POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

POL.TEC.SI.005 | 30 DE SETEMBRO DE 2024

SUMÁRIO

1. OBJETIVO

Orientar e estabelecer o padrão de Segurança da Informação do CAP, fornecendo as diretrizes de conduta para empregados, estagiários, aprendizes, terceiros, prestadores de serviços do CAP, eventuais visitantes que tenham acesso a informações, Presidente, Vice-Presidentes, seus Diretores e Assessores nomeados no contexto de suas atividades, membros do Conselho Deliberativo e do Conselho Fiscal, no uso adequado e seguro de recursos de informação, assim como as responsabilidades e deveres de todos os envolvidos nas atividades do CAP.

Todas as diretrizes estabelecidas neste documento são construídas para preservar os três aspectos básicos de segurança, sendo eles:

i. **Confidencialidade:** É o aspecto relacionado a divulgação não autorizada, acesso e uso indevido das informações do CAP.

ii. **Integridade:** A propriedade de que a informação não foi modificada ou corrompida, ou seja, preserva sua exatidão; e

iii. **Disponibilidade:** A propriedade de que a informação esteja disponível para uso devido dos usuários autorizados.

2. ABRANGÊNCIA E APLICAÇÃO

As regras, recomendações e conceitos desta Política são aplicáveis a todos empregados, estagiários, aprendizes, terceiros, prestadores de serviços do CAP, eventuais visitantes que tenham acesso a informações, Presidente, Vice-Presidentes, seus Diretores e Assessores nomeados no contexto de suas atividades, membros do Conselho Deliberativo e do Conselho Fiscal.

Todos esses grupos são denominados 'usuários" sempre que tratados de forma indistinta neste documento.

Empregados, estagiários e prestadores de serviços que trabalham na área da Tecnologia da Informação distinguem-se dos demais usuários pelo fato de possuírem obrigações, direitos e privilégios diferenciados para a necessária administração do ambiente computacional e de rede e, neste documento, são denominados "equipe de TI".

Todos, indistintamente, são responsáveis pela observação e cumprimento da Política de Segurança da Informação.

3. TERMINOLOGIA E CONCEITOS

Campo destinado à definição de conceitos e siglas, se necessário.

ITEM	DEFINIÇÃO
Software	É a parte lógica, o conjunto de instruções e dados processados nos servidores e computadores. Toda interação dos usuários de computadores é realizada através de softwares.
Backup	É a cópia de dados de um dispositivo de armazenamento a outro para que possa ser restaurado em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados.
Firewall	É um dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.
Spam	E-mails não solicitados e normalmente enviados para muitas pessoas.
Custodiante	Quem detém a guarda da informação, mas não é necessariamente seu proprietário.
Vírus	Programa malicioso que se propaga e infecta o computador.
Cavalo de Troia	Programa malicioso que cria abertura para outros programas e invasões indesejadas.
Ativo	Patrimônio composto por bens e direitos do CAP.
Ativo de TI	Equipamentos ou programas de computador que suportam o ambiente organizacional e de negócios do CAP.
Ferramentas	É um conjunto de equipamentos, programas, procedimentos, processos e demais recursos através dos quais se aplica a Política de Segurança da Informação do CAP.
Ativos de informação	É o patrimônio composto por todos os dados e informações gerados e manipulados durante a execução dos sistemas e processos do CAP.
Ativos de processamento	É o patrimônio composto por todos os elementos de hardware e software necessários para a execução dos sistemas e processos do CAP, tanto os produzidos internamente quanto os adquiridos.
CFTV – Circuito fechado de Televisão	É um sistema consiste na captação de imagens realizadas por câmeras digitais ou analógicas que permitem a vigilância de ambientes por meio de monitores conectados a gravadores de vídeo ou rede central.

4. CONSIDERAÇÕES INICIAIS

4.1. REGRAS GERAIS

Para o perfeito entendimento e aplicação desta Política são estabelecidas as seguintes regras gerais:

i. Toda e qualquer ação em relação a informação no CAP deve ser orientada explicitamente por esta Política resguardando os direitos e penalidades conforme legislação vigente;

ii. Todas as regras, recomendações e quaisquer outras ações contidas nesta Política não podem se sobrepor a legislação vigente;

iii. A Política de Segurança da Informação do CAP se aplica a todos os seus recursos humanos, administrativos e tecnológicos. A abrangência dos recursos citados refere-se tanto àqueles ligados a ela em caráter permanente como em temporário;

iv. Os processos de aquisição de bens e serviços, especialmente de TI, estão em conformidade com esta Política;

4.2. DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE

Para garantir as regras mencionadas nesta Política, o CAP poderá:

i. Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes de rede. A informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

ii. Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação de gerente (ou superior) ou por solicitação da Diretoria de Governança;

iii. Realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;

iv. Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

4.2.1. Requisitos de segurança do ambiente físico

Os requisitos de segurança do ambiente físico seguem os seguintes critérios abaixo:

i. A localização das instalações e os sistemas do CAP não são publicamente identificados;

ii. Sistemas de segurança para acesso físico estão instalados para controlar e auditar o acesso aos sistemas do CAP;

iii. Controles duplicados sobre o inventário e cartões/chaves de acesso devem ser mantidos acompanhados de lista atualizada do pessoal que possui cartões/chaves;

iv. Chaves criptográficas sob custódia do responsável são fisicamente protegidas contra acesso não autorizado, uso ou duplicação;

v. Perdas de cartões/chaves de acesso são imediatamente comunicadas ao responsável pela gerência de segurança da informação do CAP que tomará as medidas apropriadas para prevenir acessos não autorizados;

vi. Recursos e instalações críticas ou sensíveis são mantidos em áreas seguras, protegidas por um perímetro de segurança definido, com controle de acesso. Elas são fisicamente protegidas de acesso não autorizado, dano ou interferência. A proteção fornecida é proporcional aos riscos identificados;

vii. A entrada e saída, nestas áreas ou partes dedicadas, são automaticamente registradas com data e hora definidas e são revisadas periodicamente pela área responsável pela segurança da informação do CAP e mantidas em local adequado e sob sigilo;

viii. O acesso aos componentes da infraestrutura, atividade fundamental ao funcionamento dos sistemas do CAP, como painéis de controle de energia, comunicações e cabeamento, é restrito ao pessoal autorizado;

ix. Sistemas de detecção de intrusão são utilizados para monitorar e registrar os acessos físicos aos sistemas de certificação nas horas de utilização;

x. O inventário de todo o conjunto de ativos de processamento é registrado e deve ser mantido atualizado, no mínimo, semestralmente;

xi. Quaisquer equipamentos de gravação (fotografia, vídeo, som ou outro tipo de equipamento similar) só são utilizados a partir de autorização formal da TI e mediante supervisão;

xii. Nas instalações do CAP, todos os empregados e parceiros devem utilizar alguma forma visível de identificação (por exemplo, crachá) e devem informar à Segurança sobre a presença de qualquer pessoa não pertencente àquela área;

xiii. Visitantes das áreas de segurança são supervisionados. Suas horas de entrada e saída e o local de destino são registrados. Essas pessoas obtêm acesso apenas às áreas específicas, com propósitos autorizados, e esses acessos seguem instruções baseadas nos requisitos de segurança da área visitada;

xiv. Os ambientes onde ocorrem os processos críticos do CAP são monitorados, em tempo real, com as imagens registradas por meio de sistemas de circuito fechado de televisão – CFTV;

xv. Nos ambientes onde ocorrem processos críticos, existe sistema de detecção de intrusos instalados e testados regularmente de forma a cobrir os ambientes, as portas e janelas acessíveis;

xvi. As condições de uso definem os padrões e as recomendações de segurança que os usuários devem cumprir para obter acesso aos ativos de TI do CAP;

xvii. Os ativos de TI são de propriedade do CAP e são de uso exclusivo para execução dos trabalhos.

4.2.2. Utilização de hardware

i. Os ativos de hardware de TI devem ter seu uso racional, observando os limites de utilização estabelecidos pelo CAP;

ii. É dever de todos os usuários proteger os ativos de TI contra qualquer tipo de danos e perdas;

iii. O Departamento de TI poderá efetuar e/ou autorizar qualquer tipo de alteração e reparo interno ou externo nos ativos;

iv. Os usuários dos ativos da TI somente estão autorizados a utilizar os hardwares homologados pelo CAP;

4.2.3. É proibido aos usuários:

i. Disponibilizar o acesso a pessoas não autorizadas;

ii. Instalar ou alterar as configurações do hardware sem autorização formal do Departamento de TI;

iii. Instalar servidores, computadores, periféricos e acessórios na infraestrutura computacional, sem prévia autorização formal do Departamento de TI;

iv. Promover qualquer manutenção ou tentativa de manutenção dos ativos de TI;

4.2.4. Cópias de segurança (backup)

i. É necessário que a área de TI realize regularmente os backups e teste de restauração desses backups, bem como o armazenamento dos dados nos sistemas do CAP de acordo com a sua classificação.

ii. Os backups devem ser armazenados externamente ou em uma área separada do arquivo original e apropriadamente protegida, sendo somente acessível por pessoas autorizadas.

4.3. GESTÃO DE ATIVOS DE INFORMAÇÃO

Os ativos de informação devem:

i. Ser inventariados e protegidos;

ii. Ter identificados os seus proprietários e custodiantes;

iii. Ter mapeadas as suas ameaças, vulnerabilidades e interdependências;

iv. Ter a sua entrada e saída nas dependências do CAP autorizadas e registrada por responsável.

v. Ser passíveis de monitoramento e ter seu uso investigado quando houver indícios de quebra de segurança, por meio de mecanismos que permitam a rastreabilidade do uso desses ativos;

vi. ser utilizados estritamente dentro do seu propósito, sendo vedado seu uso para fins particulares ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins.

E, além disso:

vii. O CAP deve criar, gerir e avaliar critérios de tratamento da informação de acordo o sigilo requerido, relevância, criticidade e sensibilidade, observando a legislação em vigor.

viii. Os recursos tecnológicos e as instalações de infraestrutura devem ser protegidos contra indisponibilidade, acessos indevidos, falhas, bem como perdas, danos, furtos, roubos e interrupções não programadas.

ix. Os sistemas de informação devem ser protegidos contra indisponibilidade, alterações ou acessos indevidos, falhas e interrupções não programadas.

x. O acesso dos usuários aos ativos de informação e sua utilização, quando autorizados, deve ser condicionado ao aceite a termo de sigilo e responsabilidade.

xi. Os ativos de informação devem possuir mecanismos que permitam a auditoria dos eventos de acesso e alteração de registros. Esta auditoria deve estar sempre ativa (salvo quando explicitamente dispensado este requisito) e os registros devem ser armazenados pelo período mínimo de um ano.

4.4. GESTÃO DE RISCOS E INCIDENTES

O gestor dos ativos de informação deve estabelecer processos de gestão de riscos de segurança da informação que possibilitem identificar ameaças e reduzir vulnerabilidades dos ativos de informação, assim como reduzir os impactos de eventuais incidentes.

A gestão de riscos de segurança da infração é um processo contínuo e deve ser aplicado na implementação e operação, levando em consideração o planejamento, execução, análise crítica e melhorias da segurança da informação do CAP.

4.5. SEGURANÇA EM RECURSOS HUMANOS

i. Os usuários devem ter ciência:

- Das ameaças e preocupações relativas à segurança da informação e;
- De suas responsabilidades e obrigações no âmbito desta política.

ii. Todos os usuários devem difundir e exigir o comprimento da Política de Segurança da Informação, das normas de segurança e da legislação vigente acerca do tema.

iii. Devem ser estabelecidos processos permanentes de conscientização, participação, sensibilização em segurança da informação, que alcancem todos os destinatários de acordo com seu relacionamento e atribuições no CAP.

iv. Deve ser implementado controles de perfis, permissões e procedimentos necessários para salvaguarda dos ativos de informações do CAP.

4.6. POLÍTICA DE ANTIVÍRUS

i. Todos os recursos de informação aplicáveis devem estar configurados com software antivírus aprovados pelo Área de Segurança da Informação. A solução antivírus deve ser capaz de detectar, remover e proteger contra todos os tipos de software malicioso tais como vírus, trojans, worms, spyware, adware e rootkits. O software deve estar configurado para receber atualizações automáticas, executar varreduras periódicas, registrar eventos com vírus em uma solução central de login, e os usuários finais não devem ser capazes de configurar ou desabilitar o software;

ii. Todos os sistemas com software antivírus devem estar configurados para atualizar as assinaturas de vírus e realizar varreduras ao menos semanalmente;

iii. O software antivírus deve alertar a Área de Segurança da Informação em tempo real sobre a detecção de qualquer vírus e gravar tais eventos em um servidor de log central.

4.7. DIRETRIZES QUANTO À UTILIZAÇÃO DA REDE CORPORATIVA

i. A rede de computadores do CAP deve ser utilizada de forma proficiente e produtiva, mantendo sua integridade, disponibilidade e confidencialidade das informações e conhecimento.

ii. É expressamente proibido o uso, sem autorização, de softwares não aderentes à política de segurança do CAP;

iii. Seja localmente em seu computador ou por meio da rede, os usuários não podem alterar copiar e/ou excluir arquivos pertencentes a outro usuário sem sua permissão;

iv. A rede não deve ser utilizada para transmitir ou armazenar informações que não sejam do interesse ou não contribuam com os objetivos do CAP;

v. O tráfego das informações no ambiente de rede deve ser protegido contra danos ou perdas, bem como acesso, uso ou exposição indevida, e os componentes críticos da rede local deve ser mantido em salas protegidas e com acesso físico e lógico controlado, sendo protegidos contra danos, furtos, roubos e intempéries;

vi. Devem ser adotadas as facilidades de segurança disponíveis de forma inata nos ativos de processamento da rede; contudo, a configuração de todos os ativos de processamento será averiguada quando da sua instalação inicial, para que sejam detectadas e corrigidas as vulnerabilidades inerentes à configuração padrão que se encontram nesses ativos em sua primeira ativação;

vii. Serviços vulneráveis devem receber nível de proteção adicional, e o uso de senhas é submetido a uma política específica para sua gerência e utilização;

viii. O acesso lógico aos recursos da rede local deve ser realizado por meio de sistema de controle de acesso. O acesso é concedido e mantido pela administração da rede, baseado nas responsabilidades e tarefas de cada usuário;

ix. Os ativos de TI e quaisquer informações e conteúdos neles armazenados pertencem ao CAP; sendo assim, serão submetidos a processos de monitoramento de tráfego e segurança, garantindo estabilidade, integridade, disponibilidade e confidencialidade do ambiente. Ressalta-se que o CAP não necessitará de qualquer tipo de aviso ou autorização judicial para executar tais ações;

x. O tráfego de informações poderá/deverá ser monitorado, a fim de verificar sua normalidade, assim como detectar situações anômalas do ponto de vista da segurança; igualmente serão observadas as questões envolvendo propriedade intelectual quando da cópia de software ou arquivos de outras localidades;

xi. A utilização por trabalhadores terceirizados de qualquer mecanismo capaz de realizar testes de qualquer natureza, como por exemplo, monitoramento de dados dos sistemas e dispositivos que compõem a rede, somente serão utilizados a partir de autorização formal e mediante supervisão do Departamento de TI;

xii. Devem ser definidos relatórios de segurança (logs) de modo a auxiliar no tratamento de desvios, recuperação de falhas, contabilização e auditoria. Os logs são analisados periodicamente e o período de análise estabelecido deve ser o menor possível;

xiii. Devem ser adotadas proteções físicas adicionais para os recursos de rede considerados críticos, e a proteção lógica adicional é adotada para evitar o acesso não autorizado às informações;

xiv. A conexão com outros ambientes de rede e alterações internas na sua topologia e configuração devem ser formalmente documentadas e mantidas, de forma a permitir registro histórico. O diagrama topológico, a configuração e o inventário dos recursos são mantidos atualizados;

xv. Informações sigilosas, corporativas ou que possam causar prejuízo ao CAP são protegidas e não serão enviadas para outras redes, sem proteção adequada;

xvi. Todo serviço de rede não explicitamente autorizado será bloqueado ou desabilitado, e mecanismos de segurança baseados em sistemas de proteção de acesso (firewall) serão utilizados para proteger as transações entre redes externas e a rede interna do CAP;

xvii. Adoção de um padrão de segurança para todos os tipos de equipamentos servidores, considerando aspectos físicos e lógicos, e todos os recursos considerados críticos para o ambiente de rede, e que possuam mecanismos de controle de acesso;

xviii. A localização dos serviços baseados em sistemas de proteção de acesso (firewall) deve ser resultante de uma análise de riscos. Os seguintes aspectos devem ser considerados: requisitos de segurança definidos pelo serviço, objetivo do serviço, público-alvo, classificação da informação, forma de acesso, frequência de atualização do conteúdo, forma de administração do serviço e volume de tráfego;

xix. Ambientes de rede considerados críticos devem ser isolados de outros ambientes de rede, de modo a garantir um nível adicional de segurança;

xx. Conexões entre as redes do CAP e redes externas estarão restritas somente àquelas que visem efetivar os processos;

xxi. As conexões de rede são ativadas: primeiro, sistemas com função de certificação; segundo, sistemas que executam as funções de registros e repositório. Se isto não for possível,

emprega-se controles de compensação, tais como o uso de proxies que são implementados para proteger os sistemas que executam a função de certificação contra possíveis ataques;

xxii. Sistemas que executam a função de certificação estão isolados para minimizar a exposição contra tentativas de comprometer o sigilo, a integridade e a disponibilidade das funções de certificação;

xxiii. As ferramentas de detecção de intrusos devem ser implantadas para monitorar as redes críticas, alertando os administradores das redes sobre as tentativas de intrusão. Os registros de eventos serão analisados periodicamente, no menor prazo possível e em intervalos de tempo adequados.

4.8. SENHAS

O CAP adota política de troca obrigatória de senhas com período de uso contínuo de no máximo 90 (noventa) dias.

A senha é o meio de validação de acessos a recursos e serviços, funcionando como a assinatura digital do empregado, portanto, devem ser verificados os seguintes cuidados básicos para sua proteção:

i. Manter sua confidencialidade;
ii. Criar senhas fortes, respeitando, ao menos, os critérios abaixo:
   - As senhas não podem ser óbvias, como senhas sequenciais (ex.: sequências numéricas ou alfabéticas) ou derivadas de dados pessoais (ex.: nome ou data de nascimento do usuário), e;
   - Devem ter pelo menos 8 caracteres, com ao menos um caractere especial e um número.

Os acessos, validados por meio da utilização de senha, serão limitados aos recursos e serviços necessários para o desempenho das atividades exercidas por cada empregado, e poderão ser revogados rapidamente quando necessário.

4.9. CORREIO ELETRÔNICO

O uso do correio eletrônico do CAP é para fins corporativo relacionados as atividades do usuário.

É expressamente proibido:

i. Enviar ou ser conivente com conteúdo não aderente a esta Política de Segurança da Informação;

ii. Enviar mensagens para listas de fornecedores e parceiros que não sejam de interesse do CAP sem a devida autorização da área responsável;

iii. Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas ao uso legítimo da instituição;

iv. Enviar mensagens por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;

v. Enviar mensagens que configurem phishing para usuários internos e externos;

vi. Enviar mensagens com a identificação do remetente alterada ou falsificada;

vii. Enviar mensagens com o conteúdo alterado ou falsificado;

viii. Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;

ix. Enviar informações confidenciais do CAP; para redes públicas (internet), sem autorização;

x. Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;

xi. Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou o CAP vulneráveis a ações civis ou criminais;

xii. Apagar mensagens pertinentes de correio eletrônico quando estiver sujeita a algum tipo de investigação.

xiii. Produzir, transmitir ou divulgar mensagem que contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses do CAP;

xiv. Enviar mensagens que contenham ameaças eletrônicas, como: spam, vírus de computador, ou arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;

xv. Enviar mensagens objetivando obter acesso não autorizado a outro computador, servidor ou rede;

xvi. Enviar mensagens objetivando interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

xvii. Enviar mensagens objetivando burlar qualquer sistema de segurança;

xviii. Enviar mensagens objetivando vigiar secretamente ou assediar outro usuário;

xix. Enviar mensagens objetivando acessar informações confidenciais sem explícita autorização do proprietário;

xx. Enviar mensagens objetivando acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;

xxi. Enviar mensagens que incluam imagens criptografadas ou de qualquer forma mascaradas (esteganografia);

xxii. Enviar mensagens com conteúdo considerado impróprio, obsceno ou ilegal;

xxiii. Enviar mensagens de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;

xxiv. Enviar mensagens que contenham perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;

xxv. Enviar mensagens que tenham fins políticos locais ou do país (propaganda política);

xxvi. Enviar mensagens que incluam material protegido por direitos autorais sem a permissão do detentor dos direitos;

xxvii. Evitar utilizar e-mail do CAP para assuntos pessoais.

4.9.1. Requisitos obrigatórios

As mensagens de correio eletrônico sempre deverão incluir assinatura com:

- Nome do empregado;
- Gerência ou departamento;
- Logo e nome do CAP;
- Telefone(s);
- E-mail;
- Site institucional – www.paulistano.org.br ;
- Endereço do CAP;
- Redes sociais oficiais;
- É expressamente proibido alterar a assinatura.

A padronização das assinaturas é realizada via sistema Code Two e os dados são inseridos no sistema pelo Departamento de TI;

4.10. DIRETRIZES QUANTO AO USO DA INTERNET

Todas as regras atuais do CAP visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos da informação. Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto o CAP, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos.

Segue as regras que devem ser observadas por todos os usuários quando da utilização da internet em dispositivos do CAP ou na utilização de dispositivos pessoais na rede do CAP:

i. Alguns sites (páginas da internet) contêm ou distribuem material não apropriado ao ambiente de trabalho, portanto, os usuários não devem acessar tais sites nem tampouco distribuir / obter material similar. Dessa forma, é proibido acessar locais virtuais (sites) que:

   - Possam violar direitos de autor, marcas, licenças de programas (softwares) ou patentes existentes.
   - Possuam conteúdo pornográfico, relacionado a sexo, exploração infantil ou ao crime de pedofilia.
   - Contenham informações que não colaborem para o alcance dos objetivos do CAP.
   - Defendam atividades ilegais.
   - Menosprezem, depreciem ou incitem o preconceito a determinadas classes como sexo, raça, orientação sexual, religião, nacionalidade, local de nascimento ou deficiência física.

ii. Os acessos a sites estão sendo monitorados, portanto, em caso de dúvida, deve-se verificar junto aos superiores imediatos ou o time de TI se o respectivo site pode ser acessado;

iii. Todo o conteúdo recebido ou enviado através da internet será automaticamente submetido a verificações de segurança para eliminação de vírus e tentativas de invasão da rede corporativa;

iv. É permitido o uso de serviços de mensagens (WhatsApp, Hangouts, Skype, Messenger etc.) desde que para fins profissionais. O uso pessoal desses aplicativos deve ser limitado e com bom-senso, nunca com finalidades conflitantes aos interesses do CAP, bem como nunca infringindo nenhuma lei, norma, regulamentação e políticas internas. Vale lembrar também que todas as comunicações feitas em computadores do CAP ficam armazenadas

e podem ser consultadas pelo CAP como determinam suas políticas, bem como que o compartilhamento de qualquer assunto referente ao CAP é expressamente proibido;

v. O CAP não se responsabilizará por problemas ocasionados em virtude do fornecimento de informações pessoais dos seus usuários na internet, tais como: números de cartão de crédito ou contas correntes bancárias e senhas para acesso a sistemas de internet banking;

vi. Novos recursos na internet, além do acesso à web e ao correio eletrônico, deverão ser liberados somente mediante prévia análise de riscos de segurança e comprovação da necessidade e/ou benefícios do serviço para o CAP;

vii. Os usuários não poderão utilizar os recursos do CAP para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores. O acesso a softwares peer-to-peer (Kazaa, BitTorrent e afins) não serão permitidos.

viii. O CAP, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer usuário, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao usuário e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos o CAP cooperará ativamente com as autoridades competentes.

4.11. USO DAS IMPRESSORAS

Seguem as regras que devem ser observadas por todos os usuários quando da utilização deste equipamento:

i. Quaisquer impressões, sobretudo as que contêm informações confidenciais, devem ser imediatamente retiradas da impressora;

ii. Esta ferramenta deve ser utilizada apenas quando o documento físico se fizer imprescindível, evitando desperdícios ou gastos desnecessários;

iii. As impressoras são ferramentas para fins profissionais, objetivando aumentar a produtividade nas atividades desenvolvidas pelo CAP. Impressões para finalidade pessoal devem ser limitadas e com bom-senso, nunca com finalidades conflitantes com os interesses do CAP, bem como nunca infringindo nenhuma lei, norma, regulamentação e políticas internas do CAP, e;

iv. Impressões coloridas apenas devem ser feitas apenas em caráter excepcional, quando a utilização da cor interferir na compreensão do documento ou quando a situação assim exigir;

v. Os relatórios impressos devem ser protegidos contra perda, reprodução e uso não autorizado.

4.12. MESA LIMPA

A política de mesa limpa consiste em não deixar informações confidenciais ou bens do CAP, incluindo, mas não se limitando a papéis, pen-drives ou quaisquer outros tipos de mídias removíveis, acessíveis a outras pessoas sem a devida proteção, quando o usuário estiver fora de sua estação de trabalho.

5. PRINCÍPIOS E DIRETRIZES

Os princípios básicos da Segurança da Informação são a confidencialidade, integridade e disponibilidade das informações. Outras características são a irrefutabilidade, a autenticação e o controle de acesso. Os benefícios evidentes são reduzir os riscos com vazamentos, fraudes, erros, uso indevido, sabotagens, roubo de informações e diversos outros problemas que possam comprometer esses princípios básicos. Dessa forma listamos abaixo algumas dicas e atitudes de segurança que esperamos de vocês.

5.1. ATITUDES PARA A SEGURANÇA DA INFORMAÇÃO

5.1.1. Controle de acesso

O controle de acesso é parte central da segurança do ponto de vista da segurança da informação. Por isso, é fundamental o uso diário do crachá nas instalações do CAP.

5.1.2. No ambiente externo, é melhor ficar atento

Falar sobre informações restritas em um lugar público ou por telefone merecem cuidado especial. Frequentemente, as pessoas são o elo mais fraco na segurança da informação de uma empresa.

Quando seu equipamento viajar com você, evite deixá-lo por muito tempo sozinho em uma sala ou mesa da empresa. Qualquer pendrive ou conexão de rede pode levar dados valiosos.

5.1.3. Cuidado com o lixo que você produz

O lixo pode ser uma fonte de informações para pessoas mal-intencionadas. Destrua os documentos que contenham informações sensíveis, pessoais ou do CAP antes de descartá-

los. Se o papel que vai ser jogado no lixo contém informações que não devem ser lidas por estranhos, rasgue-o antes de jogá-lo fora.

5.1.4. Cuidados com senhas de acessos no sistema

Cada tarefa desenvolvida em sistemas, deve e precisa ter um responsável. A única forma de saber o responsável por cada atividade é através da identificação do usuário.

Tudo que é feito com a sua identificação (assinatura ou senha) é de sua responsabilidade. Portanto, cuidado com seus dados, seja na rede ou nos sistemas, pois ela serve para garantir que você é realmente quem está usando esse acesso.

Se uma outra pessoa tem acesso a sua senha, ela poderá utilizá-la para se passar por você, porém, a responsabilidade por tudo que ela fizer será sua.

Alguns exemplos de ações que podem ser atribuídas a você, são:

- liberação de atendimentos indevidos;
- e-mails com informações inadequadas;
- acesso a páginas da internet proibidas;
- downloads proibidos.

Compartilhar sua senha é como assinar um cheque em branco.

Utilize senhas fortes, isto é, com mais de 8 caracteres, combinando numéricos e alfanuméricos, maiúsculas e minúsculas e não utilize datas comemorativas, sobrenomes, nome do cônjuge, nome dos filhos, placas de carro, etc. Não escreva a senha em local público ou de fácil acesso, como por exemplo, em sua agenda, em um pedaço de papel pregado no seu monitor ou guardado na sua gaveta. Utilize uma senha diferente para cada serviço. Sempre que suspeitar de perda de sigilo das suas senhas, altere-as imediatamente.

5.1.5. Pausa para o café

Apesar de saber que você é bastante cuidadoso, acidentes acontecem, e ao derramar café ou água em um documento ou no computador você poderá danificá-los.

Quanto às bolachas, os resíduos no teclado diminuem consideravelmente a vida útil do equipamento. A sujeira acumulada embaixo das teclas é difícil de limpar, portanto aproveite o momento do cafezinho, da água e da bolacha para esticar as pernas e fique longe dos computadores e papeis. Você pode até aproveitar para fazer um alongamento rápido.

Não esqueça de bloquear o computador nesses momentos de intervalo. Use o Ctrl+ALT+Del e você não perderá nada do que está fazendo (apenas a tela ficará protegida e sua senha deverá ser digitada novamente quando você voltar).

5.1.6. Uso de e-mails

Sua conta de e-mail foi criada para ser usada em atividades ligadas ao trabalho. Alguns cuidados são indispensáveis em sua utilização:

i. Não abra e-mails enviados por desconhecidos, principal - mente se eles contiverem arquivos anexados;

ii. Não responda mensagens de propaganda;

iii. Não repasse mensagens com notícias sensacionalistas, pedidos de ajuda, avisos devírus, textos de autoajuda e outras similares;

iv. Não cadastre seu endereço do CAP em listas de discussão, sites de compra ou similares;

v. Confirme se os destinatários estão corretos;

vi. Avalie a necessidade de enviar "com cópia";

vii. Verifique se é necessário o envio de mensagens encadeadas e o envio de anexos;

viii. Escreva textos claros, simples e objetivos;

ix. Não acredite em todos os e-mails sobre vírus, principal - mente aqueles de origens duvidosa, que mandam em anexo um arquivo para ser executado prometendo solucionar o problema. Verifique sua veracidade com a TI.

x. Atenção: o correio eletrônico deve ser usado apenas para assuntos relacionados com o CAP.

5.1.7. Fique atento a vírus

Os vírus são programas que se multiplicam e podem afetar o funcionamento de toda a rede, além de roubar sua senha ou apagar arquivos preciosos na sua máquina. Ao perceber que o computador que você usa foi infectado, desligue a máquina e comunique imediatamente ao Departamento de Tecnologia.

A melhor forma de combater os vírus é proceder da seguinte forma:

I. Verifique se o antivírus da máquina que você usa está liga - do (cor verde no canto inferior direito da tela) e mantenha-o atualizado;

II. Não abra e-mails e arquivos enviados por desconhecidos;

III. Não abra programas ou fotos que dizem oferecer prêmios;

IV. Cuidado com os e-mails falsos de bancos, lojas e cartões de crédito;

V. Jamais abra arquivos que terminem com PIF, SCR, BAT, VBS e, principalmente, os terminados com EXE e COM;

VI. Nunca acredite em pedidos de pagamento, correção de senhas ou solicitação de qualquer dado pessoal por e-mail. Comunique-se por telefone com a instituição que supostamente enviou a mensagem e confira o assunto;

VII. Se você desconfiar de um e-mail recebido, mesmo quando enviado por pessoa conhecida, não abra, pois pode ser falso. Entre em contato com o Departamento de Tecnologia.

5.1.8. Instalação de softwares

A instalação de softwares não autorizados pode colocar em risco toda a rede do CAP. Mesmo que seja para melhorar o seu desempenho no trabalho, solicite ao Departamento de Tecnologia a análise prévia do programa que você pretende instalar. O uso de cópias não autorizadas pode acarretar multa de 3 mil vezes o valor de sua licença. Dessa forma, até um simples descompactador pode sair muito caro.

5.1.9. Navegando na internet

Para acesso a internet, esteja atento aos seguintes requisitos:

I. Verifique se o endereço que está aparecendo em seu navegador é realmente o que você deseja acessar;

II. Antes de clicar em um link, veja na barra de status do navegador se o endereço de destino está de acordo com a sua descrição;

III. Não autorize a instalação de softwares de desconhecidos ou de sites estranhos;

IV. Confie em seus instintos. Se você desconfiar de um site, saia da página imediatamente;

V. Não clique em OK ou confirme sem entender a mensagem que está sendo confirmada. Na dúvida, ligue para o Departamento de Tecnologia;

VI. Use a internet somente para assuntos relacionados exclusivamente com o seu trabalho.

5.1.10. Adote um comportamento seguro

I. Não utilize ferramentas da empresa como "Notebook" ou "PC" para armazenar conteúdo particular como fotos ou textos;

II. Não baixe nem instale qualquer programa no PC sem ter autorização expressa do Departamento de Tecnologia;

III. Não compartilhe nem divulgue sua senha a terceiros;

IV. Não transporte informações confidenciais do CAP em qualquer meio (CD, DVD, disquete, pendrive, papel, etc.) sem as devidas autorizações e proteções;

V. Assuntos confidenciais de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas;

VI. Não abra mensagens de origem desconhecida nem utilize a internet para acessar sites de relacionamento e/ou salas de bate-papo;

VII. Armazene e proteja adequadamente documentos impressos e arquivos eletrônicos que contêm informações confidenciais;

VIII. Siga corretamente a política para uso de internet e correio eletrônico estabelecida pelo CAP.

6. RESPONSABILIDADES

6.1. SÃO DE RESPONSABILIDADE DO DEPARTAMENTO DE TERCNOLOGIA DA INFORMAÇÃO

I. Pela característica de seus privilégios, manter sigilo sobre suas informações e dados do CAP e dos usuários, restringindo-se a acessá-los somente quando forem necessários para execução das atividades operacionais sob sua responsabilidade;

II. Restringir a apenas ao necessário os poderes de cada usuário e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações;

III. Testar a eficácia dos controles e ferramentas de segurança utilizadas e informar aos Gestores das demais áreas sobre os riscos residuais;

IV. Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelo CAP;

V. Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências;

VI. Definir as regras formais para instalação de software e hardware, exigindo seu cumprimento dentro do CAP;

VII. Propor e apoiar inciativas que visem a segurança dos ativos de informações do CAP;

VIII. Garantir, no menor prazo possível, o bloqueio de acesso de usuários por motivo de desligamento, rescisão de contrato, incidente, investigação ou qualquer outra situação que exija medidas restritivas para fins de salvaguardar o CAP;

IX. Informar imediatamente ao Data Protection Officer – DPO sobre o incidente com vazamentos e segurança da informação;

X. Estabelecer as regras de proteção dos ativos do CAP;

XI. Decidir quanto às medidas a serem tomadas no caso de violação das regras estabelecidas;

XII. Revisar, pelo menos anualmente, as regras de proteção estabelecidas;

XIII. Restringir e controlar o acesso dos usuários remotos e externos;

XIV. Executar as regras de proteção estabelecidas por esta Política de Segurança da Informação – PSI;

XV. Detectar, identificar, registrar e comunicar as violações ou tentativas de acesso não autorizadas;

XVI. Definir e aplicar, para cada usuário de TI, restrições de acesso à rede, tais como horário autorizado, dias autorizados, entre outras;

XVII. Manter registros de atividades de usuários de TI (logs) por um período não inferior a 5 (cinco) anos. Os registros conterão a hora e a data das atividades, a identificação do usuário de TI, comandos (e seus argumentos) executados, identificação da estação local ou da estação remota que iniciou a conexão, número dos processos e condições de erro observadas (tentativas rejeitadas, erros de consistência etc.);

XVIII. Garantir o cumprimento do procedimento de backup para os servidores e Ativos, e;

XIX. Limitar o prazo de validade das contas de prestadores de serviço ao período da contratação.

7. DISPOSIÇÕES FINAIS

A presente Política passa a vigorar a partir de sua aprovação em reunião de Diretoria, por prazo indeterminado a partir da data de sua aprovação, devendo ser revisada a cada 3 (três) anos ou em um período inferior, sempre que necessário, de forma a garantir que seu teor esteja de acordo com as necessidades do CAP, substituindo quaisquer orientações, normas ou políticas anteriores sobre o tema, podendo ser extinta, alterada ou atualizada a qualquer momento por decisão do CAP.

8. REFERÊNCIAS E RASTREABLIDADE DO PROCESSO

CÓDIGO	TÍTULO
LEI N° 13.709/2018	LEI GERAL DE PROTEÇÃO DE DADOS

HISTÓRICO DE REVISÕES	EMISSÃO
000 – EMISSÃO INICIAL	30/09/2024
PRÓXIMA REVISÃO: 09/2027	

Eder do Lago Mendes Ferreira
Presidente