



Poder Judiciário do Estado do Rio de Janeiro
Escola da Magistratura do Estado do Rio de Janeiro – EMERJ
Biblioteca do Tribunal de Justiça do Estado do Rio de Janeiro

ANEXOS

ATO NORMATIVO TJ nº 10/2019

Estabelece normas para Gestão de Ativos de Segurança da Informação (SI) do Poder Judiciário do Estado do Rio de Janeiro (PJRJ) e dá outras providências.

ANEXO I

PADRÃO DE DISTRIBUIÇÃO DE ATIVOS DE TIC			
N.º	TIPO DE ATIVO	DESTINATÁRIO	QUANTIDADE PADRÃO
1	COMPUTADOR	Usuário Interno do PJERJ	1 Computador para cada usuário
2		Estagiários do PJERJ	1 Computador para cada 2 usuários
3		Oficial de Justiça do PJERJ	1 Computador para cada 2 usuários
4		Sala de Audiências	Nas unidades eletrônicas: 02 computadores. Nas demais unidades, apenas 01 computador.
5	MONITOR	Usuário Interno do PJERJ	1 Monitor para cada computador
6		Usuários Internos do PJERJ que utilizam o Processo Eletrônico	2 Monitores para cada computador
7		Usuários Internos da área Administrativa do PJERJ	02 monitores para usuários que operam com processo eletrônico administrativo
8		Sala de Audiências	Nas unidades eletrônicas, 03 monitores, sendo um voltado para as partes. Nas demais, 01 monitor.
9	NOTEBOOK	Magistrados do PJERJ	1 Notebook para cada Magistrado
10		Diretorias Gerais	1 notebook para cada Diretor-Geral
11	IMPRESSORA	Usuário Interno do PJERJ	1 Impressora Laser para cada 6 computadores
12		Magistrados do PJERJ	1 Impressora Colorida
13		Sala de Audiências	1 impressora preto e branco



Poder Judiciário do Estado do Rio de Janeiro
Escola da Magistratura do Estado do Rio de Janeiro – EMERJ
Biblioteca do Tribunal de Justiça do Estado do Rio de Janeiro

14		Diretorias-Gerais, Departamentos e Divisões Administrativas do PJERJ	1 Impressora Colorida
15		Demais Unidades judiciais e administrativas do PJERJ	1 Impressora Laser para cada 6 computadores
16	SCANNER	Unidades Judiciais do PJERJ	1 Scanner por local (Gabinete, Sala de Audiências, Cartório)
17		Unidades Administrativas do PJERJ	1 Scanner por local (Diretoria-Geral, Departamento, Divisão e Serviço)

ANEXO II
GLOSSÁRIO

Backup: É um termo inglês que tem o significado de cópia de segurança. É frequentemente utilizado em informática para indicar a existência de cópia de um ou mais arquivos guardados em diferentes dispositivos de armazenamento. Se, por qualquer motivo, houver perda dos arquivos originais, a cópia de segurança armazenada pode ser restaurada para repor os dados perdidos.

Condição de concorrência: É uma falha num sistema ou processo em que o resultado do processo é inesperadamente dependente da sequência ou sincronia doutros eventos. Apesar de ser conhecido em português por 'condição de corrida' uma tradução melhor é 'condição de concorrência' pois o problema está relacionado justamente ao gerenciamento da concorrência entre processos teoricamente simultâneos. O fenômeno pode ocorrer em sistemas eletrônicos, especialmente em circuitos lógicos, e em programas de computador, especialmente no uso de multitarefa ou computação distribuída.

Cross Site Script: É um tipo de vulnerabilidade do sistema de segurança de um computador, encontrado normalmente em aplicações web que ativam ataques maliciosos ao injetarem *client-side script* dentro das páginas web vistas por outros usuários. Um *script* de exploração de vulnerabilidade *cross-site* pode ser usado pelos atacantes para escapar aos controles de acesso que usam a política de mesma origem.

Downgrade: É um termo utilizado para designar o método oposto ao "*Upgrade*". Caracteriza-se por retornar um *hardware* ou *software* à um ponto anterior. Foi amplamente difundido na época do lançamento do Windows Vista, por este ser tachado como inferior ao seu antecessor por algumas pessoas, consequentemente, muitos usuários e empresas realizaram o *downgrade* para o Windows XP.

Fail-secure: É a uma forma de se projetar os sistemas que objetiva impedir que erros no sistema sejam usados como portas de entrada para ataques.

Firmware: É uma classe específica de *software* de computador que fornece controle de baixo nível para o *hardware* específico do dispositivo. Atua como o sistema operacional completo do dispositivo. Quase todos os dispositivos eletrônicos, por mais simples que seja, contêm algum *firmware*.

Hash: Uma função *hash* é um algoritmo que mapeia dados de comprimento variável para dados de comprimento fixo. Os valores retornados por uma função *hash* são chamados valores *hash*, códigos *hash*, somas *hash* (*hash sums*), *checksums* ou simplesmente *hashes*. Normalmente os sistemas não armazenam as senhas dos usuários. São aplicados cálculos que convertem as senhas em códigos *Hash* de forma a protegê-las.

Host name: É nome que é dado ao computador, ele serve para que possamos identificar uma máquina na rede, com mais facilidade.

Kernel: É um componente do Sistema Operacional, que fica escondido para maioria dos usuários domésticos. Ele gerencia os recursos do sistema e permite que os programas façam uso deles.

Log: Em computação, log de dados é uma expressão utilizada para descrever o processo de registro de eventos relevantes num sistema computacional. Esse registro pode ser utilizado para restabelecer 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.

Media Access Control (MAC): *Media Access Control* ou MAC (Português: Controle de Acesso ao Meio) é um termo utilizado em redes de computadores para designar parte da camada de enlace, camada número



Poder Judiciário do Estado do Rio de Janeiro
Escola da Magistratura do Estado do Rio de Janeiro – EMERJ
Biblioteca do Tribunal de Justiça do Estado do Rio de Janeiro

2 segundo o modelo OSI. É provedora de acesso a um canal de comunicação e o endereçamento neste canal possibilitando a conexão de diversos computadores numa rede.

Menor privilégio: é um princípio muito utilizado em segurança da informação. É uma estratégia de segurança, aplicável a diferentes áreas, que se baseia na ideia de conceder autorizações apenas quando realmente sejam necessárias para o desempenho de uma atividade específica.

Middleware: é o *software* de computador que fornece serviços para *softwares* aplicativos além daqueles disponíveis pelo sistema operacional. O *middleware* facilita aos desenvolvedores de *software* implementarem comunicação e entrada/saída, de forma que eles possam focar no propósito específico de sua aplicação.

Modelo OSI: Acrônimo do inglês *Open System Interconnection* é um modelo de rede de computador referência da ISO dividido em camadas de funções, criado em 1971 e formalizado em 1983, com objetivo de ser um padrão, para protocolos de comunicação entre os mais diversos sistemas em uma rede local (*Ethernet*), garantindo a comunicação entre dois sistemas computacionais.

POST: é um dos muitos métodos de requisição suportados pelo protocolo HTTP usado na *World Wide Web*. O método de requisição POST foi projetado para solicitar que o servidor web aceite os dados anexados no corpo da mensagem de requisição para armazenamento.

Secure Hash Algorithm (SHA): é uma função de dispersão criptográfica (ou função *hash* criptográfica) projetada pela Agência de Segurança Nacional dos Estados Unidos. Existem quatro algoritmos: SHA0, SHA1, SHA2, SHA3. A diferença mais significativa entre eles está na especificação da dispersão. A SHA-1 é a mais utilizada das funções de dispersão SHA existentes, sendo empregada em vários protocolos e aplicações amplamente utilizadas.

Storage: Equipamento que armazena dados da rede local;

Smartphones: é um telefone celular, e significa telefone inteligente, em português, e é um termo de origem inglesa. O *smartphone* é um celular com tecnologias avançadas, o que inclui programas executados um sistema operacional, equivalente aos computadores.

Tablets: é um tipo de computador portátil, de tamanho pequeno, fina espessura e com tela sensível ao toque (*touchscreen*). É um dispositivo prático com uso semelhante a um computador portátil convencional, no entanto, é mais destinado para fins de entretenimento que para uso profissional.

Timestamp: Uma marca temporal, estampa de tempo ou *timestamp* é uma cadeia de caracteres denotando a hora ou data que certo evento ocorreu. A cadeia é geralmente apresentada num formato consistente, permitindo fácil comparação entre duas marcas temporais distintas.

Tokens: é um dispositivo eletrônico gerador de senhas, geralmente sem conexão física com o computador, podendo também, em algumas versões, ser conectado a uma porta USB. Existe também a variante para *smart cards* e smartphones, que é capaz de realizar as mesmas tarefas do *token*.

Upgrade: Atualização dos componentes do *hardware* ou do *software*, de um computador.

URL: Forma padronizada de representação de diferentes documentos, mídia e serviços de rede na internet, capaz de fornecer a cada documento um endereço único.

VOIP: *Voice over Internet Protocol*, voz sobre IP é a conversação humana usando a Internet ou qualquer outra rede de computadores baseada em protocolo IP.

Protocolo IP: O IP (*Internet Protocol*) é o principal protocolo de comunicação da Internet.

Este texto não substitui o publicado no Diário Oficial.