meio da assinatura do Termo de Responsabilidade;
* VLAN (Virtual Local Area Network ou Virtual LAN) – (Rede Local Virtual) é um agrupamento lógico de estações, serviços e dispositivos de rede que não estão restritos a um segmento físico de uma rede local;
* VPN (Virtual Private Network) – (Rede Privada Virtual) é uma rede de dados privada que faz uso das infraestruturas públicas de telecomunicações, preservando a privacidade, logo é a extensão de uma rede privada que engloba conexões com redes compartilhadas ou públicas. Com uma VPN pode-se enviar dados entre dois computadores através de uma rede compartilhada ou pública de uma maneira que emula uma conexão ponto a ponto privada;
* Vulnerabilidade - conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação;
* Wireless (rede sem fio) - rede que permite a conexão entre computadores e outros dispositivos através da transmissão e recepção de sinais de rádio.