tecnologia a serviço da cidade
procempa

Política de Segurança da Informação

Dezembro 2020

Sumário

Apresentação

A Revolução Digital consolidada nas últimas décadas tornou possível um enorme avanço: a coleta, contabilização e processamento de quantidades significativas de dados do turbilhão de eventos que ocorrem todos os dias na sociedade. Hoje podemos extrair mais facilmente desses dados muitas informações que servem como farol orientador importantíssimo para tomada de decisões e identificação de oportunidades.

Considerando que os dados podem ser usados na tomada de decisões importantes, seu valor é reconhecido e deve ser preservado. O grande valor atrai grandes ameaças. Não devem cair nas mãos erradas. Adulterações e indisponibilidade podem levar a decisões erradas ou falta de ação.

Estas são as bases e justificativas para a Segurança da Informação, que visa a manutenção da Confidencialidade, Integridade e Disponibilidade das informações. E o instrumento importante para isso é a Política de Segurança da Informação, um conjunto de diretrizes, normas, procedimentos e padrões a serem observados e seguidos por todas as pessoas que utilizarem a infraestrutura da Companhia.

Diretrizes

Estes são os princípios básicos que regem a Política de Segurança da Procempa, estabelecidos de acordo com as necessidades da instituição.

1. À Procempa é atribuída a guarda de informações de seus clientes diretos e indiretos, fornecedores e empregados. Portanto, a criação de um ambiente que garanta a disponibilidade e proteção é essencial para a continuidade de negócio da Companhia.
2. Toda a informação deverá ser classificada formalmente quanto à sua confidencialidade, integridade e disponibilidade e ser tratada de acordo com a sua classificação, independente da sua forma de armazenamento, digital ou não.
3. Dados Pessoais e informações relacionadas a pessoa natural identificada ou identificável, devem obrigatoriamente ser protegidos de acordo com a Lei Geral de Proteção de Dados (LGPD) e tratados como confidenciais quando não houver justificativa legitima em contrário. Cuidados redobrados devem ser tomados em relação aos Dados Pessoais Sensíveis, aqueles que podem revelar origem racial, étnica, opinião política, convicção religiosa, filosófica, filiação sindical, dados genéticos ou biométricos, relacionados a saúde, vida sexual ou orientação sexual.
4. As informações devem ter o ciclo de vida programado. Informações consideradas confidenciais, quando não mais necessárias, devem ser destruídas através de mecanismos apropriados. O descarte ou reutilização de mídias contendo essas informações deve ser feito de forma a inviabilizar a recuperação das mesmas.
5. Todo o indivíduo que tenha acesso as dependências da Procempa deverá ser identificado. O acesso de terceiros em áreas onde exista o processamento físico ou digital de informações deverá ser fundamentado pela estrita necessidade e deverá ocorrer sempre com o acompanhamento de empregado da Companhia, responsável pelas informações naquele setor.
6. Todos os equipamentos na Companhia deverão estar inventariados e identificados de forma individual.
7. Credenciais de acesso as instalações e sistemas são pessoais, não compartilháveis e intransferíveis. O usuário é responsável por todas as atividades desenvolvidas mediante autenticação com sua credencial, por isso deve zelar por sua proteção e sigilo, e realizar as ações de manutenção apropriadas para cada tipo de credencial, como a troca periódica de senhas.
8. Alterações no ambiente de produção devem ser previamente estudadas, formalizadas por processo padronizado, comunicadas, autorizadas e, sempre que possível, testadas em ambiente apropriado e isolado, anteriormente à efetiva colocação dos recursos em produção, para verificação e avaliação dos impactos causados no processo produtivo, com o objetivo de garantir a estabilidade do ambiente..
9. Os empregados, durante a vigência e após o término do contrato de trabalho ou prestação de serviço, não podem se apropriar de informações ou de mídias, equipamentos, componentes ou acessórios que as contém, como por exemplo: e-mails corporativos, planilhas, arquivos de dados ou vídeos.
10. A responsabilidade de manter a segurança é compartilhada por todos os funcionários. A Procempa deverá ministrar treinamentos para promover a conscientização e preparo.

Normas

Violações das normas abaixo relacionadas, incidentes ou falhas de segurança devem ser notificadas imediatamente à equipe de Segurança da Informação da Procempa.

Se houver mera possibilidade de vazamento de Dados Pessoais, deve ser notificado também imediatamente o Encarregado de Processamento de Dados (DPO).

Segurança Física

1. Todo o indivíduo ao ingressar nas instalações da Procempa deverá usar crachá de identificação.
2. Pessoas externas à Companhia deverão ser identificadas na recepção e o seu ingresso nas instalações da Procempa será realizado mediante autorização e acompanhamento do empregado da Companhia.
3. Todo o equipamento que ingressar ou sair da Procempa, deverá estar acompanhado da respectiva nota fiscal e autorização do setor de Patrimônio.
4. Os prestadores de serviços da Procempa são responsáveis pelas ações ou prejuízos causados por seus empregados ao patrimônio da Procempa, bem como deverão garantir a manutenção da confidencialidade das informações acessadas.
5. Documentos ou papeis contendo informações confidenciais, quando não mais necessários, devem ser triturados ou destruídos de forma a impossibilitar leitura.
6. Mídias do tipo somente leitura (discos CD-ROM, CD-R, DVD, etc) contendo informações confidenciais, quando não mais necessárias, devem ser quebradas ou destruídas de forma a impedir seu uso indevido.
7. Mídias regraváveis (drives HD ou SSD, pen drives, cartões SD, fitas, discos CD ou DVD do tipo RW, ou assemelhados) contendo informações confidenciais, quando não mais necessárias, devem ser zeradas com o procedimento seguro adequado indicado pela equipe de Segurança da Informação antes de seu reuso ou descarte.
8. A entrega de documentos com informações confidenciais pode ocorrer apenas com registro e a garantia de identificação de quem recebe e mediante prévia assinatura de termo de confidencialidade.
9. Os equipamentos e seus componentes internos serão inventariados periodicamente e somente funcionários autorizados podem fazer remanejo de equipamentos e peças.

Credenciais

1. Credenciais, identificações e senhas de acesso devem ser individuais e mantidas em sigilo, não devem ser transferidas ou compartilhadas.
2. Cada funcionário deve trocar periodicamente suas senhas e é de sua responsabilidade escolher senhas robustas, complexas e longas.
3. As senhas devem ser únicas, não devem ser usadas senhas idênticas ou semelhantes para identificação em sistemas, sites ou serviços não gerenciados pela Procempa, sejam de natureza pessoal ou não.

Uso da Rede

1. O acesso a Internet é fornecido para atividades e finalidades da Companhia. Acessos com fins particulares lícitos podem ser feitos ocasionalmente, preferencialmente fora do horário de expediente, desde que não violem as demais normas.
2. É proibido usar a rede para acessar ou enviar conteúdo pornográfico, ofensivo ou difamatório, bem como para constranger terceiros, sejam eles funcionários ou não.
3. O uso para fins particulares de redes sociais como Facebook ou Twitter e sítios de vídeos como YouTube, Vimeo e Netflix durante o horário de expediente é considerado inadequado e pode estar bloqueado a qualquer horário a critério da Companhia.
4. Qualquer sítio conhecido de conteúdo vedado ou inadequado pode estar em listas de bloqueio automático. Eventuais erros na classificação de determinado sítio podem ser comunicados à equipe responsável pelos proxys para retificação.
5. Os acessos à Internet podem ser monitorados e registrados pela Companhia. Os registros ficam a disposição da Companhia pelo tempo que esta julgar adequado.
6. O compartilhamento de recursos nas estações de trabalho deve ser limitado a atividades de interesse da Companhia, com liberação somente para leitura por conjunto restrito de usuários.
7. Não é permitido instalar, usar ou configurar equipamentos (hardware ou software) que deem acesso à rede corporativa sem autorização formal e conhecimento da Equipe de Segurança da Informação. Em especial, não é permitida a instalação de ponto de acesso wifi, bluetooth, modem, hub, switch, vpn, roteador ou software de acesso remoto para fins pessoais.
8. Não é permitido copiar arquivos ou realizar acessos com fins particulares que onerem excessivamente a utilização da rede.
9. Todas as mensagens enviadas por correio eletrônico com o endereço profissional são de propriedade da Companhia, portanto devem ser usadas para assuntos de interesse da Procempa e não se deve manter qualquer expectativa de privacidade de seus conteúdos.
10. É vedado o envio ou participação em correntes, mesmo de solidariedade, premiações ou informações.
11. É vedado o envio de mensagens com conteúdo eleitoral, difamatório, ofensivo, preconceituoso, obsceno, pornográfico ou que dê margem a interpretação de discriminação racial, sexual, religiosa ou política.
12. Não é permitido distribuir, via correio eletrônico, grupos de discussão, fóruns e formas similares de comunicação mensagens não solicitadas do tipo “corrente” e mensagens em massa, comerciais, de propaganda política ou o envio de correio eletrônico não solicitado, SPAM.
13. Notebooks, laptops, tablets e outros equipamentos pessoais ou de terceiros não devem ser ligados diretamente na rede da Companhia sem autorização. Tais equipamentos podem ser conectados à rede wifi e ter acesso a serviços internos via VPN gerenciada pela Companhia.

Proteção de Estações

1. Em todas as estações de trabalho, notebooks e laptops deve estar instalado, ativo e atualizado o antivírus corporativo indicado pela equipe de administração do antivírus para o seu sistema operacional.
2. O usuário não deve impedir a operação e atualização do antivírus sem autorização e conhecimento da equipe de administração do antivírus.
3. Constatado qualquer problema com o antivírus, o usuário deverá comunicar aos responsáveis pela administração do antivírus que tomarão as providencias cabíveis.

Utilização de Programas

1. As estações de trabalho são disponibilizadas com os programas - sistema operacional e aplicativos - mínimos necessários para o desempenho de sua função básica.
2. São considerados legítimos os softwares instalados e utilizados conforme suas licenças de uso e que não contrariem as demais regras da Companhia e a legislação. Em especial, esta norma contempla a possibilidade de uso de software livre para fins legítimos e não abusivos.
3. Não é permitida a instalação nos equipamentos da Companhia de qualquer software, gratuito ou não, sem as devidas licenças para uso comercial da Companhia.
4. O uso ou instalação de software sem licença de uso ou em nome de outros sem autorização caracteriza crime de pirataria, ficando o usuário e o instalador sujeitos às sanções administrativas, legais e penais da legislação.
5. Ocasionalmente serão realizadas verificações no inventário dos equipamentos, com relação a hardware e software permitindo identificar desvios das normas.

Cópias de Segurança ou Backup

1. Cada usuário é responsável pela manutenção de cópias de segurança de seus arquivos de dados.
2. Arquivos gerados nas estações de trabalho que necessitem cópia de segurança deverão ser armazenados em servidor de arquivos apropriado da Companhia, desde que autorizado pelo supervisor. É responsabilidade do funcionário confirmar com a equipe de Backups que as pastas estão incluídas nas rotinas de cópias de segurança.
3. Não é permitida a cópia de dados confidenciais para processamento ou armazenamento em serviços externos, de terceiros não autorizados pela Companhia ou cliente.
4. Sempre que possível, os dados confidenciais devem estar criptografados nos backups.
5. O responsável pelo servidor deverá ativar processo de backup das informações críticas, incluindo serviços como correio eletrônico, banco de dados e aplicações.
6. Todo o backup deve periodicamente passar por teste de restauração.
7. Meios de armazenamento devem ser guardados em local seguro, armário, cofre ou sala com chave ou controle de acesso e devem ser respeitados os tempos de vida útil sugeridos pelo fabricante.

8. Alguns backups tem tempo de vida determinado por lei, portanto a equipe responsável pelos backups deve ser informada e zelar por mantê-los disponíveis durante esse tempo, bem como os equipamentos necessários para sua recuperação quando necessário.

Sistemas e Aplicações

1. Não é permitida a transferência de dados para processamento ou armazenamento em serviços externos, de terceiros não autorizados expressamente pela Companhia ou cliente.
2. Armazenamento e transferências de dados confidenciais devem ser sempre criptografadas com mecanismos aprovados pela Companhia.
3. Os sistemas deverão gerar registros (logs) de eventos de segurança. Devem ser utilizados para este fim funções do Sistema de Segurança em uso, recursos do sistema operacional, recursos de banco de dados e/ou recursos da aplicação. Os registros deverão conter ao menos as seguintes informações: identificação da aplicação e função, momento da ocorrência (timestamp), informações que identifiquem a máquina ou local da ocorrência e os dados relevantes manipulados pela aplicação. O Sistema de Segurança poderá se encarregar do registro de algumas dessas informações. Informações confidenciais não devem ser registradas em log sem estarem criptografadas.
4. No desenvolvimento e manutenção de sistemas é obrigatório o uso de software e repositório de controle e versionamento de arquivos (como fontes, modelos, documentos, diagramas, páginas web) aprovado pela Companhia.
5. Cada desenvolvedor é responsável pela integridade dos arquivos de sistema que estão sendo trabalhados, devendo utilizar preferencialmente áreas de trabalho em servidores designados. Caso estejam residentes em sua máquina, o desenvolvedor deve providenciar cópia de segurança (backup) dos mesmos, quando necessária.
6. Todo o desenvolvedor de aplicações deverá seguir, quando disponíveis e forem aplicáveis, as recomendações de segurança para o desenvolvimento.

Administração de Servidores

1. Todas as instalações de novos servidores deverão seguir procedimentos padrões e incluir pacotes, Service Packs, Hot Fixes obrigatórios.
2. Após sua instalação o responsável deverá encaminhar à Equipe de Segurança solicitação para verificação complementar do servidor.
3. A instalação das atualizações de segurança deverá ser realizada pelo responsável direto de cada servidor, seguindo as orientações de segurança no que tange ao backup antes do procedimento, adequação de horário e plano de recuperação de falhas;
4. Acessos remotos devem ser feitos sempre usando mecanismos criptografados. Devem ser desativados os serviços de acesso remoto que não usam criptografia, tais como TELNET, FTP e VNCSERVER;
5. Os equipamentos utilizados devem possuir sistema operacional atualizado e com recursos de segurança.

7. A ativação de novos serviços de rede será condicionada a uma análise de riscos (a ser realizada pela Equipe de Segurança), onde, no mínimo, os seguintes aspectos serão considerados: requisitos de segurança do serviço, objetivo, alvo do serviço, forma de acesso, forma da administração e volume de tráfego.
8. Não é permitida a instalação de serviços de rede não autorizados pela Equipe de Segurança.
9. Todo o tráfego de informações confidenciais por meio compartilhado será protegido através de criptografia.
10. Sistemas de proteção de acesso (firewall) devem ser utilizados para permitir apenas às redes ou máquinas alvo dos serviços o acesso aos mesmos mediante solicitação para a equipe de Segurança.
11. A equipe de Segurança da Informação pode indicar e usar ferramentas de detecção e prevenção de intrusos, para emitir alertas e registrar possíveis tentativas de invasão.

Registros e Auditoria

1. Os administradores devem habilitar registros de segurança (logs), de forma a auxiliar no tratamento de desvios, recuperação de falhas, contabilização e auditorias;
2. Os registros de segurança deverão ser analisados periodicamente (manual ou automaticamente).

Documentação Exigida

1. É fortemente recomendado que sistemas críticos tenham documentado Plano de Continuidade de Negócio ou Recuperação de Desastre.
2. Todas as instalações e atualizações deverão ser documentadas pelo responsável, administrador ou desenvolvedor, inclusive:
    - Procedimentos para instalação;
    - Correções instaladas (service packs, hot fixes, patches);
    - Softwares instalados/atualizados;
    - Configurações a serem realizadas;
    - Permissões de acesso;
    - Contatos para suporte;
    - Informações Complementares.

Segurança Física de Servidores

1. O acesso físico aos servidores e equipamentos de infraestrutura deve ser restrito aos empregados e terceiros autorizados.
2. Os servidores e equipamentos de infraestrutura devem operar em ambiente adequado, sob condições (temperatura, nível de poeira, umidade, etc) indicadas pelo fabricante.