1 INTRODUÇÃO

OBJETIVOS

A Política Corporativa de Segurança da Informação (PSI) é a incorporação lógica dos requisitos de negócio da **LICITANET LICITACOES ELETRONICAS LTDA** para segurança e controle das informações, ativos de tecnologia e pessoas. Objetiva estabelecer instruções e diretrizes para assegurar a INTEGRIDADE, CONFIDENCIALIDADE e DISPONIBILIDADE das informações, sistemas e ativos. Também esclarece as responsabilidades dos diretores, colaboradores, terceiros, parceiros e fornecedores; bem como as diretrizes a serem consideradas para preservar e proteger as informações e recursos que processam e/ou transportam estas informações.

ESCOPO

Esta política abrange todas as informações, os sistemas e recursos de Tecnologia da Informação da **LICITANET LICITACOES ELETRONICAS LTDA**, designada neste documento como ***LICITANET***, incluindo também seus diretores, colaboradores, estagiários, terceirizados, temporários e fornecedores em quaisquer das dependências da ***LICITANET*** ou locais onde estes se façam presentes através da utilização, manuseio ou processamento das informações de propriedade ou custodiadas por esta.

RESPONSABILIDADES

Necessidade de saber - Todas as diretrizes estabelecidas neste documento são fundamentadas no princípio da "***necessidade de conhecer***", "Need to Know". Se não estiver claro para o colaborador como as diretrizes estabelecidas nesta Política devem ser aplicadas a uma determinada circunstância, Ele ou Ela deve aplicar de forma conservadora o princípio de necessidade de saber. Isso quer dizer que as informações devem ser tratadas apenas por aquelas pessoas que têm necessidade funcional legítima para o tratamento destas. Em caso de dúvida o gestor imediato deve ser consultado. Esse princípio se aplica a qualquer informação de propriedade ou custodiadas pela ***LICITANET***.

Abordagem Consistente Necessária - Uma única falha na segurança da informação pode gerar consequências adversas para o negócio da ***LICITANET***. O uso consistente desta Política é essencial para a implementação de controles de proteção de dados e, em especial, dados sensíveis de acordo com a definição estabelecida na Lei Geral de Proteção de Dados Pessoais (LGPD) 13.708/2018. Não aderir à Política Corporativa de Segurança da Informação implica em submeter as *Empresas* a incidentes de privacidade e/ou segurança da informação que podem resultar em impactos na reputação, imagem e receita para as organizações. Além disso, multas podem ser aplicadas pela violação de requisitos estabelecidos em leis e normas regulatórias. Esta Política protege consistentemente informações e ativos de propriedade ou sob custódia da ***LICITANET***, quanto aos requisitos INTEGRIDADE, CONFIDENCIALIDADE e DISPONIBILIDADE, independentemente da forma que assumam, das tecnologias utilizadas, quem as manipulam e onde possam estar localizados.

A Tecnologia da Informação (TI), seus recursos e informações são imprescindíveis para o negócio da ***LICITANET***. Portanto, é premente assegurar a proteção destes ativos através da gestão contínua de Segurança da Informação (SI).

Assim, a área de Planejamento é responsável pela Gestão de Segurança da Informação (SGSI – Sistema de Gestão de Segurança da Informação) bem como por estabelecer, manter, publicar e divulgar as políticas de segurança, padrões e procedimentos. Além disso, é de sua responsabilidade a operação, manutenção dos serviços de segurança, a investigação de intrusão em sistemas e outros incidentes de segurança da informação, auxiliando as demais áreas da ***LICITANET*** no suporte e nas soluções de segurança de forma corporativa, cabendo ao gestor de cada área de negócios identificar as irregularidades em seus processos, reportando-as ao Gestor da área de Infraestrutura.

É responsabilidade da área de Planejamento garantir o bom andamento do processo de gestão de SI, bem como a aderência de todas as áreas da ***LICITANET*** a esta Política, por meio da publicação mensal de indicadores, realização de auditorias internas e/ou externas em intervalos regulares e assegurando que riscos sejam mitigados em conjunto com a Alta Direção da ***LICITANET***. Qualquer anomalia ou incidente ocorrido deve ser reportado ao Gestor da área

de Tecnologia da Informação (TI) para identificar e classificar o risco a fim de direcionar os procedimentos de comunicação e tratativa do incidente.

A área Jurídica deve garantir que contratos com clientes, fornecedores, prestadores de serviços e parceiros de negócio possuam cláusulas de Segurança da Informação, que assegurem a proteção das informações e recursos de TI. Sempre que existir a necessidade, o Termo de Confidencialidade deve ser assinado entre as partes antes do início da prestação de serviços e/ou projetos que envolvam informações sensíveis, seja em instrumento apartado ou através de cláusula específica contida no próprio contrato de prestação de serviços, sendo responsabilidade da área contratante a garantia de que as cláusulas e termo de confidencialidade estejam presentes durante e após a negociação.

Colaboradores da ***LICITANET*** devem familiarizar-se, aderir e praticar as políticas e/ou diretrizes contidas na PSI, bem como observar os processos, procedimentos e padrões relacionados à Segurança da Informação. As informações resultantes das atividades comerciais da ***LICITANET***, principalmente aquelas que envolvam o tratamento de dados pessoais devem garantir adequação a Lei Geral de Proteção de Dados Pessoais (**LGPD**) 13.709/2018. Portanto, todos os colaboradores têm a obrigação de tratar dados pessoais com rigor e observando a classificação da informação estabelecida conforme **Política Corporativa para Classificação da Informação** (PCCI), referência **POL-002**, sob pena de serem submetidos a aplicação de sansões, punições, processos cíveis e criminais no rigor da Lei.

A área de Recursos Humanos é responsável por informar sobre os requisitos de Segurança da Informação aos possíveis candidatos a vagas de emprego da ***LICITANET*** mesmo antes de se concretizar a contratação, bem como apoiar e garantir os processos de educação e conscientização em Segurança da Informação durante o ciclo de vida do colaborador nA ***LICITANET***, sem prejuízo de que sejam informados regularmente, ou sempre que necessário, quando houver qualquer alteração nesta Política ou nos procedimentos e processos que a suportam.

Ações disciplinares resultantes da violação dos requisitos e diretrizes de Segurança da Informação serão tratadas pelo gestor do colaborador em conjunto com a área de Recursos Humanos.

Visando a evolução do processo de gestão de Segurança da Informação e Privacidade de Dados Pessoais, a ***LICITANET*** estabelece o Comitê para Governança de Privacidade e Segurança da Informação (CGPSI) por meio de estatuto designado e aprovado pela empresa. O Comitê deve avaliar e revisar o estado corrente da Gestão de Privacidade e Segurança da Informação da ***LICITANET***, aprovar novas ou modificar políticas de segurança, privacidade e deliberar sobre outras questões de alto-nível relacionadas aos processos, procedimentos e atividades associados ao **Sistema de Gestão de Segurança da Informação** (SGSI).

A Alta Direção da ***LICITANET*** deve supervisionar e garantir recursos para a atuação eficaz do **Comitê de Gestão de Privacidade e Segurança da Informação** (CGPSI).

COMUNICADO DA PRESIDÊNCIA

São deveres de todos os colaboradores da ***LICITANET*** aderir e cumprir as diretrizes da Política Corporativa de Segurança da Informação. Pois, a integridade, confidencialidade e disponibilidade são fatores primordiais a manutenção dos negócios, satisfação dos clientes e garantia da competitividade da ***LICITANET***.

Portanto, a alta direção e presidência da ***LICITANET*** endossam e apoiam esta Política na sua integralidade e estarão atentas a sua manutenção, evolução e adesão.

2 RECURSOS HUMANOS

Assim que realizada a contratação, novos colaboradores da ***LICITANET*** devem ser engajados em treinamento introdutório sobre segurança da informação, receber cópia da PSI, ler e assinar o Termo de Responsabilidade e Confidencialidade, caracterizando a concordância com as diretrizes definidas nesta Política.

É responsabilidade da área de Recursos Humanos garantir este processo, bem como o arquivamento da cópia do Termo de Responsabilidade e Confidencialidade assinado na pasta do colaborador.

Todos os colaboradores em processo de término do contrato de trabalho devem ter os acessos revogados o mais rápido possível. É responsabilidade da área de Recursos Humanos garantir a execução fim-a-fim deste processo. É responsabilidade do gestor do colaborador iniciar a exclusão através dos trâmites de acionamento e comunicação do desligamento à área de Recursos Humanos, esta por sua vez, deve iniciar e garantir a exclusão dos acessos sistêmicos. A área de Tecnologia da Informação (TI) deve garantir a remoção e/ou bloqueio dos acessos.

É responsabilidade da área de Recursos Humanos prover meios de divulgação desta Política e de aculturação relacionada à Segurança da Informação para colaboradores já contratados e/ou em fase de contratação.

3 AUDITORIA, SANÇÕES E PUNIÇÕES

A ***LICITANET*** reserva para si o direito de monitorar e manter registros de todos os tipos de acesso aos seus sistemas, redes e informações. Incluindo-se o uso particular (pessoal) por meio destes recursos, quando da existência ou suspeita de informações e/ou evidências de atos ilícitos ou conduta inadequada. Estes registros também podem ser utilizados para análises estatísticas visando a boa prestação de serviços e para verificação em casos relacionados a incidentes de segurança.

Auditorias internas podem ser executadas sem aviso prévio pela área de TI ou empresa especializada para a verificação do atendimento das considerações que compõem e suportam esta Política.

Como medidas disciplinares poderão ser consideradas desde simples advertência verbal, advertência escrita, suspensão, e, quando for o caso, o término do contrato por justa causa, quando incorrer em qualquer das hipóteses contidas no art. 482 da CLT.

4 DÚVIDAS, SUGESTÕES E EXCEÇÕES

A área de TI é responsável pelo esclarecimento de dúvidas, recepção e tratativa de sugestões relativas a esta Política. Dúvidas, sugestões e relatos de incidentes devem ser enviados para o endereço seguranca@licitanet.com.br.

Exceções a esta Política devem ser apresentadas a gerência imediata do colaborador, a qual deverá submetê-las à Alta Direção, onde serão discutidas e avaliadas. Caso necessário, a exceção será submetida para apreciação do Comitê de Gestão de Privacidade e Segurança da Informação e/ou a alta direção da ***LICITANET***.

Todas as exceções devem ser devidamente registradas e documentadas de forma a propiciar a evolução futura desta política.

5 CLASSIFICAÇÃO DA INFORMAÇÃO

Para assegurar que a informação receba um nível adequado de proteção de acordo com sua importância, tratamento, sensibilidade e requisitos legais, a ***LICITANET*** estabelece responsabilidades e diretrizes específicas na **Política Corporativa para Classificação da Informação** (PCCI), referência **POL-002,** que é parte integrante do Sistema de Gestão de Segurança da Informação (SGSI). Portanto, a observância e aderência a esta política é responsabilidade de todos na ***LICITANET***.

6 GOVERNANÇA E TECNOLOGIA

Todas as áreas da ***LICITANET*** devem inteirar-se sobre melhores práticas para governança corporativa e suportar a área de Tecnologia da Informação (TI) com recursos e informações necessários ao bom desempenho da TI.

É responsabilidade da área de Infraestrutura, em conjunto com a área de TI, estruturar, manter e divulgar processos e procedimentos para gestão de desempenho, segurança da informação, requisição de serviços, operação de TI, gestão

de mudanças, incidentes e problemas. Devendo apresentar indicadores de acompanhamento mensalmente e planos de correção de rumo no caso de desvios.

É responsabilidade da área de Infraestrutura realizar a gestão de riscos de ambiente e de processos relacionados à Segurança da Informação, visando mitigar a ocorrência de incidentes de disponibilidade.

A área de Infraestrutura deve garantir que recursos de hardware e software para suportar serviços críticos, em especial aqueles direcionados a clientes externos, tenham características básicas de contingência e redundância. Bem como garantir a existência de documentação estruturada da topologia e inventário de serviços críticos, implantada, monitorada e atualizada.

Equipamentos que armazenam e processam informações da ***LICITANET***, devem estar acondicionados em ambiente com controle de acesso físico, energia estabilizada e condições de climatização adequadas aos requisitos técnicos de cada equipamento. Estes ambientes devem ser devidamente gerenciados e eventos que extrapolem condições mínimas ou requisitos de operação devem ser tratados como incidentes de (in)disponibilidade, registrados e acompanhados.

Todas as alterações de configuração na infraestrutura de TI, segurança da informação e sistemas críticos da ***LICITANET*** devem ser registradas e aprovadas através de processo específico para Gestão de Mudanças.

O processo de gestão de mudanças deve assegurar no mínimo que os riscos operacionais foram identificados, que o processo de retomada/recuperação em caso de problemas existe e está validado pelos responsáveis pela gestão de mudança.

Todas as alterações de configuração na rede e sistemas críticos da ***LICITANET*** requerem obrigatoriamente a realização de cópia de segurança das configurações antes e após a realização das mudanças. A equipe responsável pelas alterações também é responsável pela realização, classificação e armazenamento das cópias de segurança.

Mudanças emergenciais devem ser registradas, aprovadas e validadas em prazo mínimo possível após a sua execução.

É responsabilidade da área de Infraestrutura definir e monitorar níveis de serviço para segurança da informação providos (contratados de) por fornecedores de mercado, bem como monitorar mudanças nas práticas de SI destes fornecedores e na prestação de serviços. Os riscos devem ser avaliados e tratados por meio do registro de mudanças para serviços de terceiros.

É responsabilidade da área de Infraestrutura que a implantação e manutenção de serviços de TI, rede e segurança da informação sejam implantados e configurados seguindo boas práticas de *hardening* para redução da superfície de ataques e consequente mitigação de riscos de SI.

7 RECURSOS DE TECNOLOGIA

7.1. DIRETRIZES GERAIS

Os ativos de tecnologia da ***LICITANET***, incluindo software, hardware e informações, devem ser utilizados pelos colaboradores somente para as atividades laborais associadas as suas funções previstas em contrato de trabalho. Estes devem garantir a aplicação dos princípios “necessidade de saber” e “abordagem consistente necessária”.

Os colaboradores da ***LICITANET*** devem praticar a política de mesa e tela limpa sempre que se ausentarem de suas dependências de trabalho, durante ou fora do expediente. Proteções de tela devem ser ativadas, documentos, anotações e informações impressas devem ser armazenados em locais seguros como gavetas com trancas.

7.2. USO DE SOFTWARE

O uso de software é regulamentado por legislação específica e qualquer ato que a viole pode ser punido com os rigores da lei. É PROIBIDA a instalação de software não licenciado.

Existe software de livre distribuição (*freeware*, *open source*) e outros cuja aquisição e registro de licença são obrigatórios. Para os que requerem licença é necessário que a ***LICITANET*** mantenha as devidas autorizações, contratações de uso para que estes possam ser instalados e utilizados nos ativos de TI. É responsabilidade da área de TI manter inventário de hardware, software e controle de licenças atualizados.

Cuidado adicional deve ser prestado quanto ao software de livre distribuição (*freeware*, *open source*), pois há grande probabilidade deste carregar e inserir ameaças no ambiente de tecnologia da ***LICITANET***. Assim, estes não podem ser utilizados sem a devida homologação e aprovação pela área de TI. Um processo de aprovação formal deve ser gerenciado por esta área com os devidos registros de liberação e restrição.

É responsabilidade da área de TI manter registro e licença de software necessário ao desempenho das funções dos usuários. Sempre que houver dúvida sobre a legalidade de uso de algum software, a equipe de TI, responsável pelo inventário e administração de software, deve ser consultada a fim de fornecer os esclarecimentos pertinentes.

A ***LICITANET*** é proprietária de todos os direitos sobre patentes, direitos autorais, invenções ou outras propriedades intelectuais originadas e desenvolvidas por seus colaboradores individualmente ou em grupo constituído por outros fornecedores de serviço, durante a vigência dos respectivos contratos de trabalho e prestação de serviço. Todos os programas e documentos criados ou providos pelos colaboradores em benefício da ***LICITANET*** são considerados propriedades destas.

A ***LICITANET*** é as custodiante legal das informações contidas em sistemas de informação sobre seu controle e/ou administração. A ***LICITANET*** reserva-se o direito de acesso, uso e poder de decisão sobre estas informações respeitando-se os requisitos vigentes nas leis federais, estaduais e municipais.

Sistemas que tratam informações sensíveis ao negócio e ou aqueles utilizados para prover acesso remoto ao ambiente de TI devem prover mecanismos de geração de *logs* de acesso e trilha de auditoria visando a rastreabilidade de eventos. A área de TI é responsável por assegurar estes recursos na implantação e configuração de serviços e ativos de tecnologia.

O uso de serviços de TI e SI providos por terceiros deve ser avaliado previamente a contratação quanto a requisitos e melhores práticas de segurança. A área de TI é responsável pela avaliação formal das práticas de segurança adotadas por estes utilizando-se minimamente da aplicação de questionário padronizado de acordo com os requisitos de integridade, confidencialidade e disponibilidade inerentes aos serviços a serem contratados. Em casos mais criteriosos *due diligence* deve ser realizada para confirmação de evidências. Após a contratação as mudanças nestes serviços devem ser acompanhadas e o fornecedor deve ser reavaliado pelo menos 01 (uma) vez por ano.

É responsabilidade da área de TI desenvolver e manter processo e procedimento para a aplicação de patches (correções) de segurança no software utilizado pela ***LICITANET*** de forma a mitigar riscos de segurança.

7.3. USO DE HARDWARE

A ***LICITANET*** considera como estações de trabalho quaisquer equipamentos de sua propriedade associados aos domínios e grupos de trabalho disponibilizados pela área de TI. Assim, desktops, laptops, notebooks, tablets e smartphones corporativos são considerados estações de trabalho

Como equipamentos de rede, a ***LICITANET*** considera quaisquer equipamentos de sua propriedade associados ao transporte e armazenamento das informações entre as redes desta, Internet, clientes, parceiros e fornecedores. Como exemplo de equipamentos de rede destacam-se: switches, roteadores, firewall e equipamentos detectores de intrusos (IPS).
Os colaboradores/terceiros não devem utilizar computadores e periféricos pessoais, tais como discos externos, roteadores *wireless*, *pendrive* e impressoras, bem como software pessoal nas redes da ***LICITANET***, salvo com autorização formal e prévia da Alta Direção.

Todos os servidores, estações de trabalho e equipamentos de rede da ***LICITANET*** devem obrigatoriamente apresentar aviso de advertência (banner) no processo de *logon/login* para reiterar a propriedade das *Empresas* e uso somente por pessoas autorizadas.

Os servidores e equipamentos de rede críticos têm que estar em local fisicamente protegido contra ameaças naturais, variações ou interrupção no fornecimento de energia, ambiente provido de acesso físico controlado, que possua condições de temperatura e umidade adequadas ao bom funcionamento destes. É responsabilidade da Infraestrutura garantir estas condições previamente a instalação destes ativos.

Manutenções e intervenções realizadas por terceiros nos equipamentos de rede, segurança e servidores requerem acompanhamento obrigatório por pessoal especializado da ***LICITANET*** e processo registrado (formalizado) por meio de Gestão de Mudança.

O transporte de equipamentos, incluindo servidores, desktops, switches, roteadores, *storage* (armazenamento), firewall e outros; só poderá ser realizado através de liberação formal da área de Infraestrutura, e ocorrer por meio de acondicionamento adequado, possuindo devido registro da autorização e do transporte.

É vedada a instalação de hardware sem prévia aprovação da área de Infraestrutura e /ou projeto previamente aprovado. A utilização de hardware por clientes, fornecedores e terceiros nas redes de propriedade da ***LICITANET*** deverá ser habilitada somente após inspeção e verificação das condições de segurança do hardware pela área de TI.

O descarte de hardware que não será reutilizado, dever ser supervisionado pela área de Infraestrutura e o processo deve garantir que informações não possam ser recuperadas utilizando técnicas conhecidas. O processo de descarte, sempre que possível, deve garantir a destruição física por meio de trituração. Discos físicos, quando descartados e não haver opção de trituração, devem ser formatados considerando o uso de técnicas de sobrescrita.

7.4. ACESSO REMOTO

O acesso remoto às redes da ***LICITANET***, ou seja, o acesso a partir de outra empresa deve ser realizado somente por meio de projeto elaborado e implementado pela área de Infraestrutura aplicando controles de acesso e comunicação criptografada como VPN (Rede Privativa Virtual) ou repositórios seguros.

Os equipamentos conectados à rede corporativa da ***LICITANET*** não podem ser diretamente conectados a outras redes ou diretamente à Internet. Estas conexões devem ser feitas através de serviços seguros sustentados por segurança de perímetro, redes privadas virtuais (VPN), proteção contra malware e outros; validados e homologados pela área de Infraestrutura. Conexões de exceção devem ser aprovadas, configuradas e monitoradas pela área de TI.

Todos os computadores conectados às redes internas da ***LICITANET*** por meio de VPN devem estar com as versões mais atualizadas de software de proteção antivírus, e com os patches de segurança mais recentes aplicados.

O acesso remoto para terceiros só pode ser feito por intermédio de projeto específico da área de Infraestrutura, considerando que terão acesso controlado e apenas aos recursos e serviços de infraestrutura necessários para o exercício da atividade contratada. Além disso, os equipamentos de terceiros e clientes devem atender aos requisitos de segurança e utilizar os sistemas operacionais suportados e informados pela ***LICITANET***.

O acesso remoto para colaboradores só pode ser realizado através de protocolos seguros, por meio de plataformas homologadas e validadas pela área de Infraestrutura. É responsabilidade da área de Infraestrutura disponibilizar, gerenciar e monitorar os acessos remotos, além disso prover a instalação de software necessário para o uso da VPN. Sempre que possível a área de Infraestrutura deverá implementar controle de acesso que utiliza VPN com autenticação segura, robusta e uso de autenticação com duplo fator.

7.5. INTERNET, E-MAIL E REDES SOCIAIS

7.5.1. INTERNET

A Internet é estrutura fundamental ao desempenho das atividades de negócio da ***LICITANET*** e por ser uma rede com abrangência mundial, permite a conexão de entidades com todos os tipos de propósito. Em virtude disso, cuidados devem ser considerados ao utilizá-la.

A ***LICITANET*** reserva-se no direito de monitorar e/ou bloquear acesso a sites de conteúdo ilícito, pornografia, atividades hacker e outros, sem aviso prévio e de forma automática.

A navegação na Internet propicia o acesso a qualquer tipo de conteúdo. Desde páginas idôneas, úteis e produtivas até as páginas de conteúdo impróprio. Desta forma, é proibido o acesso, cópia ou armazenamento de páginas, programas ou qualquer outro material (músicas, fotos e vídeos) que violem a lei de direitos autorais (*copyright*), bem como aqueles de conteúdo adulto ou ilícito, pois estes podem promover as atividades de hackers e improdutividade funcional.

É proibido também acesso e divulgação de qualquer conteúdo discriminatório, político, homofóbico, racista, misógino ou que faça apologia ao crime. A ***LICITANET*** promove o controle automático de navegação a sites não considerados apropriados ao desempenho das funções do colaborador.

A ***LICITANET*** armazena os registros de navegação na Internet e poderão monitorá-los para avaliar atividades ilícitas, possíveis fraudes, comportamentos impróprios e que destoam do exercício da função definida em contrato de trabalho bem como gerar estatísticas de uso e desempenho visando aprimorar seus serviços internos e externos.

Toda informação recebida a partir da Internet deve ser trabalhada com cautela. Colaboradores não estão autorizados a compartilhar e/ou salvar informações da ***LICITANET*** ou sob custódia desta em sites que provêm serviço de guarda e compartilhamento de arquivos (*file sharing*), salvo se autorizado formalmente pela área de Infraestrutura. Somente devem ser utilizados os repositórios de arquivos disponibilizados pela ***LICITANET***.

Sempre que possível a ***LICITANET*** deverá utilizar-se de protocolos seguros criptográficos (HTTPS, IPSec, SFTP) para transmissão de informações críticas e sensíveis via Internet. Cabe aos gestores avaliar a criticidade das informações e solicitar os recursos necessários para a área de Infraestrutura. A área de Infraestrutura é responsável por garantir a utilização de versões não vulneráveis destes protocolos.

7.5.2. E-MAIL

Colaboradores da ***LICITANET*** que possuem contas de e-mail associadas ao desempenho de suas funções, devem utilizá-la somente para fins específicos desta função.

Contas de e-mail de uso pessoal não podem ser utilizadas para envio e recebimento de informações de propriedade da ***LICITANET***.

A ***LICITANET*** armazena os registros de uso de e-mail corporativo e poderá monitorá-los para avaliar atividades ilícitas, possíveis fraudes, comportamentos impróprios ao exercício da função definida em contrato de trabalho; bem como gerar estatísticas de uso e desempenho visando aprimorar seus serviços internos e externos. Cuidados especiais devem ser prestados aos e-mails recebidos de origem desconhecida. A grande maioria são vetores que carregam vírus, armadilhas e outros códigos maliciosos. Nenhum anexo destes e-mails deve ser visualizado, baixado ou executado.

Ao redigir e-mails, os colaboradores devem anexar somente os arquivos necessários. Tendo ciência que cada mensagem enviada, principalmente com anexos, consome consideráveis recursos da rede e de servidores.

A comunicação via e-mail pode ser monitorada em casos de investigação relacionada a incidentes de segurança e fraudes, incluindo-se os e-mails pessoais acessados no e através do ambiente corporativo da ***LICITANET***.

E-mails não solicitados não devem ser respondidos, pois na maioria das vezes e-mails são enviados a uma infinidade de destinatários válidos ou não. O ato de responder o e-mail confirma ao agressor a validade do endereço de e-mail de destino, logo este e-mail poderá ser inserido em um cadastro que poderá ser disponibilizado para a prática do SPAM.

Não é permitido o uso do sistema de e-mail, cujos domínios pertencem à ***LICITANET***, ou aqueles administrados por esta, para o repasse de correntes, mensagens com conteúdo ilegal, racista, pornografia, religioso, preconceituoso, pejorativo ou ameaçador; bem como qualquer outro conteúdo inadequado ao ambiente corporativo e ou que possa trazer instabilidade de relacionamento pessoal e queda desempenho nos recursos de TI.

Os colaboradores devem estar atentos a e-mails que possam conter vetores de ataque associados a *Phishing*. Não clicar em links que apresentam promoções extremamente atrativas, links que solicitem usuário e senhas corporativas. Os sinais de alerta incluem endereços de e-mail ou nomes de domínio estranhos, e-mails estranhos, incomuns ou inesperados, anexos com tipos de arquivo estranhos e hiperlinks de aparência suspeita. Mesmo com as proteções automáticas, providas pela ***LICITANET*** contra este tipo de ataque, podem ocorrer situações em que o colaborador receberá mensagem suspeita e, nestes casos, deverá registrar um chamado no Service Desk, não abrir o e-mail, nem clicar em hiperlinks, nem baixar arquivos anexados.

A área de TI é responsável por prover serviços de mensageria considerando padrões e protocolos seguros. Os serviços de e-mail providos pela ***LICITANET*** devem suportar os padrões: *DomainKeys Identified Mail* (DKIM), *Domain-based Message Authentication Reporting and Conformance* (DMARC) e *Sender Policy Framework* (SPF).

A área de TI é responsável por prover mecanismos para que o remetente possa classificar e-mails de forma automatizada e corriqueira de acordo com a Política Corporativa para Classificação da Informação.

7.5.3.REDES SOCIAIS

Colaboradores devem ter especial atenção e assegurar que NÃO representam a ***LICITANET*** em grupos de discussão na Internet, fóruns públicos e redes sociais; salvo com autorização expressa da área de Marketing ou função expressamente atribuída através do cargo em vigência.

É vedada aos colaboradores a publicação de informações em qualquer rede social, salvo por área devidamente autorizada pela ***LICITANET***. Mesmo as áreas autorizadas devem ter especial atenção ao conteúdo, bem como a classificação da informação a qual, para ser divulgada, deverá previamente ser classificada como #PÚBLICO (rótulo). Um processo de revisão e aprovação da comunicação deve ser devidamente registrado pelas áreas autorizadas.

A ***LICITANET*** coíbe automaticamente o acesso a redes sociais, através de sua infraestrutura de TI, para colaboradores que NÃO tenham em sua função de trabalho as necessidades de acesso a redes sociais.

7.6. INTELIGÊNCIA ARTIFICIAL (IA) GENERATIVA

Os colaboradores devem usar sistemas de IA, estritamente autorizados pela ***LICITANET***, de forma responsável e ética, evitando quaisquer ações que possam prejudicar outros indivíduos, violar a privacidade ou facilitar atividades maliciosas.

É proibido o uso de sistemas (plataformas) de IA não autorizados pela ***LICITANET***. É responsabilidade da área de TI validar e informar plataformas de IA que poderão ser utilizadas pelos colaboradores.

Os sistemas de IA devem ser usados em conformidade com todas as leis e regulamentos aplicáveis, incluindo leis de proteção de dados pessoais, privacidade e propriedade intelectual.

Os colaboradores devem ser transparentes sobre o uso de IA em seu trabalho, garantindo que as partes interessadas estejam cientes do uso da tecnologia nos processos de negócio. Os colaboradores devem utilizar o sistema centralizado da ***LICITANET*** para governança de IA e esforços de conformidade para garantir a transparência das atividades de IA propostas e ativas. Os colaboradores são responsáveis pelos resultados gerados pelos sistemas de IA e devem estar preparados para explicar e justificá-los.

Os colaboradores devem aderir às políticas de privacidade e segurança de dados da ***LICITANET*** ao usar sistemas de IA. Eles devem garantir que quaisquer dados pessoais e/ou sensíveis usados pelos sistemas de IA sejam anonimizados e armazenados com segurança.

8 CONTROLE DE ACESSO LÓGICO E FÍSICO

8.1. LOGIN ÚNICO E IDENTIFICÁVEL E PERMISSIONAMENTO DE ACESSO

Acesso às informações e sistemas da ***LICITANET*** deve ser autorizado de acordo com as atividades atribuídas ao cargo ou função exercida pelo colaborador, cliente, fornecedor e terceiros. Os privilégios de acesso atribuídos para eles devem ser revistos periodicamente pelos gestores responsáveis.

Todo colaborador, cliente, fornecedor e terceiros deve possuir uma única identificação de usuário (*User IDs*, ou *logon*) e senha(s) (*password*) relacionados às suas atribuições ou funções em exercício no contrato de trabalho ou de prestação de serviço, sempre que tecnologia dispor/suportar recurso para tal. Os privilégios e direitos de acesso devem ser atribuídos de acordo com as atribuições ou funções em exercício no contrato de trabalho ou de prestação de serviço. Colaborador, cliente, fornecedor e terceiros são responsáveis pelo uso e segurança de suas credenciais de acesso e senhas.

É proibido o empréstimo e compartilhamento de credenciais de usuários e senhas associadas a qualquer tipo de acesso às informações, sistemas e equipamentos da ***LICITANET***.

8.2. SENHA FORTE

É responsabilidade da área de TI garantir configurações no(s) domínio(s) de controle para assegurar a construção de senhas fortes, aplicação de histórico e expiração automática das senhas.

A construção de qualquer senha deve considerar o uso e composição entre caracteres alfabéticos, maiúsculos, minúsculos e números. Toda senha deve ter no **mínimo** 08 (oito) caracteres.

Os colaboradores, clientes, fornecedores e terceiros devem escolher senhas fáceis de serem memorizadas, porém ao mesmo tempo difíceis de serem descobertas ou quebradas. Técnicas para esta escolha incluem:

- Combinar palavras de fácil memorização através de caracteres alfanuméricos, por exemplo: Barco01&amarelo, Tempo02+Nublado;
- Combinar as primeiras letras das palavras que compõe o trecho de uma música ou frase;
- Combinar sinais de pontuação e números com uma palavra conhecida, por exemplo: Deserto1023w.

As senhas devem ser alteradas obrigatoriamente a cada 60 (sessenta) dias. É responsabilidade da área de T.I garantir as configurações necessárias nos sistemas para que as senhas expirem automaticamente. Informações de expiração da senha devem ser apresentadas no processo de identificação (logon) do usuário, no mínimo 5 (cinco) dias antes da expiração. Após 5 (cinco) tentativas incorretas na obtenção de login no sistema, este bloqueará automaticamente as tentativas de login por 30 (trinta) minutos.

O colaborador não poderá repetir nenhuma das últimas 13 (treze) senhas já previamente utilizadas.

Quando o colaborador suspeitar de utilização indevida de sua(s) senha(s) deverá alterá-la(s) imediatamente e tratar a situação como um incidente de segurança reportando ao seu superior imediato o qual deverá comunicar a área de TI.

Para evitar a divulgação inadvertida e uso indevido destas, as senhas não devem ser armazenadas em forma compreensível (leitura) em código fonte, scripts, macros e papel.

Todas as estações de trabalho da ***LICITANET*** devem utilizar proteção de tela (*screensaver*) previamente homologada pela área de TI e com ação automática de execução da proteção a partir de 10 (dez) minutos de inatividade destas. É

responsabilidade da área de TI configurar políticas nos diversos domínios de acesso para assegurar a utilização de proteção de tela. É vedada a qualquer usuário a remoção das configurações de proteção de tela da estação de trabalho.

8.3. ACESSO FÍSICO

O acesso às dependências físicas da ***LICITANET*** deve ser controlado e gerenciado através de procedimento construído e mantido de acordo com a criticidade do ambiente. Mecanismos de dissuasão, controle, monitoramento de ambiente tais como vídeo vigilância, porta com acesso biométrico e/ou guardas devem ser implementados e monitorados.

9 MALWARE

Malware (código maléfico), junção das palavras "***mal****icious*" e "*soft****ware***" é um software projetado para infiltrar e danificar um sistema de computador sem o consentimento do proprietário do sistema. A expressão constitui um termo geral utilizado pelos profissionais da área de Tecnologia da Informação para designar uma série de ameaças hostis, intrusivas e perigosas inseridas em algum código de computador.

O termo "vírus de computador" é o mais abrangente e utilizado para incluir todos os tipos de malware. Porém, existem também os chamados vermes, cavalos de Tróia, *spyware*, *keystroke loggers*, *ransomware* etc.

Toda estação de trabalho e servidor deve possuir software antivírus instalado e atualizado automaticamente. É responsabilidade da área de T.I. assegurar o processo de controle de *malware* na ***LICITANET***.

Ransomware é um tipo de malware que é usado para infectar computadores e criptografar arquivos de computador até que um resgate seja pago. Após a infecção inicial, o *ransomware* tentará se espalhar para sistemas conectados, incluindo unidades de armazenamento compartilhadas e outros computadores acessíveis. O *ransomware* é comumente entregue por meio de e-mails de *phishing* ou por meio de "*drive-by downloads*". Os e-mails de *phishing* geralmente parecem ter sido enviados por uma organização legítima ou alguém conhecido da vítima e induzem o usuário a clicar em um link malicioso ou abrir um anexo malicioso. Um "*drive-by download*" é um programa que é baixado automaticamente da Internet sem o consentimento do usuário ou, muitas vezes, sem seu conhecimento. É possível que o código malicioso seja executado após o *download*, sem interação do usuário. Após a execução do código malicioso, o computador é infectado com *ransomware*.

Um incidente causado por *ransomware* pode representar impacto irreversível para uma organização. Assim, a ***LICITANET*** deve utilizar proteção do tipo XDR (*Extended Detection and Response*) - detecção e resposta estendidas - que coleta e correlaciona automaticamente os dados em várias camadas de segurança – e-mail, *endpoint*, servidor, *workload* em nuvem e rede. Isso permite uma detecção mais rápida de ameaças e melhor investigação e tempos de resposta por meio de análises de segurança. É responsabilidade a área de TI a escolha, instalação e configuração deste tipo de proteção nos ativos de TI.

É responsabilidade do colaborador comunicar a área de TI comportamentos anômalos associados a *malware* identificados em suas estações de trabalho.

O uso de dispositivos do tipo "mídia removível" (*pendrives*) deve ser previamente autorizado formalmente e controles de segurança da informação devem ser empregados pela área de TI coibindo o uso não autorizado.

10 CRIPTOGRAFIA

Criptografia é a ciência ou arte de escrever mensagens em forma cifrada (codificada). É usada, dentre outras finalidades para: autenticar a identidade de usuários; autenticar transações bancárias; proteger a integridade de transferências eletrônicas de fundos; proteger o sigilo de comunicações pessoais e comerciais.

As comunicações e transferências de informações entre a ***LICITANET***, clientes, instituições financeiras, parceiros e fornecedores estratégicos devem ser realizadas através de redes privadas (VPN) ou utilizando-se de protocolos de transporte calcados em esquemas criptográficos previamente avaliados e aprovados pela área de Infraestrutura.

As bases de dados contendo senhas devem estar criptografadas e o com respectivo controle adequado das chaves de criptografia. A responsabilidade pela gestão das ferramentas de criptografia, chaves e códigos fonte é da área de Infraestrutura.

Notebooks devem possuir criptografia em disco nativa e, portanto, devem ser adquiridos com o recurso TPM (*Trusted Platform Module*) ou Módulo de Plataforma Confiável, para suportar a criptografia. É responsabilidade da TI a substituição gradual do parque de equipamentos para atingir o objetivo de proteção.

É responsabilidade da área de Infraestrutura avaliar e implementar mecanismos de criptografia para codificar dados pessoais sensíveis de clientes e da própria organização, em repouso ou trânsito. É recomendável que estes mecanismos sejam nativos, sempre que possível, das plataformas de mercado incluindo, mas não se limitando a *storage*, Sistemas Gerenciadores de Bancos de Dados (SGBD) e redes com capacidade de criptografia.

11 CÓPIAS DE SEGURANÇA E CONTINGÊNCIA

Todas as informações críticas de negócio da ***LICITANET*** têm que possuir cópia de segurança (*backup*) realizada de acordo com planejamento associado a criticidade da informação para o negócio, atendendo aos requisitos operacionais, legais e históricos.

É responsabilidade da área de TI providenciar os recursos físicos e lógicos para armazenamento e restauração das cópias de segurança das informações associadas aos colaboradores e departamentos da ***LICITANET***. Também deve assegurar que cópias estejam presentes em locais físicos diferentes do local de origem da informação e devidamente acondicionadas.

É responsabilidade da área de Infraestrutura providenciar os recursos físicos e lógicos para armazenamento e restauração das cópias de segurança das informações associadas aos clientes da ***LICITANET***. Também deve assegurar que cópias estejam presentes em locais físicos diferentes do local de origem da informação e devidamente acondicionadas.

É responsabilidade do Proprietário da informação definir os requisitos mínimos de salvaguarda da informação, tais como tempo de retenção e periodicidade da cópia para as informações associadas aos departamentos da ***LICITANET***. Para os clientes da ***LICITANET***, os requisitos mínimos de salvaguarda da informação devem estar contratualmente definidos. A área de Infraestrutura deverá observar e garantir estes requisitos.

As cópias de segurança devem ser verificadas sistemicamente pelas áreas responsáveis para assegurar o processo de restauração. É responsabilidade da área de TI prover os recursos necessários e realizar a restauração das cópias de segurança regularmente para informações associadas aos departamentos da ***LICITANET***. É responsabilidade da área de Infraestrutura prover os recursos necessários e realizar a restauração das cópias de segurança regularmente para associadas aos departamentos da ***LICITANET***.

O processo de restauração das informações críticas armazenadas em cópias de segurança é responsabilidade exclusiva da área de TI e deve estar formalmente documentada. A restauração da informação deverá ser solicitada formalmente a esta área pelo Proprietário da informação.

Informações críticas ao negócio da ***LICITANET*** presentes em estações de trabalho e equipamentos móveis, tais como *notebooks*, celulares e *tablets* também devem estar presentes em diretórios de rede para que o processo de cópia de segurança seja assegurado. É responsabilidade dos colaboradores garantir que estas informações estejam em diretórios de rede.

Informações de clientes cujos serviços são contratados da ***LICITANET*** e operam em ambiente SaaS ou PaaS devem possuir cópia de segurança localizada em ambiente operacional físico e logicamente distinto do ambiente de produção. As cópias (backup) devem ser protegidas contra escrita acidental ou maliciosa por software ou hardware especificado para tal proteção.

12 DESENVOLVIMENTO E AQUISIÇÃO DE SOFTWARE

O processo de desenvolvimento e aquisição de novos sistemas deve considerar as melhores práticas de segurança da informação. Estas práticas devem ser atualizadas, discutidas e disseminadas na ***LICITANET***. É responsabilidade da área de Desenvolvimento garantir a disseminação e aplicação de melhores práticas para desenvolvimento seguro e Segurança desde a Concepção.

Sem acordo, ou direitos autorais previamente expressos de outra forma, qualquer programa, sistema e/ou documentação gerada ou provida por colaboradores, consultores ou contratados, em benefício da ***LICITANET***, será de propriedade desta. Os gestores são responsáveis por assegurar esta propriedade através de assinatura de NDAs, cláusulas contratuais e outros instrumentos que tratem desta garantia.

Aquisição e implantação de novos sistemas devem considerar a verificação de requisitos mínimos de segurança da informação. A definição destes requisitos é responsabilidade da área de Infraestrutura e a verificação do emprego e uso adequado destes requisitos é da Alta Direção.

A Política Corporativa de Segurança da Informação ou seu resumo deve fazer parte como anexo de qualquer contrato envolvendo a aquisição e uso de novos sistemas. O fornecedor proponente deverá atender as condições estabelecidas neste documento para garantir a integridade, disponibilidade e confidencialidade das informações.

É mandatória a comprovação de melhores práticas de desenvolvimento seguro, realização de análise de vulnerabilidades e mapa de riscos de Segurança da Informação, para soluções e sistemas a serem adquiridos ou desenvolvidos externamente. Os sistemas devem apresentar recursos para controle de acesso lógico segregado e robusto, bem como capacidade para a execução e verificação de trilhas de auditoria. É responsabilidade da área Infraestrutura classificar os fornecedores e apresentar matriz de decisão técnica com aspectos, requisitos de SI e classificação de risco para estes.

13 GESTÃO DE RISCOS DE SI E CONTINUIDADE

O Comitê para Governança de Privacidade e Segurança da Informação (CGPSI) é responsável pela gestão de riscos de segurança da informação das Empresas. Portanto, deverá manter e monitorar a **Política Corporativa para Gestão de Riscos de Segurança da Informação** (PCGRSI), referência **POL-005**, em consonância com processo para gestão de inteligência de ameaças.

A área de Infraestrutura é responsável pela gestão de incidentes de Segurança da Informação, gerenciar e manter seus registros, bem como aplicar melhores práticas para contenção e resolução de causa raiz. Portanto, deverá manter processo e procedimento atualizado e testado pelo menos 1 (uma) vez ao ano para aferir a efetividade da gestão.

É responsabilidade da área de Infraestrutura manter e gerenciar um programa de gestão de vulnerabilidades e inteligência de ameaças de acordo com as melhores práticas de mercado e alinhado a gestão de risco de SI da ***LICITANET***.

É responsabilidade da área de Infraestrutura avaliar, manter e disponibilizar contingência de recursos críticos para a continuidade do negócio bem como aqueles necessários a continuidade da gestão de SI na ocorrência de eventos adversos.

Servidores, equipamentos de rede e segurança críticos ao negócio devem ser adquiridos e implementados com capacidades próprias para contingência tais como fontes redundantes, placas de rede alternativas, memória com

mecanismo para correção de erros, processadores duplos, placas controladoras e sistemas em alta disponibilidade. No caso da contratação de serviços de infraestrutura de TI em nuvem, os mesmos requisitos são aplicáveis. A arquitetura de processamento para serviços críticos deve ser analisada e validada quanto aos requisitos de contingência e continuidade.

14 SEGURANÇA CIBERNÉTICA

Serviços críticos e essenciais ao negócio da ***LICITANET*** devem ser protegidos de ataques cibernéticos de interrupção de serviços tais como DDoS (Ataques de Interrupção de Serviços Distribuídos), *ransomware*, envenenamento de DNS, divulgação de dados pessoais e outros. É responsabilidade da área de TI determinar as possíveis ameaças, definir e adotar medidas de proteção.

15 CONFORMIDADE

A conformidade com requisitos legais e contratuais é responsabilidade de todos os colaboradores da ***LICITANET***. Os gestores devem identificar e observar a legislação aplicável à ***LICITANET***, garantindo a adequação contratual e observância das diretrizes de Segurança da Informação desta Política.

Em especial os requisitos da Lei Geral de Proteção de Dados Pessoais (LGPD 13.709/2018) devem ser observados por todos os colaboradores visando preservar a privacidade do Titular dos Dados pessoais. Informações de Identificação Pessoal ou Dados Pessoais incluem qualquer informação que possa ser associada ou rastreada a qualquer indivíduo, incluindo o nome, endereço, número de telefone, endereço de e-mail, informações de cartão de crédito, número do CPF, RG, sexo, preferências religiosas, partidárias ou outras informações factuais específicas semelhantes independentemente da mídia na qual tais informações são armazenadas (por exemplo, em papel ou eletronicamente) incluem as informações que são geradas, coletadas, armazenadas ou obtidas como parte do exercício da função do colaborador no Contrato de Trabalho e negócios da ***LICITANET***, incluindo dados transacionais e outros referentes aos clientes.

O colaborador cumprirá todas as leis e regulamentos aplicáveis de privacidade (LGPD 13.709/2018) e outras leis relacionadas à proteção, coleta, uso e distribuição de Informações Pessoais Identificáveis. Em nenhum caso, o colaborador poderá vender ou transferir informações pessoalmente identificáveis a terceiros, ou fornecer acesso a elas sem a autorização formal e prévia.

A confidencialidade e sigilo de Dados Pessoais devem ser observados, preservados e garantidos por todos os colaboradores da ***LICITANET***. A área de Infraestrutura é responsável por propiciar mecanismos de proteção condizentes com a criticidade da informação e requerer estes aspectos de provedores de serviços e sistemas. Suspeitas de violação de Dados Pessoais devem ser comunicadas ao superior imediato e/ou envio de e-mail para privacidade@licitanet.com.br.

Relações contratuais com diretrizes de Segurança da Informação inferiores às contidas nesta Política devem ser evitadas e caso não haja opção, devem ser analisadas quanto ao risco e aprovadas formalmente pela Alta Direção.

Os gestores da organização devem observar e garantir direitos de propriedade intelectual de terceiros e da ***LICITANET***.

Enquanto durar a relação contratual, as patentes, invenções, direitos autorais, ou outras propriedades intelectuais tais como: estudos, projetos, relatórios e demais dados desenvolvidos pelo colaborador são de direito exclusivo da ***LICITANET*** que poderá registrá-los nos órgãos competentes e utilizá-los ou cedê-los sem qualquer restrição ou custo adicional.

A análise crítica e independente do processo de gestão de Segurança da Informação deve ser realizada pelo menos uma vez ao ano, considerando a capacidade orçamentária da empresa, por meio de auditoria interna ou externa especializada. A área de Infraestrutura é responsável pela garantia de isenção neste processo devendo acompanhar e zelar pela execução das correções de acordo com o risco para o negócio.

Anexo 1- Procedimentos Implementados para garantis a Segurança da informação na plataforma

A plataforma dispõe de uma série de mecanismos para assegurar a integridade e a confidencialidade das informações durante todas as etapas do processo licitatório, conforme descrito a seguir:

Seleção de Empresa e Geração de Token JWT: Após o login bem-sucedido, o usuário visualiza uma lista de empresas às quais possui acesso. Ao selecionar a empresa desejada, é gerado um Token JWT (JSON Web Token) com expiração definida em duas horas, utilizando a hash HS256 para garantir a segurança.Exemplo:
"eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE3MjQzMzMyNjgsImlzcyI6ImxpY2l0YW5ldC5jb20uYnIiLCJleHAiOjE3MjQzNDA0NjgsIm5iZiI6MTcyNDMzMzI2NywiZGF0YSI6eyJtb2MlM0QiOiJaMW10bFo4JTNEIiwiblpMYnp0dyUzRCI6Imw0am0wOCUyRlAyTmpQME5xWHBLRSUzRCIsImxKTFl4TkhRNGRuVnl0Q2hvZyUzRCUzRCI6IllnJTNEJTNEIiwibEpMWXhOVFE1dGZJek5HV242USUzRCI6IiIsImxKTFl4TlRXNHN6TTJOcVRvcHVnIjoiYVZXcCIsImxKTFl4T0xLNU5qQ3olMkJHZ2s1dWdrZFhYMTlBJTNEIjoiYVElM0QlM0QiLCJwWXprMUElM0QlM0QiOiJsSkxoMWVEQzJOalYiLCJscHZrenVERyI6IllscW1tYUdWcEoyWm9RJTNEJTNEIn19.Cfx7a_9xiqs8PI0BFOssGUpMtSqCGTrGt8B3ErcvZO". Este token contém informações essenciais, como a identificação do usuário, a empresa selecionada, o tipo de acesso concedido, quais funções podem ser executadas, e é utilizado em todas as requisições feitas ao servidor. As informações contidas no token são criptografadas com uma chave interna, proporcionando uma camada extra de proteção.

Controle de Acesso e Permissões: O token gerado é fundamental para o controle de acesso aos diferentes módulos da plataforma. Cada requisição ao servidor é acompanhada pelo token, que é verificado internamente para assegurar que o usuário possui as permissões necessárias para acessar o módulo solicitado. Somente com a confirmação dessas permissões os dados requisitados são retornados ao usuário. O token é utilizado em todas as requisições que são feitas no servidor, em conjunto com o módulo e a permissão que está desejando acessar. Internamente verificamos se aquele token tem acesso ao módulo requisitado e se sim, retornamos os dados.

Logs de Operações Sensíveis: As ações consideradas mais sensíveis, como cadastro, atualização ou exclusão de informações, são registradas em logs detalhados, que incluem informações como data, hora, IP do usuário, tipo de ação realizada, estado anterior e posterior das informações. Estes logs são armazenados em um banco de dados separado, em um servidor dedicado exclusivamente para essa finalidade, garantindo a segregação dos dados e aumentando a segurança.

Exemplo de Log: CADASTRO/ATUALIZAÇÃO PROPOSTA, POST, 2024-07-08 08:54:28, [], "[{""marca"":""SERVIÇO"",""modelo"":""SERVIÇO"",""valor"":""0.01"",""codFornecedor"":300,""codItem"":4298490,""codProposta"":14371651,""valorMinimo"" }]"

Acesso Restrito aos Logs: O acesso aos logs que contêm informações sensíveis é restrito e não está disponível diretamente na plataforma para os operadores. Os operadores têm acesso apenas aos logs que registram informações cadastrais, como alterações de e-mail, telefone, razão social, e renovação de planos. Isso limita o risco de exposição indevida de dados críticos.

Essas medidas visam garantir que a plataforma seja um ambiente seguro, íntegro e confiável para todos os envolvidos, protegendo as informações sensíveis em todas as fases da licitação.

Dispositivos de segurança como criptografia e anonimização de dados:

Nossa plataforma utiliza o produto Amazon Relational Database Service (RDS) que oferece suporte à **criptografia em repouso** para bancos de dados, incluindo MySQL, para proteger dados sensíveis. A criptografia de banco de dados em repouso refere-se à proteção dos dados armazenados em um banco de dados enquanto eles não estão sendo usados ou transferidos. Isso é feito para garantir que, mesmo que alguém consiga acessar os dados fisicamente ou por meios não autorizados, eles não possam ser lidos ou usados sem a chave de decriptação apropriada. A criptografia em repouso do Amazon RDS é gerenciada pelo AWS Key Management Service (KMS), que fornece uma maneira fácil e segura de criar e gerenciar chaves de criptografia.

Criptografia em Trânsito: Além da criptografia em repouso, o RDS também suporta a criptografia de dados em trânsito usando SSL/TLS para proteger a comunicação entre o banco de dados e os aplicativos.

Snapshots Criptografados: Quando você cria um snapshot de uma instância de banco de dados criptografada, o snapshot é automaticamente criptografado.

Restauração de Snapshots Criptografados: Você pode restaurar um snapshot criptografado em uma nova instância de banco de dados que também estará criptografada.

Réplicas: Réplicas de leitura de uma instância de banco de dados criptografada também são c riptografadas.

Criptografia Transparente: A criptografia de dados em repouso no RDS é transparente para a aplicação. Isso significa que as operações de criptografia e decriptação são gerenciadas automaticamente pelo RDS e são invisíveis para os usuários e aplicações que acessam o banco de dados.

Criptografia Tabelas do banco de dados

- **Tabela comprador**: Os campos **nome**, **CNPJ**, **email** e **telefone** são criptografados, assegurando que os dados sensíveis dos compradores estejam protegidos contra acessos não autorizados.
- **Tabela fornecedor**: Os campos **nome**, **CNPJ**, **CPF**, **email** e **telefone** são criptografados, oferecendo uma camada adicional de segurança para as informações dos fornecedores.
- **Tabela funcionário**: Os campos **nome**, **CPF**, **email** e **telefone** são criptografados, garantindo que os dados pessoais dos funcionários sejam armazenados de forma segura e protegida contra possíveis ameaças.
- **Tabela usuario**: Os campos login e senha são criptografados, garantindo que os dados de acesso dos usuários do sistema sejam armazenados de forma segura e protegida contra possíveis ameaças.

A criptografia aplicada tanto em repouso quanto em trânsito reforça o compromisso com a proteção das informações sensíveis em todas as tabelas do sistema, assegurando que não seja possível a identificação de pessoas ou empresas envolvidas durante a fase de disputa e em eventual violação ao banco de dados.

Anonimização e Confidencialidade na Sala de Disputa:

- **Anonimização de Dados**: Durante o processo de licitação, especialmente na sala de disputa, a identificação dos fornecedores é cuidadosamente protegida. No momento do cadastro da proposta, um ID dinâmico e único é gerado para cada processo, fornecedor e lote, sendo está a única forma de identificação visível ao pregoeiro no chat. Este ID é específico para cada item e lote, impedindo a identificação cruzada dos licitantes. Assim, até o momento do aceite das propostas, informações sensíveis como documentações, marca, modelo, CNPJ, e razão social dos participantes permanecem ocultas, garantindo a imparcialidade e a confidencialidade do processo.
-

Mecanismos para garantir a rastreabilidade e a auditabilidade dos processos licitatórios:

A plataforma possui mecanismos que garantem a rastreabilidade e a auditabilidade de todos os processos licitatórios, assegurando a transparência e integridade das operações realizadas. A seguir, descrevemos as principais funcionalidades que suportam essas garantias:

Transparência do Processo via Site: A plataforma disponibiliza o site da Licitanet, que apresenta publicamente os processos licitatórios, bem como editais, documentos de impugnação, esclarecimento etc. Esse site permite que qualquer interessado acompanhe as disputas em tempo real como visitante, proporcionando um alto nível de transparência ao processo. O acompanhamento ao vivo das disputas assegura que todas as etapas sejam visíveis e auditáveis por qualquer cidadão, reforçando a confiança na lisura do processo licitatório.

Chat na Sala de Disputa: Dentro da sala de disputa, a plataforma oferece um chat onde os condutores do processo e os licitantes podem se comunicar. Este chat é uma ferramenta essencial para a interação durante o processo, permitindo o envio de mensagens, entre fornecedores e condutores do processo, todas as mensagens possuem data e horário. Alguns exemplos de ação: prazo de documentação, declaração de vencedor, exclusão de lances, propostas desclassificadas entre outros. Todas as mensagens do chat e ações no processo constam na ata final do processo, garantindo que todas as interações sejam documentadas e possam ser auditadas. As mensagens do chat não podem ser excluídas.

Registro de Ações em Tabela de Logs: As ações realizadas pelos fornecedores no processo licitatório são registradas nas tabelas do sistema e seu log é armazenado em um banco de dados específico para logs, evitando qualquer tipo de alteração manual. Esta tabela armazena informações sobre as ações, incluindo data, hora, código do usuário, tipo de ação realizada. Esse registro permite a rastreabilidade completa das atividades, facilitando a auditoria e a verificação da conformidade com as normas estabelecidas.

Relatórios de Extrato e Envio de E-mails: A plataforma fornece o relatório de extrato do processo, que envia quem cadastrou, publicou, voltou publicação, suspendeu etc., o processo. Além disso, o sistema faz envio de e-mails de algumas ações, assegurando que todas as partes envolvidas sejam notificadas sobre eventos importantes do processo. Essas notificações via e-mail são parte do registro auditável, reforçando a transparência e a comunicação eficiente entre os participantes.

Esses mecanismos, integrados à plataforma, garantem que as etapas dos processos licitatórios sejam rastreáveis e auditáveis, atendendo às exigências de transparência e confiabilidade essenciais para o setor público.

Protocolos de Segurança:

Protocolo Secure Sockets Layer – SSL de ponta a ponta: Utilizamos SSL (Secure Sockets Layer) em todos os nossos servidores web. Isso garante que todas as comunicações entre os nossos servidores e os usuários sejam criptografadas, protegendo as informações contra interceptações e acessos não autorizados. Com essa abordagem, asseguramos que nossos clientes e parceiros possam confiar na integridade e confidencialidade de seus dados ao interagir com nossos serviços.

Firewall para bloqueio de boots e ataques indesejados: Em nossa infraestrutura na AWS, implementamos um rigoroso sistema de segurança utilizando o AWS WAF (Web Application Firewall) para proteger nossos servidores contra bots maliciosos e ataques indesejados. O AWS WAF nos permite criar regras customizadas para bloquear tráfego suspeito, protegendo nossos aplicativos web contra ameaças como ataques de negação de serviço (DDoS), injeções de SQL e outras explorações comuns. Além disso, utilizamos o firewall para filtrar bots indesejados, garantindo que apenas tráfego legítimo acesse nossos serviços, mantendo assim a segurança e a performance das nossas aplicações na nuvem.

***PenTeste* com detalhamento de impacto e criticidade – frequência de no mínimo 1 (uma) vez ao ano, por empresa reconhecida em Segurança da Informação:**

Realizamos um teste de penetração (pentest) completo uma vez por ano, conduzido por uma empresa reconhecida no ramo de segurança da informação. Este pentest envolve uma análise minuciosa e abrangente de nossos sistemas, identificando possíveis vulnerabilidades e avaliando a eficácia das nossas medidas de proteção. Ao realizar esses testes regularmente, garantimos que nossas defesas estejam sempre atualizadas e que nossos dados e os de nossos clientes permaneçam seguros contra ameaças emergentes. O relatório dos testes é armazenado em nossos servidores, caso precise revisar algum item ou algum teste.

Objetivos do Penteste: Identificar e analisar vulnerabilidades de segurança nas aplicações, garantindo a integridade, confidencialidade e disponibilidade dos serviços. Avaliar a eficácia dos controles de segurança, incluindo autenticação, autorização, criptografia e outras medidas de proteção de dados. Testar a resiliência das aplicações contra diversos tipos de ataques, como injeções SQL, XSS, CSRF, LFI, entre outros, garantindo uma postura robusta contra ameaças conhecidas. (Port Scan,XSS (Cross-site-scripting),CSRF (cross-site request forgery),IDOR (Insecure Direct Object Reference),SQLi (SQL Injection),Staging (Redirect to Phishing URL),Exploits,Bruteforce,DDOS (Distributed Denial of Service) & DOS (Denial of Service) dentre outras). Realizar uma análise minuciosa das vulnerabilidades documentadas pelo OWASP e outros órgãos

internacionais, abordando aspectos cruciais de segurança. (PCI Penetration Testing Guidance,NIST SP 800-115,OSSTMM).

Código Seguro: Adotamos as melhores práticas de programação para garantir a qualidade e a segurança de nosso software. Isso inclui a implementação de técnicas de programação segura, que nos permitem identificar e mitigar potenciais vulnerabilidades desde as fases iniciais de desenvolvimento. Nossos processos de codificação seguem padrões rigorosos, focando na prevenção de falhas, no controle de acesso, e na proteção contra ameaças comuns, como injeção de código e ataques de negação de serviço. Dessa forma, asseguramos que o software entregue seja robusto, confiável e seguro, alinhado às exigências de qualidade e segurança da informação.

Validação e Sanitização de Entradas:

- **Prevenção de Injeção SQL**: Validar e sanitizar todas as entradas de usuário para evitar que comandos maliciosos sejam executados no banco de dados.
- **Escapamento de Dados em HTML/CSS/JavaScript**: Impedir ataques de Cross-Site Scripting (XSS) ao escapar ou codificar caracteres especiais inseridos pelo usuário.

Autenticação e Autorização Fortalecidas:

- **Autenticação Multi-Fator (MFA)**: Adicionar uma camada extra de segurança além de senhas, exigindo múltiplas formas de verificação de identidade.
- **Controle de Sessão**: Implementar tokens de sessão seguros.

Gestão Segura de Senhas:

- **Hashing Seguro**: Utilizar algoritmos de hashing para armazenar senhas de forma segura.
- **Política de Senhas Fortes**: Encorajar ou exigir senhas complexas e longas, além de gerenciar expiração e rotação de senhas.

Configurações Seguras de Servidor:

- **TLS/SSL**: Criptografar o tráfego entre o cliente e o servidor utilizando HTTPS, garantindo que os dados em trânsito sejam protegidos.
- **Cabeçalhos de Segurança**: Configurar cabeçalhos como Content Security Policy (CSP), Strict-Transport-Security (HSTS), X-Frame-Options, e X-Content-Type-Options para mitigar ataques de XSS, clickjacking e outros.

Monitoramento e Logging:

- **Monitoramento Contínuo**: Implementar sistemas de monitoramento para detectar atividades suspeitas ou tentativas de ataque em tempo real.
- **Logging Seguro**: Manter registros detalhados de acesso e eventos, garantindo que os logs não exponham informações sensíveis e sejam armazenados com segurança.

Segurança na Camada de API:

- **Rate Limiting**: Limitar o número de requisições que um cliente pode fazer em um determinado período para evitar ataques de força bruta e DoS.

- **Autenticação e Autorização de API**: Usar OAuth, JWT, ou outras técnicas de autenticação robustas para garantir que apenas clientes autorizados possam acessar a API.

Atualização e Patching:

- **Gestão de Vulnerabilidades**: Manter todos os componentes do software, como bibliotecas, frameworks e servidores, sempre atualizados com os últimos patches de segurança.

Diferentes níveis de acesso com segregação de funções:

A plataforma Licitanet oferece três tipos de acesso, que apresentam seus perfis, funções e permissões específicas. Abaixo estão os perfis, suas respectivas funções e as permissões associadas:

Fornecedor: Esse acesso é utilizado pelos fornecedores, que tem acesso relacionado a proposta, cadastro, edição, participação na fase de lances, anexo de documentos, recurso, readequação da proposta final, assina das ARPS, convocações reserva e manutenção do próprio cadastro da empresa.

Esse acesso tem 3 tipos de perfis são eles:

Colaborador: Acessa com o próprio login e senha, navega por todo o sistema com a visão do fornecedor, cadastra proposta, edita, participa do processo, efetua lances, envia documentação, porém não faz a assinatura da proposta final.

Representante legal: Acessa com o próprio login e senha, navega por todo o sistema com a visão do fornecedor, cadastra proposta, edita, participa do processo, efetua lances, faz o envio da documentação, faz a assinatura da proposta final e da ARP e pode cadastrar colaboradores para sua empresa.

Funcionário interno: Os mesmos acessos que os Representante legal menos a parte de cadastrar proposta.

Comprador: Esse acesso é utilizado pelos Entes Compradores para realizarem ações relacionadas ao processo, como cadastro, edição, publicação, condução da sessão, adjudicação, homologação, cadastro de ETP, pesquisa de preço, envio de contratos, atas de registro de preço, convocações de reserva e manutenção do próprio cadastro do Órgão Comprador.

Esse acesso tem vários perfis são eles:

Autoridade Competente: Consegue navegar por todo o sistema, retirar relatórios, publicar, revogar, somente ele faz a ação de Adjudicar e Homologar os processos, assinar a ARP.

Pregoeiro: Cadastra novos operadores no órgão, cadastra, publica, edita e conduz os processos, revoga, cancela, fracassa, suspende, gera a ARP, faz a convocação do cadastro reserva, retira todos os relatórios, não faz homologação e adjudicação. Pode fazer quase tudo no processo, desde que estejam vinculados a ele.

Equipe de Apoio: Cadastra o processo, não faz a publicação nem a condução do processo, somente consegue acompanhar e baixar arquivos para conferência

Homologador: Consegue navegar por todo o sistema, retirar relatórios, publicar, revogar, somente ele faz a ação de Adjudicar e Homologar os processos, assinar a ARP.

Presidente CPL: Cadastra novos operadores no órgão, cadastra, publica, edita e conduz os processos, revoga, cancela, fracassa, suspende, gera a ARP, faz a convocação do cadastro reserva, retira todos os relatórios, não faz homologação e adjudicação.

Membro CPL: Cadastra o processo, não faz a publicação nem a condução do processo, somente consegue acompanhar e baixar arquivos para conferência

Compras: Não tem acesso aos processos, somente a tela de pesquisa de preços.

Equipe Técnica: Edita, faz o cadastro e a publicação do ETP.

Agente de Contratação: Cadastra novos operadores no órgão, cadastra, publica, edita e conduz os processos, revoga, cancela, fracassa, suspende, gera a ARP, faz a convocação do cadastro reserva, retira todos os relatórios, não faz homologação e adjudicação. Pode fazer quase tudo no processo, desde que estejam vinculados a ele.

Comissão de Contratação: Cadastra o processo, não faz a publicação nem a condução do processo, somente consegue acompanhar e baixar arquivos para conferência

Leiloeiro: Cadastra, publica, edita, conduz os processos, revoga, cancela, fracassa, suspende, gera a ARP, faz a convocação do cadastro reserva, retira todos os relatórios, não faz homologação e adjudicação. Pode fazer quase tudo no processo, desde que estejam vinculados a ele.

Gestor de contrato: Tem acesso apenas para cadastrar os contratos que serão enviados para o PNCP

Agente Público: Cadastra, publica, edita, conduz os processos, revoga, cancela, fracassa, suspende, gerar a ARP, faz a convocação do cadastro reserva, retira todos os relatórios, não faz homologação e adjudicação. Pode fazer quase tudo no processo, desde que estejam vinculados a ele.

Presidente (SESI-SENAI): Cadastra novos operadores no órgão, cadastra, publica, edita e conduz os processos, revoga, cancela, fracassa, suspende, gera a ARP, faz a convocação do cadastro reserva, retira todos os relatórios, não faz homologação e adjudicação. Pode fazer quase tudo no processo, desde que estejam vinculados a ele.

Comissão (SESI-SENAI): Cadastra o processo, não faz a publicação nem a condução do processo, somente consegue acompanhar e baixar arquivos para conferência

Pregoeiro (ESTATAL): Cadastra novos operadores no órgão, cadastra, publica, edita e conduz os processos, revoga, cancela, fracassa, suspende, gera a ARP, faz a convocação do cadastro reserva, retira todos os relatórios, não faz homologação e adjudicação.

Agente de Contratação (ESTATAL): Cadastra novos operadores no órgão, cadastra, publica, edita e conduz os processos, revoga, cancela, fracassa, suspende, gera a ARP, faz a

convocação do cadastro reserva, retira todos os relatórios, não faz homologação e adjudicação.

Pregoeiro/Agente (SE): Não pode: Excluir, suspender, cancelar, revogar, alterar dados do órgão, criar cargos, Homologar / Adjudicar, não mexe no processo após publicado, Não Publica, Fazer ETP, Enviar Contratos, visualizar/Alterar operadores do órgão. Pode: Cadastrar processo, editar enquanto não está publicado.

Equipe de Apoio/Comissão (SE): Não pode: Excluir, suspender, cancelar, revogar, alterar dados do órgão, criar cargos, Homologar / Adjudicar, não mexe no processo após publicado, Não Publica, Fazer ETP, Enviar Contratos, visualizar/Alterar operadores do órgão. Pode: Cadastrar processo, editar enquanto não está publicado.

Superintendente/Secretário/Autoridade Competente (SE): Está acima do pregoeiro, faz tudo que o pregoeiro não faz. Excluir, suspender, cancelar, revogar, alterar dados do órgão, criar cargos, Homologar / Adjudicar, Não mexe no processo após publicado, Não Publica, Fazer ETP, Enviar Contratos, Visualizar/Alterar operadores do órgão.

Armazenamento de documentos e informações da licitação, além dos publicados no PNCP, pelo período de 5 (cinco) anos a contar do certame:

A plataforma armazena todos os dados em nossa base de dados pelo período de 5 anos, conforme as políticas de retenção de dados estabelecidas. Durante esse período, os dados são protegidos por medidas de segurança robustas para garantir sua integridade e confidencialidade.

Armazenamento de Arquivos:

Adotamos o Amazon S3 como solução para o armazenamento definitivo de arquivos, garantindo alta durabilidade e disponibilidade. Além disso, implementamos práticas de segurança avançadas, como o **MFA Delete** (Multi-Factor Authentication Delete), que adiciona uma camada extra de proteção ao evitar a exclusão acidental ou mal-intencionada de arquivos.

Também utilizamos a funcionalidade de versionamento de arquivos no S3, permitindo que todas as alterações realizadas sejam registradas e que versões anteriores possam ser restauradas se necessário. Essa abordagem garante a integridade dos dados e facilita a recuperação em casos de modificação ou exclusão acidental, alinhando-se às melhores práticas de gestão e segurança da informação.

16 REFERÊNCIAS

Lei Geral de Proteção de Dados Pessoais (LGPD) 13.709/2018.

Lei nº 14.133/2021 Lei de Licitações e Contratos Administrativos.

Portaria nº 93, de 26 de setembro de 2019 – Glossário de Segurança da Informação.

Portaria-TCU nº 89/2023 - Corporativa de Segurança da Informação do Tribunal de Contas da União (PCSI/TCU).

Decreto oº 11.856/2023 - Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança.

Norma ABNT NBR ISO/IEC 27001:2022 – *Segurança da informação, segurança cibernética e proteção à privacidade. Sistemas de gestão de segurança da informação — Requisitos.*

Norma ABNT NBR ISO/IEC 27002:2022 – *Segurança da Informação, segurança cibernética e proteção à privacidade – Controles de Segurança da Informação.*

Norma ABNT NBR ISO/IEC 27701:2019 – *Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes.*

POL-002 – Política Corporativa para Classificação da Informação.

POL-003 – Política Corporativa para Desenvolvimento Seguro.

POL-004 – Estatuto do Comitê para Gestão de Privacidade e Segurança da Informação – CGPSI.

POL-005 – Política Corporativa para Gestão de Riscos de Segurança da Informação.

17 VERSIONAMENTO

DATA	VERSÃO	RESPONSÁVEL	DESCRIÇÃO
10/01/2025	V1r0	Edmo Lopes Filho	Elaboração e revisão final da PSI.
03/04/2025	V1r0	Edmo Lopes Filho	Assinatura pelo CEO e publicação da PSI.

18 APROVAÇÃO

ELABORAÇÃO:	***VALIDAÇÃO:***
Noussec Tecnologia da Informação LTDA	
Área Emitente *Edmo Lopes Filho*	*CEO* *Paulo Gustavo Lourenço de Oliveira*

19 GLOSSÁRIO SUPLEMENTAR

Acesso remoto – Acesso no qual o usuário utiliza-se de algum mecanismo, rede ou ligação telefônica, para obter acesso a um sistema fisicamente localizado em outro local. Exemplos incluem um acesso via VPN, através de linha discada, banda larga.

Access Point (AP) - Ponto de acesso sem fio, dispositivo que atua como ponte entre uma rede sem fio e uma rede tradicional.

Anonimização - utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

Antivírus - Programa ou software especificamente desenvolvido para detectar, anular e eliminar de um computador vírus e outros tipos de código malicioso.

Atacante - Pessoa responsável pela realização de um ataque. Veja também Ataque.

Ataque - Tentativa, bem ou mal-sucedida, de acesso ou uso não autorizado a um programa ou computador. Também são considerados ataques quaisquer tentativas de negação de serviço.

Backdoor - Código malicioso instalado em um computador, geralmente sem o consentimento do usuário. O *backdoor* provê uma porta dos fundos por onde um hacker pode obter acesso oportunamente.

Backup - Processo que objetiva manter as informações a salvo de problemas nos meios de armazenamento, é feita uma cópia de segurança que pode ser restaurada caso haja necessidade.

Banco de dados - conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

Banner - É uma forma comum na internet, em que as empresas utilizam para divulgar informações de seus sistemas para seus colaboradores através de um “anúncio” na tela.

Cavalo de Tróia - Programa, normalmente recebido como um "presente" (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo, etc), que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário.

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, *worms*, *bots*, cavalos de Tróia, *rootkits*, etc.

Colaborador - O mesmo que funcionário.

Consentimento - Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Controlador - pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

Criptografia - Ciência e arte de escrever mensagens em forma cifrada ou em código. É parte de um campo de estudos que trata das comunicações secretas. É usada, dentre outras finalidades, para: autenticar a identidade de usuários; autenticar transações bancárias; proteger a integridade de transferências eletrônicas de fundos, e proteger o sigilo de comunicações pessoais e comerciais.

Cracker - Os crackers são pessoas aficionadas por informática que utilizam seu grande conhecimento na área para quebrar códigos de segurança, senhas de acesso a redes e códigos de programas com fins criminosos. Em alguns casos, o termo “Pirata Virtual” é usado como sinônimo para cracker.

Dado pessoal - informação relacionada a pessoa natural identificada ou identificável;

Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

DDoS - *Distributed Denial of Service*. Tipo de ataque cibernético onde os recursos são exauridos em sua capacidade de forma a se impedir o acesso ou uso final pelo cliente.

Desktop - Veja Estação de trabalho.

Dispositivo Móvel - Designado popularmente em inglês por handheld é um computador de bolso habitualmente equipado com um pequeno monitor e um teclado em miniatura (entrada de informação). No caso dos PDAs, a saída de informação e a entrada combinam-se em um monitor tipo *touch screen*. Os dispositivos móveis mais comuns são: Smartphones, PDA, Console portátil, tablets, notebooks e televisão portátil.

DNS - *Domain Name System* – Serviço de Internet que transforma a URL em um endereço localizável. Responsável por descodificar os nomes dos domínios dos sites que as pessoas digitam nos navegadores web em números IP.

E-mail - Veja Endereço eletrônico.

Endereço eletrônico - É um método que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação.

Endereço IP - Este endereço é um número único para cada computador conectado à Internet, composto por uma sequência de 4 números que variam de 0 até 255, separados por ".". Por exemplo: 192.168.34.25.

Engenharia social - Método de ataque onde uma pessoa faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações.

Estação de trabalho - Nome genérico dado a computadores, situados, em termos de potência de cálculo, entre o computador pessoal e o computador de grande porte.

Feedback - O significado de feedback é utilizado em teorias da Administração de Empresas, quando é dado um parecer sobre uma pessoa ou grupo de pessoas na realização de um trabalho com o intuito de avaliar o seu desempenho. É uma ação que revela os pontos positivos e negativos do trabalho executado tendo em vista a melhoria do mesmo.

Firewall - Dispositivo constituído pela combinação de software e hardware, utilizado para dividir e controlar o acesso entre redes de computadores.

Freeware - Software de livre distribuição, não é necessário que sejam adquiridas licenças para que tal tipo de software seja usado.

FTP - *File Transfer Protocol*, é um protocolo de transferência de arquivos muito utilizado na Internet. Este protocolo não tem mecanismos de segurança em sua implementação.

Hacker - Indivíduo com elevados conhecimentos de computação e segurança que os utiliza com propósitos de identificar e publicar falhas relacionadas à segurança em aplicativos, sistemas e equipamentos.

Hardware - Parte física do computador, equipamento de rede e outros.

HTTPS - HTTPS é um protocolo de segurança que criptografa a comunicação entre um navegador e um site. A sigla significa "*Hypertext Transfer Protocol Secure*".

IA Generativa - Inteligência Artificial Generativa – é um tipo de Inteligência Artificial que pode criar conteúdo e ideias, incluindo conversas, histórias, imagens, vídeos e músicas.

Invasão – Ataque que resulte no acesso, manipulação ou destruição de informações em um computador.

Invasor - Pessoa responsável pela realização de uma invasão (comprometimento). Veja também Invasão.

IP - Veja Endereço IP.

IPsec - IPsec (*IP Security Protocol*) é um conjunto de protocolos que protege as comunicações na internet. Ele é usado para criar conexões seguras entre dispositivos, como redes virtuais privadas (VPNs).

Laptop - Veja Estação de trabalho.

Log - Registro de atividades gerado por programas de computador. No caso de logs relativos a incidentes de segurança, eles normalmente são gerados por firewalls ou por IDSs (Sistemas de Detecção de Intrusos).

Malware - Do Inglês *malicious* software (software malicioso). Veja Código malicioso.

Mídia Removível - É qualquer meio de armazenamento que pode facilmente ser conectado e desconectado de computadores, exemplos incluem disquetes, CD's, DVD`s, ZipDrives, PenDrives, fitas magnéticas e outros.

Mídia Magnética ou ópticas - é uma mídia de armazenamento não-volátil que consiste em uma fita plástica coberta de material magnetizável. A fita pode ser utilizada para registro de informações analógicas ou digitais, incluindo áudio, vídeo e dados de computador.

Notebook - Veja Estação de trabalho.

Operador - pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Password - Veja Senha.

Phishing - Também conhecido como *phishing scam* ou *phishing/scam*. Mensagem não solicitada que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou site popular, e que procura induzir usuários ao fornecimento de dados pessoais e financeiros. Inicialmente, este tipo de mensagem induzia o usuário ao acesso a páginas fraudulentas na Internet. Atualmente, o termo também se refere à mensagem que induz o usuário à instalação de códigos maliciosos, além da mensagem que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros.

Ransomware – Tipo de vírus que criptografa as informações do computador e exige resgate para recuperação das mesmas pago em moeda virtual.

Rede sem fio – (*Wireless*) Rede que permite a conexão entre computadores e outros dispositivos através da transmissão e recepção de sinais de rádio.

Rootkits – Conjunto de código malicioso que substitui o código original e executa ações programadas pelo agressor, escondendo-se da detecção padrão executada através de comandos do sistema operacional.

Scam - Esquemas ou ações enganosas e/ou fraudulentas. Normalmente, têm como finalidade obter vantagens financeiras.

Scan - Técnica normalmente implementada por um tipo de programa, projetado para efetuar varreduras em redes de computadores. Veja Scanner.

Scanner - Programa utilizado para efetuar varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. Amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.

Screensaver - Imagem animada que é ativada quando nenhuma atividade no computador do usuário for detectada por um determinado tempo.

Senha - Conjunto de caracteres, de conhecimento único do usuário, utilizado no processo de verificação de sua identidade, assegurando que ele é realmente quem diz ser.

Servidor c Sistema de computação que fornece serviços a uma rede de computadores. Esses serviços podem ser de natureza diversa, por exemplo, arquivos e correio eletrônico

Service Desk - É uma central de serviços que conecta a empresa aos seus clientes, parceiros e colaboradores. Recebe, registra e gerencia tíquetes de serviços de TI, incidentes e dúvidas.

SFTP – É a sigla para *Secure File Transfer Protocol*, que significa Protocolo de Transferência de Arquivos Segura. É um protocolo de rede que permite a transferência de arquivos entre um servidor e um cliente de forma segura.

Software - Um programa de computador é composto por uma sequência de instruções, que é interpretada e executada por um processador ou por uma máquina virtual. Em um programa correto e funcional, essa sequência segue padrões específicos que resultam em um comportamento desejado

Spam - Termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para muitas pessoas. Quando o conteúdo é exclusivamente comercial, este tipo de mensagem também é referenciada como UCE (do *Inglês Unsolicited Commercial* E-mail).

Spammer - Indivíduo que envia spam.

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.

SSH - *Secure Shell* (SSH) é um protocolo de rede criptográfico para operação de serviços de rede de forma segura sobre uma rede insegura. O melhor exemplo de aplicação conhecido é para login remoto de utilizadores a sistemas de computadores.

Titular - pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Tratamento - toda operação realizada com as informações, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Touch screen – Sensível e responsivo ao toque.

Trojan Horse - Veja Cavalo de Tróia.

UCE - Do inglês *Unsolicited Commercial* E-mail. Termo usado para se referir aos e-mails comerciais não solicitados.

URL - Do Inglês *Universal Resource Locator*. URL – é a especificação de endereços de páginas web.http://www.virtualconnection.com.br/

Uso compartilhado de dados - comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

Verme - Um tipo especial de vírus que não depende de estímulo para ser ativado, geralmente usa a rede para novas infecções.

Vírus - Programa ou parte de um programa de computador, normalmente malicioso, que se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador. O vírus depende da execução do programa ou arquivo hospedeiro para que possa se tornar ativo e dar continuidade ao processo de infecção.

VPN - *Virtual Private Network* é uma rede que provê uma conexão remota de forma segura. Muito utilizada por usuários que estão fora das dependências da empresa e para a interconexão de várias unidades de uma empresa.

Vulnerabilidade - Falha no projeto, implementação ou configuração de um software ou sistema operacional que, quando explorada por um atacante, resulta na violação da segurança de um computador.

Wi-Fi - Do Inglês *Wireless Fidelity*. Termo usado para se referir genericamente a redes sem fio que utilizam qualquer um dos padrões 802.11.

Wireless - Veja Rede sem fio.

Worms - Programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o *worm* não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar. Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de softwares instalados em computadores.