ATO TRT 11ª REGIÃO Nº 41/2019/SGP

Altera e republica o Ato TRT 11ª Região Nº 055/2010/SGP que dispõe sobre a Política de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 11ª Região.

O PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 11ª REGIÃO, no uso de suas atribuições legais e regimentais,

Considerando a necessidade de estabelecer diretrizes e padrões para garantir um ambiente tecnológico controlado e seguro de forma a oferecer todas as informações necessárias aos processos deste Tribunal com integridade, confidencialidade e disponibilidade.

Considerando que a credibilidade da instituição na prestação jurisdicional deve ser preservada;

Considerando a constante preocupação com a qualidade e celeridade na prestação de serviços à sociedade.

Considerando a necessidade de regulamentar o acesso à rede de computadores, aos sistemas informatizados, aos bancos de dados, à internet, à intranet, à rede sem fio, às redes sociais, ao teletrabalho e ao VPN (Virtual Private Network – Rede Privada Virtual);

Considerando a necessidade de regulamentar o uso do serviço de correio eletrônico corporativo, da estrutura de diretórios na rede de computadores, de programas e aplicativos, de equipamentos de tecnologia da informação, da utilização de serviços em nuvem;

Considerando a necessidade de regulamentar as práticas de mesa limpa e tela limpa, de gestão de riscos, de continuidade e de vulnerabilidades do ambiente tecnológico; bem como o controle, monitoramento e a auditoria de recursos tecnológicos no âmbito do Tribunal;

Considerando os danos potenciais decorrentes de acessos a sítios e aplicativos indevidos ou inadequados na internet, da instalação de programas não homologados e inadequados, bem como o risco de contaminação de programas maliciosos nas estações de trabalho e nos dispositivos móveis;

Considerando a Lei de Acesso à Informação, Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto no inc. XXXIII do art. 5º, no inc. II do § 3º do art. 37 e no § 2º do art. 216 da Constituição da República e dá outras providências;

Considerando a Lei Geral de Proteção de Dados, Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre a proteção de dados pessoais;

Considerando o Ato N° 27/2018/SGP, que disciplina a composição e as atribuições do Comitê de Segurança da Informação do Tribunal Regional do Trabalho – COMITÊ DE SEGURANÇA DA INFORMAÇÃO;

Considerando a Norma Complementar nº 03/IN01/DSIC/GSIPR, que estabelece diretrizes para elaboração de Política de Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal;

Considerando a Norma Complementar nº 14/IN01/DSIC/GSIPR, e sua Revisão 1, que estabelece princípios, diretrizes e responsabilidades relacionados à Segurança da Informação (SI) para o tratamento da informação em ambiente de Computação em Nuvem e em órgãos e entidades da Administração Pública Federal (APF), direta e indireta;

Considerando o conjunto de normas ABNT NBR ISO/IEC 27000, que especificam os requisitos para estabelecer, implementar, manter e melhorar continuamente o sistema de gestão da segurança da informação;

Considerando as melhores práticas para a proteção e para o controle da informação referenciadas nas disciplinas do COBIT e nos processos da biblioteca ITIL;

RESOLVE:

Art. 1º Atualizar a Política de Segurança da Informação (PSI) no âmbito do Tribunal Regional do Trabalho da 11ª Região, cabendo aos usuários a observância de suas disposições e às unidades administrativas, no âmbito de suas competências, a implementação e o acompanhamento de ações para a segurança da informação.

Art. 2º Para efeitos deste ato aplicam-se as seguintes definições:

I – Confidencialidade: Garantia de que o acesso à informação seja obtido apenas por pessoas autorizadas;

II – Integridade: Salvaguarda de exatidão e completeza da informação e dos métodos de processamento;

III – Disponibilidade: Garantia de que usuários autorizados obtenham acesso à informação e aos recursos correspondentes sempre que necessários;

IV – Ativo**:** a informação e todos os recursos e dispositivos que a manipulam;

V – Ativo de Tecnologia de Informação e Comunicação (ATIC): qualquer equipamento, dispositivo, serviço, infraestrutura ou sistema de processamento da informação, bem como as instalações físicas que os abrigam;

VI – Segurança da Informação: preservação da confidencialidade, da integridade e da disponibilidade da informação;

VII – Recurso de tecnologia de informação: qualquer equipamento, dispositivo, serviço, infraestrutura ou sistema de processamento da informação, ou as instalações físicas que os abriguem;

VIII - Incidente de segurança da informação: é identificado 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;

IX – Usuários: magistrados e servidores ocupantes de cargo efetivo ou em comissão, requisitados e cedidos, e, desde que previamente autorizados, empregados de empresas prestadoras de serviços terceirizados, consultores, estagiários, e outras pessoas que se encontrem a serviço da Justiça do Trabalho, utilizando em caráter temporário os recursos tecnológicos do TRT;

X – Plano de Continuidade do Negócio: conjunto de ações de prevenção e procedimentos de recuperação a serem seguidos para proteger os processos críticos de trabalho contra efeitos de falhas de equipamentos, acidentes, ações intencionais ou desastres naturais significativos, assegurando a disponibilidade das informações.

TÍTULO I

DAS REFERÊNCIAS (FUNDAMENTAÇÃO LEGAL)

Art. 3º Foram observadas as seguintes referências legais e normativas na elaboração desta PSI:

I - Decreto nº 3.505/2000 da Presidência da República, no Acórdão de nº 2471/2008 do Tribunal de Contas da União e na Resolução nº 90/2009 do Conselho Nacional de Justiça.

II - Decreto Nº 7.845 de 14 de novembro de 2012. Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento. Publicado em 16.11.2012;

III - Lei N° 8.112 de 11 de novembro de 1990. Dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais;

IV - Decreto N° 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional;

V - Instrução Normativa GSI nº 1, de 13 de junho de 2008. Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e

indireta, e dá outras providências. E as subsequentes Normas complementares IN01/DSIC/GSIPR 01, 02, 03, 04, 05, 06, 07 e 08;

VI - Aplicação de boas práticas em Tecnologia da Informação recomendadas pela Corte de Contas da União (TCU) e assinaladas na edição do Acórdão 2.585/2012-TCU-Plenário e Acórdão 1.233/2012-TCU-Plenário;

VII - ABNT (2013) "Tecnologia da Informação – Sistema de gestão da segurança da informação – Requisitos (NBR ISO/IEC 27001)". ABNT. 2013;

VIII - ABNT (2013) "Tecnologia da Informação – Código de prática para a gestão da segurança da informação (NBR ISO/IEC 27002)". ABNT. 2013.

TÍTULO II

DOS PRINCÍPIOS

Art. 4° A PSI neste Tribunal é guiada pelos seguintes princípios:

I – Responsabilidade: as responsabilidades primárias e finais pela proteção de cada ativo e pelo cumprimento de processos de segurança devem ser claramente definidas;

II – Conhecimento: para garantir a confiança no sistema, os administradores, os fornecedores e os usuários de um sistema de informação devem ter ciência de todas as normas e procedimentos de segurança necessários;

III – Ética: todos os direitos e interesses legítimos de usuários, intervenientes e colaboradores devem ser respeitados ao prover um sistema de informação e ao estabelecer um sistema de segurança;

IV – Legalidade: processos de segurança devem levar em consideração os objetivos e a Missão do TRT da 11ª Região, bem como as leis, normas e políticas organizacionais, administrativas, comerciais, técnicas e operacionais;

V – Integração: os processos de segurança devem ser coordenados e integrados entre si e com os demais processos e práticas da organização a fim de criar um sistema de segurança da informação coerente;

VI – Celeridade: as ações de resposta a incidentes e de correções de falhas de segurança devem ser tomadas o mais rápido possível;

VII – Revisão: os sistemas de segurança devem ser reavaliados periodicamente, uma vez que os sistemas de informação e os requisitos de segurança variam com o tempo.

TÍTULO III

DA APLICABILIDADE

Art. 5º Esta política e seus documentos complementares devem ser interpretados de forma restritiva, dentro do princípio de aplicação do menor privilégio possível, ou seja, tudo o que não estiver expressamente permitido só deve ser realizado após prévia autorização, devendo ser levada em consideração a análise de risco e a necessidade do negócio à época de sua solicitação.

Art. 6º Esta política e seus documentos complementares devem ser divulgados aos usuários, visando a sua disponibilidade para todos que se relacionam com este Tribunal, ou que, direta ou indiretamente, são impactados.

Art. 7º Esta política se aplica, no que couber, às atividades de todos os magistrados, servidores, colaboradores, consultores externos, estagiários e prestadores de serviço que exercem atividades no âmbito deste Tribunal ou quem quer que venha a ter acesso a dados ou informações protegidas por esse regulamento.

Art. 8º O uso adequado dos recursos de tecnologia da informação visa a garantir a continuidade da prestação jurisdicional deste Tribunal.

§1º Os recursos de tecnologia da informação pertencentes a este Tribunal, disponíveis para o usuário, serão utilizados em atividades estritamente relacionadas às suas funções institucionais.

§ 2º A utilização dos recursos de tecnologia da informação será monitorada, sendo seus registros mantidos pela Secretaria de Tecnologia da Informação e Comunicações.

Art. 9º As informações geradas, acessadas, manuseadas, armazenadas ou descartadas no exercício das atividades realizadas pelos usuários, bem como os demais ativos intangíveis e tangíveis disponibilizados, são de propriedade e direito de uso exclusivo deste Tribunal e devem ser empregados unicamente para fins profissionais.

§1º Toda informação gerada neste Tribunal deverá ser classificada em termos de seu valor, requisitos legais, sensibilidade, criticidade e necessidade de compartilhamento.

§2º É vedado o uso das marcas, identidade visual e qualquer outro sinal distintivo, atual e futuro, deste Tribunal em qualquer forma ou mídia, inclusive na Internet e nas mídias sociais, sem a prévia e formal autorização para tanto, até mesmo no âmbito acadêmico.

Art. 10º Os usuários devem utilizar apenas os recursos disponibilizados por este Tribunal para classificar a informação e aplicar os respectivos controles estabelecidos em documento específico, em todo o ciclo de vida da informação, ou seja, desde a sua recepção ou produção até o seu descarte.

§1º É vedada a revelação de qualquer informação de propriedade ou sob a responsabilidade deste Tribunal, por seus usuários sem a prévia e formal autorização para tanto, inclusive no âmbito acadêmico, excetuando-se a hipótese de que a informação esteja classificada como “pública”.

Art. 11º Os Ativos de Tecnologia de Informação e Comunicação de propriedade deste Tribunal devem ser utilizados apenas para fins profissionais, de modo lícito, ético, moral e aprovado administrativamente.

§1º O usuário deve utilizar apenas Ativos de Tecnologia de Informação e Comunicação previamente homologados e autorizados pela área de Tecnologia da Informação deste Tribunal, sejam eles onerosos, gratuitos, livres ou licenciados.

§2º Todos os Ativos de Tecnologia de Informação e Comunicação em uso no ambiente corporativo deste Tribunal devem atender às recomendações de seus fabricantes ou desenvolvedores, no que diz respeito à manutenção, atualizações e correções de falhas técnicas de segurança.

§3º Os Ativos de Tecnologia de Informação e Comunicação que permitem mais mobilidade ao usuário devem ser utilizados somente quando fornecidos ou autorizados por este Tribunal. Além disso, devem estar diretamente relacionados a uma justificativa do negócio, com motivo estritamente profissional, no âmbito das atribuições do usuário.

§4º O uso de Ativos de Tecnologia de Informação e Comunicação particulares na execução de qualquer atividade profissional ou na interação com os ambientes físicos ou lógicos ou com as informações deste Tribunal deve ocorrer somente após solicitação formal e fundamentada do usuário solicitante e autorização expressa do seu chefe imediato e da SETIC.

Art. 12º É vedado aos usuários o uso de repositórios digitais não homologados pela área de Tecnologia da Informação para armazenar ou publicar informações de propriedade ou sob a responsabilidade deste Tribunal, salvo casos onde a informação esteja classificada como “pública”.

Art. 13º É vedada aos usuários a instalação e o uso de softwares de comunicação instantânea não homologados pela área de Tecnologia da Informação nos Ativos de Tecnologia de Informação e Comunicação deste Tribunal.

Art. 14º A participação do usuário nas redes sociais por meio dos Ativos de Tecnologia de Informação e Comunicação deste Tribunal deve estar relacionada às atividades profissionais.

Parágrafo único: O usuário é responsável por sua conduta no uso das redes sociais, observado o código de ética do Tribunal.

Art. 15º Este Tribunal controla o acesso físico e lógico às suas dependências e aos seus Ativos de Tecnologia de Informação e Comunicação. Desse modo, cada usuário deve possuir uma credencial de acesso de uso individual, intransferível e, sempre que aplicável, de conhecimento exclusivo.

§1º O usuário é responsável pelo uso e sigilo de suas credenciais de acesso, onde não é permitido, em qualquer hipótese, compartilhar, revelar ou fazer uso não autorizado de credenciais de terceiros, sendo responsável direto pela conduta ou/e dano causado, mediante apuração de responsabilidade em processo administrativo disciplinar devidamente instaurado.

Art. 16º Os sistemas e processos suportados pelos Ativos de Tecnologia de Informação e Comunicação deste Tribunal devem ser confiáveis, íntegros e disponíveis, a quem deles necessite para execução de suas atividades profissionais.

§1º Este Tribunal deve estabelecer perímetros de segurança para proteção de seus Ativos de Tecnologia de Informação e Comunicação críticos, bem como implementar controles de identificação e registro de acesso somente de usuários autorizados.

Art. 17º Os relacionamentos e contratações, inclusive de usuários, em que ocorra o compartilhamento de informações deste Tribunal ou a concessão de qualquer tipo de acesso aos seus ambientes e Ativos de Tecnologia de Informação e Comunicação, devem ser precedidos por termos de confidencialidade e cláusulas contratuais relacionadas à Segurança da Informação e Comunicação.

Art. 18º Cláusulas contratuais que dispõem sobre a realização de auditorias eventuais ou periódicas para certificar a conformidade com a POLÍTICA DE SEGURANÇA DA INFORMAÇÃO e seus documentos complementares devem ser estabelecidas junto aos prestadores de serviço deste Tribunal.

Art. 19º O desenvolvimento interno e/ou externo de softwares, assim como a aquisição de softwares e produtos no mercado, deve possuir requisitos de segurança para garantir informações confiáveis, íntegras, autênticas e oportunas.

Art. 20º Este Tribunal deve possuir documentação adequada e suficiente para garantir a compreensão e rápida recuperação em situações de contingência de seus sistemas e processos que envolvam seus Ativos de Tecnologia de Informação e Comunicação.

Art. 21º Este Tribunal deve definir e manter um processo de salvaguarda e restauração das informações e de seus Ativos de Tecnologia de Informação e Comunicação críticos, a fim de atender aos requisitos operacionais e legais, além de garantir a continuidade do negócio em caso de falhas ou incidentes.

Art. 22º Este Tribunal deve analisar, em intervalos regulares, seus processos e Ativos de Tecnologia de Informação e Comunicação, visando assegurar que estes estejam devidamente mapeados, inventariados e com seus gestores identificados e cientes, assim como suas vulnerabilidades e ameaças de segurança identificadas.

Art. 23º Este Tribunal realiza o monitoramento, inclusive de forma remota, de todo acesso e uso de suas informações, Ativos de Tecnologia de Informação e Comunicação e seus ambientes físicos e lógicos, visando à eficácia dos controles implantados, a proteção de seu patrimônio e sua reputação, possibilitando ainda a identificação de eventos ou alertas de incidentes referente à segurança da informação.

Art. 24º Este Tribunal, sempre que considerar necessário, pode auditar ou inspecionar os Ativos de Tecnologia de Informação e Comunicação que interagem com seus ambientes lógicos, físicos ou com suas informações.

Art. 25º O andamento e o resultado de uma mudança, principalmente nos sistemas e infraestrutura tecnológica deste Tribunal devem preservar os controles relacionados à disponibilidade, integridade, sigilo e autenticidade das informações.

Art. 26º No escopo das ações de Segurança da Informação e Comunicação, os procedimentos de Gestão da Continuidade de Negócios devem ser executados em conformidade com os requisitos de segurança da informação e comunicação estabelecidos para proteção dos Ativos de Tecnologia de Informação e Comunicação críticos.

Art. 27º Este Tribunal deve possuir e manter um programa de revisão e atualização bienal desta POLÍTICA DE SEGURANÇA DA INFORMAÇÃO e de seus documentos complementares visando à garantia que todos os requisitos de segurança técnicos e legais implementados estejam sendo cumpridos, atualizados e em conformidade com a legislação vigente.

Art. 28º Este Tribunal deve possuir um Programa Anual de Conscientização em Segurança da Informação e Comunicação para capacitação e disseminação da cultura de Segurança da Informação junto aos seus usuários.

Art. 29º Este Tribunal deve manter um COMITÊ DE SEGURANÇA DA INFORMAÇÃO, com a composição prevista no art. 17º do Ato Nº 27/2018/SGP. Os representantes da SETIC no Comitê deverão assessorar a implementação das ações relacionadas à Segurança da Informação e Comunicação, além de avaliar os controles e incidentes relacionados.

Art. 30º Este Tribunal deve manter uma Equipe de Resposta a Incidentes em Segurança da Informação e Cibernética, com composição fixa ou variável, competente e preparada para receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança da informação e cibernética.

§1º Este Tribunal deve possuir um canal de comunicação divulgado aos seus usuários para reportar imediatamente os possíveis casos de incidentes de segurança da informação e cibernética, podendo fazer de modo formal ou com uso do recurso de denúncia anônima.

Art. 31º A utilização de serviços em nuvem, hospedados fora do ambiente computacional do Tribunal, deverá passar por uma análise prévia visando assegurar as garantias fundamentais no tratamento das informações pessoais, segundo preconizam os incisos e os parágrafos do artigo 31 da Lei 12.527, de 18 de novembro de 2011 – Lei de Acesso à Informação.

Art. 32º As alterações desta política de segurança da informação e de seus documentos complementares devem ser devidamente comunicadas aos seus usuários por este Tribunal.

§1º As exceções que ocorram de forma exclusiva e excepcional a essa política de segurança da informação, devem ser formalizadas e fundamentadas pelo usuário solicitante, e podem ser revogadas a qualquer tempo, por mera liberalidade deste Tribunal, conforme previsto em procedimento específico.

§2º As medidas alternativas às previstas nesta política de segurança da informação, realizadas de modo excepcional para mitigar riscos em ocasiões específicas e justificáveis, inclusive em situações emergenciais, devem ser formalizadas e fundamentadas pelo usuário de forma imediata ou assim que possível ao COMITÊ DE SEGURANÇA DA INFORMAÇÃO.

§3º Qualquer dúvida relativa a esta política de segurança da informação deve ser encaminhada a Seção da Central de Serviços por meio do e-mail ti.central@trt11.jus.br.

§4º Os incidentes de segurança da informação identificados devem ser avaliados pelo COMITÊ DE SEGURANÇA DA INFORMAÇÃO. Ao constatar uma violação, o COMITÊ DE SEGURANÇA DA INFORMAÇÃO deve encaminhar o relatório para a Secretaria Geral da Presidência, que após análise, poderá instaurar e apurar as responsabilidades dos envolvidos em procedimento administrativo disciplinar, visando aplicação de sanções administrativas cabíveis previstas em cláusulas contratuais, regimento pessoal e outros documentos normativos deste Tribunal, além da legislação vigente.

§5º A tentativa de burlar às diretrizes e controles estabelecidos, quando constatada, deve ser tratada como uma violação.

TÍTULO IV

DA ESTRUTURA NORMATIVA

Art. 33º Além do presente documento, também compõem a Política de Segurança da Informação do TRT da 11ª Região as normas complementares relativas a:

a) Classificação de Informações
b) Controle de Acesso à Rede (Intranet e Internet);
c) Uso do Correio Eletrônico e ferramentas associadas à comunicação
d) Controle de Acesso aos Programas e Diretórios
e) Monitoração e auditoria dos recursos de TI
f) Resposta a incidentes
g) Backup e Recuperação de dados
h) Controle de Terceirizados na SETIC
i) Equipe de tratamento e respostas a incidentes
j) Uso de dispositivos móveis
k) Uso dos Ativos de Tecnologia da Informação e Comunicação
l) Segurança em Desenvolvimento de Sistemas
m) Política de Backup
n) Programa de Capacitação e Conscientização em Segurança da Informação

TÍTULO V

DAS COMPETÊNCIAS E RESPONSABILIDADES

SEÇÃO I

DA PRESIDÊNCIA

Art. 34º Compete à Presidência:

I - Instituir e determinar a composição do Comitê Gestor de Segurança da Informação (CGSI), bem como da Equipe de Tratamento e Resposta de Incidentes de Segurança em Redes Computacionais (ETRISRC);

II - decidir sobre matérias referentes ao descumprimento da Política de Segurança da Informação e/ou normas encaminhadas pelo Comitê Gestor de Segurança da Informação.

SEÇÃO II

DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO

Art. 35º Ao Comitê de Segurança da Informação (ATO N° 27/2018/SGP – Manaus, 10 de abril de 2018) compete:

I - Elaborar propostas de normas e políticas de uso dos recursos de informação;

II - Rever periodicamente a política de segurança e normas a ela relacionadas, sugerindo possíveis alterações;

III - Estabelecer diretrizes e definições estratégicas relativas à Segurança da Informação;

IV – Dirimir dúvidas acerca da aplicação das normas de Segurança da Informação deste Tribunal, submetendo à deliberação da Presidência as situações não contempladas pela política e estrutura normativa vigentes;

V - Propor e acompanhar planos de ação para aplicação desta política, assim como campanhas de conscientização dos usuários;

VI - Receber as comunicações de descumprimento das normas referentes à Política de Segurança da Informação deste Tribunal, instruindo-as com os elementos necessários a sua análise e apresentando parecer à autoridade competente;

VII - Solicitar, sempre que necessário, a realização de auditorias referentes à conformidade com normas complementares, procedimentos e legislação relacionada à Segurança da Informação;

VIII - Avaliar relatórios e resultados de auditorias apresentados relativos à Segurança da Informação;

XI - Apresentar à Administração os resultados da Política de Segurança da Informação;

X - Aprovar as estratégias e os planos de continuidade dos serviços de TI;

XI - Patrocinar ações de comunicação e promoção da cultura de Segurança da Informação no âmbito do Tribunal.

SEÇÃO III

DA ETRISRC – EQUIPE DE TRATAMENTO E RESPOSTA A INCIDENTES DE SEGURANÇA EM REDES COMPUTACIONAIS (PORTARIA N° 189/2018/SGP – Manaus, 10 de abril de 2018)

Art. 36º Compete à ETRISRC:

I - Coordenar a instituição, implementação e manutenção da infraestrutura necessária à ETRISRC;

II - Garantir que os incidentes de segurança na Rede de Computadores do Tribunal Regional do Trabalho da 11a Região sejam monitorados;

III - Adotar procedimentos de feedback para assegurar que os usuários que comuniquem incidentes de segurança da informação e comunicações na rede interna de computadores sejam informados dos procedimentos adotados;

IV - Apoiar os treinamentos relacionados à Segurança da Informação e Comunicações, fornecendo casos práticos de incidentes de segurança na rede interna de computadores, garantindo-se a confidencialidade e devidos níveis de sigilo, sobre o que poderia acontecer como reagir a tais incidentes e como evitá-los no futuro;

V - Recolher provas o quanto antes após a ocorrência de um incidente de Segurança da Informação e Comunicações na rede interna de computadores;

VI - Executar uma análise crítica sobre os registros de falhas para assegurar que elas foram satisfatoriamente resolvidas;

VII - Investigar as causas dos incidentes de Segurança da Informação e Comunicações na rede interna de computadores;

VIII - Implementar mecanismos para permitir a quantificação e monitoração dos tipos, volumes e custos de incidentes e falhas de funcionamento;

IX - Indicar a necessidade de controles aperfeiçoados ou adicionais para limitar a frequência, os danos e o custo de futuras ocorrências de incidentes.

SEÇÃO IV

DA SEÇÃO DE SEGURANÇA DA INFORMAÇÃO

Art. 37º compete à Seção de Segurança da Informação:

I – Definir a estrutura para a Gestão da Segurança da Informação e Comunicações;

II – Promover cultura de segurança da informação e comunicações;

III – Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

IV – Propor recursos necessários às ações de segurança da informação e comunicações;

V – Coordenar o Comitê de Segurança da Informação e Comunicações e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

VI – Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;

VII – Propor Normas e procedimentos relativos à segurança da informação e comunicações no âmbito deste Tribunal;

VIII – Manter a Política de Segurança da Informação revisada e atualizada;

IX - Informar ao COMITÊ DE SEGURANÇA DA INFORMAÇÃO sobre alterações legais ou regulatórias que impliquem responsabilidade ou ação que envolva a gestão de Segurança da Informação;

SEÇÃO V

DO SETOR DE CADASTRO DA SECRETARIA DE GESTÃO DE PESSOAS

Art. 38º Compete ao Setor de Cadastro da Secretaria de Gestão de Pessoas:

I – Estipular controles de segurança especificamente relacionados aos processos de contratação, desligamento (ou encerramento de prestação de serviços), modificação de atividades (incluindo a promoção) e afastamentos (incluindo férias e quaisquer licenças ou suspensões);

II – Comunicar à SETIC o desligamento dos colaboradores e término de contratações, para que os acessos destes sejam desativados e se for o caso, para que sejam recolhidos os Ativos de Tecnologia da Informação e Comunicação de posse do colaborador, especialmente aqueles que detenham características de mobilidade;

III – Entregar a política de segurança da informação na ocasião da admissão do novo colaborador e colher assinatura no documento "Termo de Compromisso para colaborador interno";

IV – Realizar a guarda do documento na pasta funcional do colaborador.

SEÇÃO VI

DO NÚCLEO DE FORMAÇÃO E APERFEIÇOAMENTO DE SERVIDORES

Art. 39º compete ao Núcleo de Formação e Aperfeiçoamento de Servidores, promover ações de capacitação e conscientização em Segurança da Informação aos servidores deste Regional.

SEÇÃO VII

DA ASSESSORIA DE COMUNICAÇÃO

Art. 40º compete à Assessoria de Comunicação:

I – Assessorar a criação do Plano de Comunicação e Conscientização em Segurança da Informação; e

II – Apoiar o COMITÊ DE SEGURANÇA DA INFORMAÇÃO na elaboração de campanhas de conscientização e materiais de divulgação e alerta em segurança da informação e comunicação;

SEÇÃO VIII

DOS USUÁRIOS

Art. 41º compete aos usuários:

I - Atender aos princípios e diretrizes contidos nesta política de segurança da informação, nas normas e procedimentos definidos;

II - Proteger ativos de informação e dados, evitando perda e modificação indevida de forma proposital ou acidental;

III - Relatar incidentes de Segurança da Informação e violação da segurança dos quais tiver conhecimento;

IV - Abster-se de efetuar qualquer tipo de teste de invasão e/ou manuseio da parte interna do hardware sob sua custódia, salvo se formalmente autorizados;

V – Abster-se de oferecer qualquer tipo de resistência às atualizações de software ou hardware a serem implementados pela SETIC.

TÍTULO VI

DAS PENALIDADES

Art. 42º O descumprimento das normas referentes à política de segurança da informação deste Tribunal sujeitará o infrator às sanções administrativas e penais previstas em legislação vigente.

TÍTULO VII

DAS NORMAS COMPLEMENTARES

Art. 43º Visando detalhar as obrigações indicadas nesta PSI, as normas complementares mencionadas no art. 8º, serão discutidas e aprovadas pelo Comitê de Segurança da Informação, e mantidas em documentos a parte, disponível a partir da página principal da intranet institucional ou em site específico mantido por este Tribunal.

TÍTULO VIII

DA REVISÃO PERIÓDICA

Art. 44º Os instrumentos normativos gerados a partir desta PSI devem ser revisados sempre que se fizer necessário, não excedendo o período máximo de 2 (dois) anos.

TÍTULO IX

DA VIGÊNCIA

Art. 45º O presente Ato entra em vigor a partir da data de sua publicação.

Art. 46º Revogam-se as disposições anteriores relativas à Segurança da Informação, inclusive Ato n. º 55/2010 de 25 de outubro de 2010.

Manaus, 25 de julho de 2019.

Assinado Eletronicamente
LAIRTO JOSÉ VELOSO
Desembargador do Trabalho
Presidente do TRT da 11ª Região