Outrossim, com fundamento nos artigos 4º e 17 a 25 do Regimento Interno e nos termos da Resolução nº 606/2013 do Colendo Órgão Especial, **convoca o Tribunal Pleno para as eleições**, que serão realizadas exclusivamente em AMBIENTE VIRTUAL:

DATA: **04 de dezembro de 2019.**
HORÁRIO: **das 0 às 12 horas,** em primeiro escrutínio, e **das 13 às 16 horas,** se houver segundo escrutínio.
ACESSO AO SISTEMA: ***https://www.tjsp.jus.br/Eleicoes***

Comunica, ainda, que haverá **terminais disponíveis para votação no Salão do Júri** (2º andar do Palácio da Justiça), bem como para consulta da lista de abstenções, das 9 às 16 horas do dia 04/12/2019, e convida a todos para assistir a **apuração dos resultados**, que ocorrerá logo após a finalização dos respectivos escrutínios, no Salão dos Passos Perdidos (2º andar do Palácio da Justiça).

O procedimento de votação será divulgado oportunamente pelo e-mail institucional.

STI - Secretaria de Tecnologia da Informação

PORTARIA nº 9699/2019

Redefine a Política de Segurança da Informação do Tribunal de Justiça do Estado de São Paulo.

O DESEMBARGADOR PRESIDENTE DO TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO, no uso de suas atribuições legais,

CONSIDERANDO o esforço e o investimento empregado para a modernização do Tribunal de Justiça do Estado de São Paulo e de sua infraestrutura de tecnologia da informação e de comunicações;

CONSIDERANDO a importância, nesse contexto, de se registrar as diretrizes básicas que nortearão a implementação de medidas para a Segurança da Informação do Tribunal de Justiça do Estado de São Paulo;

CONSIDERANDO a necessidade de se redefinir parâmetros e orientações estratégicas de Segurança da Informação e, a partir da sua existência, normas técnicas, de usuários, específicas, procedimentos operacionais, instruções de trabalho e padrões de segurança, compondo, assim, uma Política de Segurança da Informação para a Instituição;

CONSIDERANDO a necessidade de assegurar que os gestores possam realizar o gerenciamento da estrutura de segurança da informação do Tribunal de Justiça de São Paulo, definindo, analisando e priorizando as ações necessárias para alcançar os objetivos estabelecidos para a segurança das informações;

CONSIDERANDO que a Política de Segurança da Informação deve ser aplicada a todos os Ambientes, Sistemas, Pessoas e Processos do Tribunal de Justiça de São Paulo;

CONSIDERANDO a necessidade de as diretrizes gerais da organização estarem em consonância com a Lei n º. 11.419 de 19 de dezembro de 2006, que dispõe sobre a informatização do processo judicial, e com as melhores práticas de mercado, notadamente, a norma ABNT NBR ISO/IEC 27002:2013 “Tecnologia da Informação – Técnicas de Segurança – Código de Prática para controles de segurança da informação”;

RESOLVE:

ARTIGO 1º. – O Tribunal de Justiça do Estado de São Paulo redefine sua Política de Segurança da Informação, objetivando assegurar que as informações e seus ativos, possuídos ou custodiados, sejam estabelecidos, protegidos e utilizados de forma a garantir sua confidencialidade, integridade e disponibilidade, de acordo com a lei, a ética e a confiança da comunidade.

Parágrafo Único - A Política de Segurança da Informação do Tribunal de Justiça de São Paulo (TJSP) será estabelecida por intermédio de Diretrizes Básicas de Segurança da Informação, Normas Gerais para Usuários, Normas Gerais para Técnicos, Normas Específicas, Procedimentos Operacionais e Instruções de Trabalho.

ARTIGO 2º. – As Diretrizes Básicas de Segurança da Informação do TJSP visam:

Propriedade da Informação – Garantir que toda informação gerada, em trânsito e/ou custodiada pelo TJSP por meio de tecnologia, procedimentos, pessoas e ambientes, seja de sua propriedade, e seja utilizada por usuários devidamente autorizados para fins profissionais, no estrito interesse da Instituição.

Proteção de Recursos – Proteger os recursos de tecnologia da informação e comunicação, as informações e sistemas contra a modificação, destruição, acesso ou divulgação não autorizada pelo TJSP, garantindo sua confidencialidade, integridade e disponibilidade, considerando níveis para a classificação da informação.

Segurança em Recursos Humanos - Assegurar que magistrados, servidores e partes externas entendam suas responsabilidades e estejam em conformidade com os papéis para os quais eles foram selecionados, bem como estejam conscientes e cumpram suas responsabilidades pela Segurança da Informação.

Nível de Segurança – Garantir que na criação de novos serviços internos e externos, a seleção de mecanismos de segurança e a aquisição de bens levem em consideração o balanceamento de aspectos, como risco, tecnologia, austeridade no gasto, qualidade, velocidade e impacto no negócio.

Utilização de Informações e Recursos – Assegurar que informações e recursos sejam disponibilizados para magistrados, servidores e terceiros devidamente autorizados, e que sejam utilizados apenas para as finalidades lícitas, éticas e administrativamente aprovadas e devidamente autorizadas pelo TJSP, bem como que suas configurações não sejam alteradas sem aprovação prévia, sendo os usuários adequadamente identificados.

Senhas e Autenticação – Estabelecer requisitos de controle, fornecimento, uso, proteção e substituição de senhas de acesso a sistemas, seja pelos usuários finais ou mesmo pelos usuários de instalação e manutenção (administradores) dos sistemas.

Classificação e Tratamento da Informação – Garantir que todas as informações tenham classificação de segurança colocada de maneira clara, permitindo que sejam adequadamente protegidas quanto ao seu acesso e uso. A informação e/ou a documentação consideradas de acesso restrito devem ter adequada guarda e armazenamento, assim como as sem utilidade devem ser destruídas no momento do seu descarte.

Criptografia – Assegurar o uso efetivo e adequado da Criptografia para proteger a confidencialidade, autenticidade e/ou a integridade das informações classificadas como críticas/confidenciais, de acordo com os padrões definidos pelo TJSP.

Sigilo Profissional – Assegurar que informações e recursos estejam sujeitos às regras referentes ao sigilo profissional, garantindo adequada proteção, considerando as cláusulas contratuais (terceiros) e os termos de responsabilidade e sigilo (magistrados e servidores), bem como a ciência inequívoca sobre o tratamento de dados pessoais gerais e dados pessoais sensíveis e implicações ao TJSP e aos usuários em caso de perda e vazamento de dados.

Conscientização – Assegurar que magistrados, servidores e terceiros com acesso às informações, ambientes e recursos do TJSP sejam devidamente conscientizados quanto à Segurança da Informação e tratamento de dados pessoais gerais e dados pessoais sensíveis, face às suas responsabilidades e atuação.

Monitoramento – Garantir o monitoramento do tráfego efetuado em ambientes e recursos de Tecnologia de Informação, rastreando eventos críticos e evidenciando possíveis ocorrências, dando ampla e geral divulgação dessa atividade e da possibilidade de uso desse recurso em casos de incidentes.

Gestão de Ativos – Assegurar a análise periódica dos ativos da informação, de forma que estejam devidamente inventariados e protegidos, bem como tenham um responsável, além de suas vulnerabilidades e ameaças de segurança mapeadas. Os ativos devem receber cuidados adequados à manutenção de sua existência junto à Instituição, independentemente da existência de solução de continuidade.

Desenvolvimento, Manutenção e Aquisição de Sistemas – Assegurar que o desenvolvimento e a manutenção de sistemas internos e/ou externos, bem como a aquisição de sistemas e produtos no mercado e customizados atendam a requisitos de segurança necessários para garantir informações confiáveis, íntegras e oportunas em todo o ciclo de vida da informação nesta Instituição.

Documentação de Tecnologia da Informação e Comunicação – Assegurar que os sistemas, equipamentos e procedimentos de Tecnologia da Informação e Comunicação (TIC) do Tribunal de Justiça do Estado de São Paulo tenham documentação e regras adequadas e suficientes para garantir seu entendimento e recuperação em casos de contingências.

Gerenciamentos das Operações e Comunicação – Garantir a operação segura e corrente dos recursos do processamento e transporte da informação e dos negócios em geral por intermédio da implementação de controles internos e de requisitos de segurança considerando as variáveis: pessoas, procedimentos, ambientes e tecnologia.

Terceirização ou Prestação de Serviços – Manter nível de segurança da informação adequado quanto aos aspectos desta política, quando a responsabilidade pelos procedimentos, sistemas e recursos, ou mesmo parte deles for terceirizada para outra entidade, provendo auditorias periódicas, buscando a certificação do cumprimento dos requisitos de segurança da informação e garantia de cláusula de responsabilidade e sigilo.

Capacidade – Assegurar que a utilização dos recursos seja monitorada e ajustada, e as projeções sejam feitas para as necessidades de capacidade futura, garantindo o desempenho requerido dos sistemas do TJSP.

Vulnerabilidades – Garantir que a Gestão de Vulnerabilidades seja implementada, com o objetivo de identifica-las no âmbito do TJSP. A exposição a estas vulnerabilidades deve ser avaliada e, em tempo hábil, devem ser tomadas as medidas apropriadas para lidar com os riscos associados.

Segurança para Serviços em Nuvem – Assegurar que sistemas e serviços utilizados pelo TJSP que sejam hospedados em provedores de serviços em nuvem atendam a requisitos de segurança estabelecidos por esta Instituição.

Continuidade das Atividades – Garantir a continuidade das atividades do TJSP, reduzindo a um nível aceitável a interrupção causada por desastres ou falhas de segurança, por meio da combinação de ações de administração de crise, prevenção e recuperação.

Prevenção e Resposta a Incidentes – Assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança da informação, incluindo medidas preventivas, tratamento e a comunicação sobre fragilidades e eventos de segurança da informação, através de canal de comunicação adequado para esse fim.

Cópias de Segurança das Informações (*backup/restore*) – Assegurar que a Instituição possua rotinas estabelecidas e ferramentas adequadas para realização de cópias de segurança de informações em periodicidade adequada para recuperação de dados e sistemas em caso de falhas operacionais e/ou incidentes de segurança, assim como estabelecer diretrizes para sua proteção e retenção.

Organização da Segurança da Informação – Assegurar que o gerenciamento da Segurança da Informação no TJSP seja feito pela alta direção da Instituição, por intermédio de área específica com responsabilidades de estabelecer, implementar, manter e coordenar a elaboração e revisão da Política de Segurança da Informação, bem como na avaliação e análise de assuntos a ela pertinentes, e de todos os assuntos referentes à segurança das informações custodiadas pelo TJSP, nos ambientes físicos e tecnológicos, nos procedimentos e pessoas.

Conformidade – Garantir o atendimento das leis, regulamentos e normas que regem as atividades do TJSP, de forma a obter absoluto cumprimento destes instrumentos legais e normativos. Além disso, garantir que os requisitos de segurança legais e/ou instituídos sejam cumpridos, assegurando o nível de segurança desejado. Para garantir a efetividade no atendimento às leis, regulamentos e normas, o TJSP deve promover auditoria interna em intervalos regulares.

Alegação de Desconhecimento – Esclarecer aos usuários de informações, procedimentos, ambientes e recursos do TJSP, que não é dado o direito de alegação de desconhecimento desta Política de Segurança da Informação, vez que a mesma é amplamente divulgada no âmbito interno da organização, devendo ser seguida em seu conteúdo e forma.

Sanções – Garantir que a não observância dos preceitos deste documento implicará na aplicação de sanções administrativas previstas nas normas internas do TJSP, nas cláusulas de responsabilidade e sigilo, e outros preceitos legais pertinentes à situação, pactuadas em contratos, declarações ou termos de responsabilidade, sem prejuízo, se for o caso, da responsabilização pecuniária que lhe for atribuída. Em se tratando de magistrado e servidor o ressarcimento do prejuízo não eximirá da penalidade disciplinar cabível.

Tratando-se de crime, serão os fatos levados ao conhecimento da autoridade policial, para instauração do respectivo inquérito, sem prejuízo das medidas de natureza cível.

ARTIGO 3º. – Competirá à Secretaria de Tecnologia da Informação e ao Comitê Gestor de Segurança da Informação a manutenção, atualização e monitoramento periódico dessas Diretrizes Básicas, bem como sua complementação por intermédio dos demais instrumentos que compõe a Política de Segurança da Informação do TJSP, conforme Parágrafo Único do Artigo 1 º. desta Portaria.

§ 1º – A revisão por completo das diretrizes deve ocorrer, obrigatoriamente, em período não superior a 02 (dois) anos, ou a qualquer momento, em virtude de demanda competente ou de necessidade urgente, como por exemplo: incidentes de segurança considerados significativos; nova tecnologia e/ou vulnerabilidades encontradas; ou novas necessidades legais e/ou de mercado.

§ 2º – A aprovação das alterações nas Diretrizes, bem como das Normas Gerais e Específicas, instrumentos que compõe a Política de Segurança da Informação, competirá à Presidência, depois de referendado pelo Comitê Gestor de Segurança da Informação.

ARTIGO 4º. – A Presidência do Tribunal de Justiça do Estado de São Paulo poderá determinar que eventuais monitoramentos possam ser utilizados em pesquisa para identificação de possíveis tentativas ou mesmo para a constatação de infrações contra as Políticas de Segurança da Informação do TJSP.

ARTIGO 5º. – Faz parte integrante desta Portaria, o Glossário (Segurança da Informação), elaborado pela Secretaria de Tecnologia da Informação.

ARTIGO 6º. – Exceções às Diretrizes estabelecidas nesta Portaria devem ser avaliadas e documentadas conjuntamente pela STI e Assessoria da Presidência para Assuntos de Informática.

ARTIGO 7º. – Esta Portaria entrará em vigor na data de sua publicação, ficando revogada a Portaria nº 7560/2008 e outas disposições em contrário.

REGISTRE-SE. PUBLIQUE-SE. CUMPRA-SE.
São Paulo, 30 de outubro de 2019.

(a) MANOEL DE QUEIROZ PEREIRA CALÇAS
Presidente do Tribunal de Justiça

GLOSSÁRIO – SEGURANÇA DA INFORMAÇÃO

Os termos e definições a seguir, elaborados em conjunto pela Secretaria de Tecnologia de Informação (STI) e pela Módulo Security Solutions, são aplicáveis à Política de Segurança da Informação do Tribunal de Justiça do Estado de São Paulo:

Aceitação do Risco - Decisão de aceitar um risco.

Acesso - Interação entre um usuário e a informação que permite a informação fluir de um para o outro; a capacidade de entrar em um prédio seguro (definição de segurança física).

Acesso a Informação - Direito concedido a um usuário de visualizar, modificar ou eliminar uma informação de propriedade do TJSP, armazenada em equipamentos específicos de processamento da informação.

Acesso Remoto - Ligação a um sistema ou rede através de linhas de comunicação, como as linhas telefônicas ou "*wide area network*" ou ainda "*virtual private network*", para acesso a aplicações e informações em redes distantes.

Ameaça - Causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.

Análise de Sistema - Processo de captar as ideias das diversas partes interessadas em um sistema, criando uma especificação de sistema lógica, consistente e não ambígua.

Análise de Riscos - Uso sistemático de informações para identificar fontes e estimar o risco. A análise de riscos fornece uma base para a avaliação de riscos, o tratamento de riscos e a aceitação de riscos.

Antivírus - Software e/ou hardware que protege contra vírus, *trojans, worms, spywares* e outras ameaças de ataques.

Auditoria - Exame analítico e pericial que segue o desenvolvimento das operações de processamento das informações desde a sua entrada até a sua saída, preocupando-se principalmente com a integridade, confidencialidade e disponibilidade.

Autoridade Certificadora - Entidade responsável por emitir certificados digitais. Estes certificados podem ser emitidos para diversos tipos de entidades, tais como: pessoa, computador, departamento de uma instituição, instituição etc.

Avaliação de Riscos - Processo de comparar o risco estimado com critérios de risco pré-definidos para determinar a importância do risco.

Área de Acesso Restrito/Sensível - Área localizada em espaço interno da Instituição, onde são realizados os processamentos de informações e/ou utilizada para guardar equipamentos de informática que necessitem de um controle de acesso e segurança mais rígido.

Ativo - Qualquer coisa que tenha valor para a Instituição. Todo e qualquer bem tangível ou intangível pertencente, administrado ou sob responsabilidade de um gestor, que tenha valor para a Instituição.

Ativos Físicos - Equipamentos computacionais, equipamentos de comunicação, mídias removíveis e outros equipamentos.

Ativos da Informação - Bases de dados e arquivos, contratos e acordos, documentação de sistemas, informações sobre pesquisa, manuais de usuários, material de treinamento, procedimentos de suporte ou operação, planos de continuidade de negócios, procedimentos de recuperação, trilhas de auditoria e informações armazenadas.

Ativos de Software - Aplicativos, sistemas, ferramentas de desenvolvimento e utilitários.

Ativo de Tecnologia - Bem da Instituição associado aos sistemas da informação.

Autenticidade - Propriedade que assegura que uma determinada entidade, um objeto (em análise) provém das fontes anunciadas e que não foi alvo de mutações ao longo de um procedimento. (Exemplo: garantir que um determinado usuário seja realmente quem ele diz ser).

Backup - Cópias de segurança de arquivos. Pode ser cópia de um programa, disco ou arquivo de dados feitos para fins de arquivamento ou para salvaguardar arquivos importantes na eventualidade de que a cópia ativa (original) seja danificada ou destruída.

Backup Contingencial - É a cópia de *softwares*, sistemas e dados vitais à continuidade dos negócios da Instituição. Deve ser guardada em local externo. Destina-se a recuperação em situações de contingência.

Backup Histórico - É a cópia de informações que obedecem a uma exigência legal e/ou diretrizes internas da Instituição.

Backup Operacional - É a cópia de dados, procedimentos e arquivos, que fazem parte do cotidiano do ambiente computacional e que são importantes para garantir a continuidade das operações do dia-a-dia. Destina-se à recuperação imediata.

Banco de Dados - São conjuntos de dados com uma estrutura regular que organizam informações.

Blackberry - É um dispositivo móvel (telefone celular) desenvolvido pela RIM (*Research in Motion*), que possui funções de editor de textos, acesso à internet, e-mail e tecnologia IPv6.

Bluetooth - É uma tecnologia de baixo custo para a comunicação sem fio entre dispositivos eletrônicos a pequenas distâncias.

Browser - Veja Navegador.

Cache - Banco de dados e linguagem para rotinas de acesso e transformação destes dados.

Chat Room - Forma de comunicar on-line escrevendo comentários e respondendo a outras pessoas que estão fazendo o mesmo.

Chave de Acesso - Veja *Login*.

Cavalo de Tróia - Programa que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário.

Contas de acesso e senhas - Credenciais para acesso a sistemas, informações etc.

Classificação da Informação - Procedimento de identificar e definir níveis e critérios adequados de proteção das informações que garantam a sua confidencialidade, integridade e disponibilidade de acordo com a importância para a organização.

Codificação - Procedimento de escrita dos códigos-fonte do aplicativo. Realizado a partir do projeto do sistema. Convém que tais códigos-fonte sejam armazenados com segurança e que os desenvolvedores ou analistas empreguem técnicas seguras de codificação.

Código-fonte - Arquivos em formato texto, contendo a descrição em uma linguagem de alto nível de programação, das instruções, modelos de dados e outros elementos do sistema a ser desenvolvido.

Código objeto - Trechos de código em linguagem de máquina, ainda não necessariamente completos.

Código Malicioso - Termo genérico que se refere a todos os tipos de programa que executam ações maliciosas em um computador. Exemplos de códigos maliciosos são: os vírus, malware, worms, bots, cavalos de tróia, rootkits etc.

Computação Portátil - Conceito que envolve o uso de microcomputadores portáteis como: notebook, Palmtops e similares.

Confidencialidade - Propriedade de manter a informação a salvo de acesso e divulgação não autorizados. Garantir que a informação seja acessível somente para aqueles que tenham a devida autorização.

Consequência - Resultado de um evento. Pode haver mais de uma consequência para um evento. As consequências podem ser positivas ou negativas. Entretanto, as consequências são sempre negativas no que se refere aos aspectos de segurança. As consequências podem ser expressas quantitativa ou qualitativamente.

Construção do sistema - Etapa do desenvolvimento do sistema que compreende a codificação, testes unitários, integração e testes integrados do mesmo.

Controle - Forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal. Controle é também usado como um sinônimo para proteção ou contramedida.

Controle de acesso - Prevenção e controle do uso não autorizado de um recurso. Tarefas executadas por hardware, software e controles administrativos para monitorar a operação do sistema, garantindo a integridade dos dados, identificando o usuário, registrando os acessos e as mudanças no sistema e permitindo o acesso aos usuários.

Controle de risco - Ações que implementam as decisões da gestão de riscos.

Cópias de Segurança - Vide *Backup*.

Criptografia - Método de codificação de mensagens transmitidas ou armazenadas através da utilização de cálculos matemáticos (algoritmo).

Cultura - Compreensão por parte de usuários, equipe de TI e mesmo de terceiros sobre o seu papel na garantia da segurança das informações de uma Instituição, nos procedimentos e interações realizados no seu dia-a-dia.

Custodiante da informação - Pessoa e/ou área responsável por supervisionar e implementar as medidas apropriadas de segurança para proteger os ativos de informação no nível de classificação definido pelo gestor da informação.

Desenvolvimento de Sistema - Procedimento que inclui a definição concreta em projeto de uma ideia de sistema (Análise e Projeto), a codificação deste projeto em uma linguagem de alto nível, a compilação e *linkeditagem* deste código de alto nível em linguagem de máquina (Construção ou Codificação), testes e homologação da solução (Testes) e a colocação da mesma em funcionamento (Transição).

Disponibilidade - Propriedade de manter a informação disponível para os usuários, quando estes dela necessitarem. Garantir que os usuários autorizados tenham acesso às informações e ativos associados quando necessário.

Dispositivos de Rede - São equipamentos e/ou meios físicos necessários para a comunicação entre os componentes participantes de uma rede.

Especificação de Sistema - Documento que detalha, na forma de requisitos, todos os aspectos de um sistema.

Evento - Ocorrência de um conjunto específico de circunstâncias. O evento pode ser certo ou incerto. O evento pode ser uma única ocorrência ou uma série de ocorrências. A probabilidade associada a um evento pode ser estimada para um dado período de tempo.

Evento de Segurança da Informação - Ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.

Fábrica de Software - Conjunto de profissionais especializados que através de metodologias, atualizam, desenvolvem e mantém aplicações e programas para clientes.

Firewall - Mecanismo de segurança que tem por objetivo impor restrições na comunicação entre computadores e outros dispositivos via rede.

Firewall Pessoal - *Software* ou programa utilizado para proteger um computador contra acessos não autorizados vindos da Internet. É um tipo específico de *Firewall*.

Funcionário - Pessoa que trabalha para a Instituição e que pertence a uma das categorias a seguir: (a) Magistrado e Servidor Público; (b) Pessoa Jurídica - profissional que atua na Instituição e é remunerado mediante emissão de nota fiscal; (c) Estagiário - vínculo pela universidade ou instituição específica, cursando nível superior ou técnico.

Gerência de Configuração - Conjunto de procedimentos, geralmente automatizados por um sistema, capaz de manter organizados todos os códigos-fonte de um sistema em um repositório central. A gerência de configuração garante a manutenção e identificação das versões do sistema e o acesso restrito aos desenvolvedores de cada parte do sistema.

Gestão de Riscos - Atividades coordenadas para direcionar e controlar uma Instituição no que se refere aos riscos. A gestão de riscos geralmente inclui a análise/avaliação de riscos, o tratamento de riscos, a aceitação de riscos e a comunicação de riscos.

Gestor da Informação - Pessoa responsável por uma determinada informação ou ativo de tecnologia e também pela manutenção de medidas apropriadas de segurança relacionadas ao ativo. Responde também por decisões em nome da Instituição no que diz respeito ao uso, a identificação, a classificação e a proteção de um recurso específico da informação. Chamado ainda de Proprietário da Informação.

Gestor de Segurança Patrimonial - Pessoa responsável pelo estudo, criação, submissão, aprovação e atualização de normas, implementação e administração dos recursos e ferramentas de segurança física na Instituição.

Homologação - Última etapa de testes do sistema, onde todos os requisitos devem ser verificados e validados pelo cliente final. Sistema homologado está pronto para a passagem para a produção.

HTML - Do Inglês "*HyperText Markup Language*", linguagem utilizada na elaboração/publicação de conteúdo na Internet.

HTTP - Do Inglês "*HyperText Transfer Protocol*", protocolo utilizado para transferir páginas Web entre um servidor e um cliente (por exemplo, o navegador).

Incidente de Segurança da Informação - Um incidente de segurança é indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.

Identificação de Riscos - Procedimento para localizar, listar e caracterizar elementos de risco.

Informação - É um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma Instituição e consequentemente necessita ser adequadamente protegida. A informação está exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades.

Informação Classificada - Toda informação pertencente ou sob custódia do TJSP que tenha um grau de sigilo definido pelo procedimento de classificação da informação.

Integridade - Propriedade de manter a informação acurada, completa e atualizada. Garantir a precisão das informações e dos métodos de processamento aos quais ela é submetida.

Inventário - É a atividade de catalogar os ativos de informação.

Inventário de Ativos - É a identificação, documentação e controle de todos os ativos, e que indique sua importância para a Instituição. O inventario de ativos deve incluir todas as informações necessárias que permitam recuperar de um desastre, incluindo o tipo do ativo, formato, localização, informações sobre cópias de segurança, informações sobre licenças e a importância do ativo para o negócio.

Java - Linguagem de programação multi-plataforma, onde o mesmo código-objeto pode ser executado em diversas plataformas de hardware e sistema operacional, como Windows, Linux etc.

LDAP - *Lightweight Directory Access Protocol*, ou seja, Protocolo de Leve Acesso a Diretórios. Como o nome sugere, é um protocolo leve para acessar serviços de diretório.

Linguagem de máquina - Sequência de códigos entendíveis pelo processador do computador.

Linguagem de programação - São estruturas de sintaxe e gramática parecidas com a linguagem humana ou, pelo menos, capazes de serem adequadamente entendidas pela mente humana, e também de fácil tradução para a linguagem de máquina, ou código objeto. As linguagens mais utilizadas atualmente são: Java, Visual Basic, ASP, PHP, Delphi (Pascal) etc.

Linkeditagem - Procedimento da união dos códigos objeto gerados por vários arquivos de código-fonte, gerando o sistema completo. Nem todas as linguagens utilizam este tipo de procedimento.

Local Area Network (LAN) - É uma rede utilizada na interconexão de equipamentos processadores com a finalidade de troca de dados. Tais redes são denominadas locais por cobrirem apenas uma área limitada.

Login - Identificação de usuário para entrada nos sistemas.

Logon - Procedimento de entrada de usuário nos sistemas.

Logoff - Procedimento de encerramento de uma sessão de usuário.

Malware - Do Inglês *Malicious Software* (software malicioso). Veja Código malicioso. ***Mecanismos*** - Ferramental técnico (hardware e software) utilizado para implementação de controles de segurança como autenticação, restrições de acesso e auditoria.

Metodologia de Desenvolvimento - Documento que descreve, de maneira formal, como deve ser feito o desenvolvimento de um sistema na Instituição. Geralmente adaptado de um modelo de metodologia como Análise Essencial, Análise Estruturada, AOO (Análise Orientada a Objetos), RUP (*Rational Unified Process*), MSF (*Microsoft Solutions Framework*), CMM, CMMI, dentre outros.

Mitigação - Limitação de quaisquer consequências negativas de um determinado evento.

Mudança no ambiente computacional - É toda e qualquer modificação aplicada em qualquer um dos componentes dos recursos computacionais, seja hardware, sistema operacional, sistemas, banco de dados, rede, serviços de rede, software de apoio e produto.

Não repúdio - Conceito de que a autoria de determinada ação/operação não possa ser negada pelo seu executor.

Navegador - É um programa (software) que habilita seus usuários a interagirem com sistemas e/ou conteúdo Web.

Notebook - É um computador portátil, leve, designado para poder ser transportado e utilizado em diferentes lugares com facilidade.

OTA - do Inglês (*Over the Air*), consiste em uma tecnologia empregada nas versões mais recentes do GSM, e permite, remotamente através da rede GSM, alterar, atualizar ou remover dados do cartão SIM ou de memória do dispositivo Smartphone, sem haver a necessidade de contato ou alteração física no mesmo.

Passagem para Produção - É um conjunto de procedimentos destinados a colocar em produção e à disposição do usuário, um sistema que foi desenvolvido. Além da instalação do sistema, medidas de segurança, documentação, treinamento, dentre outras, podem ser adequadas e necessárias.

Password - Senha - Veja Senha de Acesso.

Patch - Programas para correções de falhas no sistema.

PDA - É um computador de dimensões reduzidas, com grande capacidade computacional, cumprindo as funções de agenda e sistema informático de escritório elementar, com possibilidade de interconexão com um computador pessoal e uma rede de dados sem fios.

Perímetro de Segurança - Toda área demarcada e protegida cujo acesso é restrito e controlado.

Planejamento da Continuidade do Negócio - Preparação para enfrentar situações de potencial interrupção das atividades de negócio.

Plano de Continuidade de Negócio - É um plano para proteger os processos críticos de negócio de situações de emergência, operações de backup e recuperação após desastre, mantido por uma atividade que faz parte de um programa de segurança que garanta a disponibilidade dos recursos críticos e facilite a continuidade de operações nessa situação.

Política - Intenções e diretrizes globais formalmente expressas pela direção.

Política de Segurança da Informação (PSI) - É um conjunto de diretrizes, normas, procedimentos e instruções geradas pela organização para conhecimento e prática de seus funcionários, no sentido de proteger seus ativos de informação em quaisquer âmbitos que estejam, tais como tecnologia, procedimentos, pessoas e ambientes.

Probabilidade - Grau de possibilidade de que um evento ocorra.

Projeto de Sistema - Procedimento que, a partir de uma especificação de sistema lógica e consistente, define como tais requisitos serão atendidos na plataforma, ambiente e linguagens adotadas para o sistema. Geralmente inicia-se pela definição dos casos de uso, seguido pela indicação em diagrama de blocos, ou classes, com diagramas adicionais para auxiliar no entendimento da solução ao problema. Varia muito conforme a metodologia de desenvolvimento empregada.

Projeto Físico do Sistema - Parte final do projeto do sistema onde se define os diagramas de classe, estruturas de dados, declaração de interfaces, dentre outros. Varia muito conforme a metodologia de desenvolvimento empregada.

Projeto Lógico de Sistema - Parte inicial do projeto do sistema onde se define os casos de uso, eventos externos e forma geral do sistema. Varia muito conforme a metodologia de desenvolvimento empregada.

Proprietário da Informação - Vide Gestor da Informação.

Protocolo de Comunicação - É a "linguagem" que os diversos dispositivos de uma rede utilizam para se comunicar.

Recurso de Informação - Tudo que faz parte dos componentes de tecnologia da informação da Instituição (ex.: *hardware, software*, documentação, dados).

Recursos de Segurança Física - Barreiras físicas e ações de segurança em torno de uma área, conjunto de áreas, ambientes e/ ou instalações da Instituição.

Redução de Riscos - Ações tomadas para reduzir a probabilidade, as consequências negativas, ou ambas, associadas a um risco.

Registro de Eventos - Registro de atividades gerado por programas de computador. ***Requisitos*** - Frases adjetivas, preferencialmente afirmativas, que descrevem um aspecto desejado ou necessário do sistema. São divididos em requisitos funcionais e não-funcionais. Podem ser ordenados conforme o grau de importância num sistema.

Requisitos de Segurança - São os requisitos funcionais que expressam as necessidades de segurança do aplicativo. Devem estar associadas a ameaças, aspectos da política de segurança da Instituição ou legislação aplicável ao sistema.

Requisitos Funcionais - São aqueles que descrevem uma funcionalidade ou algo que o sistema tem que fazer. Uma parte importante dos requisitos funcionais são os requisitos de segurança.

Requisitos Não-funcionais - Descrevem características importantes do sistema, porém não associadas a algo que o sistema tem que fazer, por exemplo, o prazo de desenvolvimento do sistema, o nível de testes a que este será submetido, dentre outros.

Retenção do Risco - Aceitação do ônus da perda ou do benefício do ganho associado a um determinado risco.

Risco - Combinação da probabilidade de um evento e de suas consequências. Geralmente o termo "risco" é utilizado apenas quando há pelo menos a possibilidade de consequências negativas. Em alguns casos, o risco decorre da possibilidade de desvio em relação ao evento ou resultado esperado.

Risco Residual - Risco remanescente após o tratamento do risco.

Segurança - Ausência de riscos inaceitáveis.

Segurança da Informação - Preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas.

Segurança Física - Conjunto de medidas destinadas à proteção e integridade dos ativos físicos da Instituição.

Segurança Física Condominial - Políticas, procedimentos e meios de segurança física implementados pelo condomínio nas áreas internas e externas do prédio onde a Instituição está instalada (recursos compartilhados com outras empresas).

Segurança Física Corporativa - Políticas, procedimentos e/ou recursos de segurança física implementados pela Instituição para serem observados exclusivamente nas suas instalações, mesmo que dentro de um prédio ou instalação compartilhados com outras empresas.

Segurança Física Perimetral - Políticas, procedimentos e/ou recursos de segurança física implementados nas áreas de perímetro externo, ao redor da Instituição.

Senhas - Veja Senha de Acesso

Senha de Acesso - É um conjunto de caracteres secreto (*password*) de conhecimento somente pelo usuário para autenticar seu acesso a um sistema em especifico.

Serviços de Diretório - Sistemas desenvolvidos para gerenciar, armazenar e organizar informações sobre os recursos e usuários de uma ou mais redes de computadores.

Servidores - São computadores com alta capacidade de processamento e armazenagem que tem por função disponibilizar serviços, arquivos ou aplicações a uma rede.

Sistema de Gerência de Configuração - Sistemas automatizados destinados a fazer a gerência de configuração dos códigos-fonte do sistema. Os mais comuns são: *Source Safe, Clear Case, PVCS, CVS, Change-man*, dentre outros.

Sistema em Produção - Diz-se do sistema que já está operando no ambiente final previsto para tal, acessado pelos usuários reais.

Sistema Operacional - É um programa ou um conjunto de programas cuja função é servir de interface entre um computador e o usuário.

Smartphone - É um telefone móvel com funcionalidade computacional estendida por meio de programas executados no seu Sistema Operacional, possibilitando interconexão com um computador pessoal e/ou uma rede de dados sem fios.

SPAM - Termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de grupos e/ou pessoas.

Spyware - Termo utilizado para se referir a uma grande categoria de software que tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros. Podem ser utilizados de forma legítima, mas, na maioria das vezes, são utilizados de forma dissimulada, não autorizada e maliciosa.

SSL - Do Inglês " *Secure Sockets Layer* ". Protocolo que fornece confidencialidade e integridade na comunicação entre um cliente (navegador) e servidores, através do uso de criptografia.

Termo de Responsabilidade e Sigilo (TRS) - É um documento contendo uma declaração formal em que o funcionário manifesta de livre e espontânea vontade seu conhecimento e adesão à Política de Segurança da Informação da Instituição, reconhecendo seus deveres, obrigações e responsabilidades perante a Instituição, dentro deste assunto.

Teste de Invasão - Também chamado de teste de penetração. Teste de segurança onde se utilizam ferramentas de ataque para a verificação da robustez do sistema contra ataques externos ou internos.

Teste Funcional - Teste das funcionalidades do sistema. Verifica-se se o sistema atende a todos os requisitos funcionais indicados na especificação do sistema. Inclui o teste funcional de segurança, que testa os requisitos de segurança.

Teste Funcional de Segurança - Parte do teste funcional que visa identificar se os requisitos de segurança são atendidos.

Teste Integrado - Teste, ainda no ambiente de desenvolvimento, de todo o sistema em funcionamento.

Teste Unitário - Teste de um componente ou função do sistema, ainda no ambiente de desenvolvimento.

Tipos de Ativos - (a) Ativos Físicos, (b) Ativos da Informação, (c) Ativos de *Software*, (d) Serviços (serviços de computação e comunicações, utilidades em geral, por exemplo, aquecimento, iluminação, eletricidade e refrigeração), (e) Pessoas e suas qualificações, habilidades e experiências, e (f) Intangíveis, tais como reputação e a imagem da Instituição.

Transferência de Riscos - Compartilhamento com uma outra parte do ônus da perda ou do benefício do ganho associado a um risco.

Tratamento de Riscos - Procedimento de seleção e implementação de medidas para modificar um risco.

Trojan horse - Cavalo de Tróia - Veja Cavalo de Tróia.

Usuário - Toda categoria de pessoa - magistrado, servidor público, estagiário, prestador de serviço - quando devidamente autorizada, por meio formal, a ter acesso à informação da Instituição.

Violação - Tentativa frustrada ou bem sucedida de acesso indevido.

Vírus - Programa capaz de infectar outros programas e arquivos de um computador. Para realizar a infecção, o vírus embute uma cópia de si mesmo em um programa ou arquivo, que quando executado também executa o vírus, dando continuidade ao procedimento de infecção.

Virtual Private Network (VPN) - Termo utilizado para se referir à construção e/ou utilização de uma rede privada utilizando redes públicas (por exemplo, a Internet) como meio de conexão. Estes sistemas utilizam criptografia e outros mecanismos de segurança para garantir que somente usuários autorizados possam ter acesso a uma rede privada e que nenhum dado será interceptado enquanto estiver passando pela rede pública.

Vulnerabilidade - Fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

Webmail - Permite o acesso ao correio eletrônico através de um navegador internet (exemplo: Internet Explorer).

Wide Area Network (WAN) - É uma rede de computadores que abrange uma grande área geográfica, com frequência um país ou continente.

WWW - Do Inglês " ***World Wide Web*** ", definição de todos os recursos e usuáriosna Internet que estão usando o HTTP.

SJ - Secretaria Judiciária

COMUNICADO Nº 380/2019

O Excelentíssimo Senhor Desembargador Fernando Antonio Torres Garcia, Presidente da Seção de Direito Criminal do Tribunal de Justiça, COMUNICA que a distribuição dos feitos em grau de recurso prevista para o dia 15 de novembro, será realizada no dia 14 de novembro do corrente, quinta-feira, às 09 horas, na sala 35 do prédio do Tribunal de Justiça, localizado na Rua Agostinho Gomes nº 1225 (Praça Nami Jafet nº 235) – Bairro do Ipiranga, com a supervisão da Presidência da Seção de Direito Criminal.

(12, 13 e 14/11/2019)

SEÇÃO I

ATOS DO TRIBUNAL DE JUSTIÇA

Subseção I: Atos e comunicados da Presidência

SECRETARIA DA PRESIDÊNCIA

Diretoria de Relações Institucionais - SPr 4

COORDENADORIA DE CERIMONIAL
CONVITE

O Presidente do Tribunal de Justiça do Estado de São Paulo, Desembargador **Manoel de Queiroz Pereira Calças**, tem a honra de convidar os Senhores Desembargadores e Juízes de Direito da 23ª, 24ª, 25ª, 32ª e 33ª Circunscrições Judiciárias para o **Encontro Regional de Trabalho da 3ª Região Administrativa Judiciária**, a realizar-se no dia **14 de novembro** de 2019 (quinta-feira), das **11 às 12 horas,** no **prédio da DARAJ**, na Rua Amazonas, 1-41 – Jardim Paulistano – Bauru/SP.