Política de Segurança da Informação

Aprovação
Comitê Gestor de Segurança da Informação – CGSI dia 20/10/2020
Diretoria Colegiada dia 29/10/2020 - ATA 084/2020

Índice

1 Apresentação

A informação constitui um ativo valioso e de extrema importância para a preservação de uma empresa e necessita ser convenientemente protegida, independentemente de sua natureza ou de sua origem.

Segurança da Informação consiste na adoção de medidas para proteção da informação das diversas ameaças com a finalidade atingir os seguintes objetivos:

- **Confidencialidade:** garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas;
- **Integridade:** garantir que as informações sejam mantidas íntegras, sem modificações indevidas - acidentais ou propositais;
- **Disponibilidade:** garantir que as informações estejam disponíveis a todas as pessoas autorizadas a tratá-las;
- **Autenticidade:** confirmar a identidade de quem se diz ser.

Esta política apresenta diretrizes para orientar as ações para iniciar, implementar, manter e melhorar a gestão da segurança da informação de maneira a promover a criação de alicerces para a proteção da informação.

A Política de Segurança da Informação é uma declaração formal acerca do compromisso com a proteção, controle e monitoramento das informações processadas, armazenadas, transmitidas ou custodiadas, de sua propriedade e/ou sob sua guarda.

As diretrizes apresentadas nesta Política foram baseadas nas recomendações das publicações da família de normas NBR ISO/IEC 27000.

2 Objetivo

O objetivo desta Política de Segurança da Informação é orientar as ações e procedimentos que viabilizem a disponibilidade, integridade, confidencialidade

e autenticidade das informações críticas, a fim de garantir a continuidade e competitividade do negócio.

3 Abrangência e Divulgação

Todos os dirigentes, empregados, servidores, colaboradores, estagiários, prestadores de serviços e visitantes da empresa.

4 Conceituação e Definições

Acordo de Confidencialidade - Cláusula ou instrumento contratual que contém responsabilidades, direitos e deveres dos empregados, prestadores e prospectores de serviços, tais como de leis de direito autorais ou de proteção de dados, bem como a extensão da responsabilidade para fora das dependências da organização e após a rescisão do vínculo contratual.

Análise de Risco - Processo que envolve a consideração detalhada das incertezas, dos eventos, das causas e das consequências, a fim de se determinar as probabilidades dos riscos se tornarem reais e os impactos decorrentes.

Arquivo de *log* - Registro detalhado de todas as transações efetuadas durante a utilização de um aplicativo e necessário ao rastreamento do seu uso.

Ativo - Patrimônio composto por bens e direitos da empresa.

Ativo Tecnológico - Equipamentos ou programas de computador que suportam o ambiente organizacional e de negócios da empresa.

Colaborador - Empregado ou pessoa que presta serviços à empresa, sejam através de Contrato Individual de Trabalho, ou por vínculo a um Contrato de Prestação de Serviço.

Disponibilidade - Diz respeito à garantia de que a informação estará acessível às pessoas, processos automatizados, órgãos ou entidades no momento que

for requerida. Logo a disponibilidade está relacionada à prestação continuada de um serviço, sem interrupções no fornecimento de informações.

Integridade - A integridade da informação está relacionada à sua fidedignidade. Assegurar a integridade da informação, portanto, significa garantir que a informação não foi modificada ou destruída de maneira não autorizada, quer de forma acidental ou intencional.

Confidencialidade - Implica em impedir o acesso não autorizado, quer acidental quer intencional, garantindo que apenas pessoas, sistemas, órgãos ou entidades devidamente autorizados e credenciados tenham acesso à informação.

Autenticidade - Mediante a autenticação é possível confirmar a identidade de quem presta a informação. Ou seja, a autenticação permite assegurar a fidedignidade da fonte da informação.

Perímetro - Área física ou lógica da empresa onde são aplicadas proteções contra acessos indevidos.

Risco - É o efeito da incerteza nos objetivos.

Computação em nuvem (*Cloud Computing*) - Modelo de negócio que disponibiliza (compartilha) recursos computacionais e serviços sob demanda, os recursos são configuráveis pelo próprio cliente, de acordo com a sua necessidade, e cobrados apenas pelo que foi consumido. A computação na nuvem oferece escalabilidade e mecanismos de gestão dos serviços.

Conformidade - aderência a um padrão previamente estabelecido e aceito como ideal.

Backup - Cópia de segurança gerada para possibilitar o acesso ou recuperação futura de dados existentes no Data Center. O termo também pode ser associado ao processo de geração da cópia de segurança, acepção que tem no *restore* seu complemento. (vide *restore*).

Dispositivos móveis - qualquer equipamento ou acessório portátil, capaz de se conectar à *internet* e/ou armazenar dados, tais como: celular, *smartphone*, *tablet*, *notebook*, *netbook*, mp4, *pendrive*, CD/DVD e outros semelhantes.

Restore - É a ação de recuperar os dados armazenados em determinado dispositivo durante a rotina de *backup*, garantindo que todas as informações gravadas estejam intactas.

Sistema de Gestão da Segurança da Informação (SGSI) - É um sistema de gestão corporativo voltado para a Segurança da Informação, que inclui toda a abordagem organizacional usada para proteger a informação empresarial e seus critérios de Confidencialidade, Integridade e Disponibilidade. O SGSI inclui estratégias, planos, políticas, medidas, controles, e diversos instrumentos usados para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação.

Logs – Em computação, *log* de dado é uma expressão utilizada para descrever o processo de registro de eventos relevantes em um sistema computacional. Esse registro pode ser utilizado para restabelecer o estado original de um sistema ou para que um administrador conheça o seu comportamento no passado. Um arquivo de *log* pode ser utilizado para auditoria e diagnóstico de problemas em sistemas computacionais.

5 Estrutura Normativa da Segurança da Informação

Deve ser estabelecido um sistema normativo capaz de fazer a gestão das normas da empresa. O sistema deve permitir o armazenamento, consulta e impressão das normas. Além disso, deverá ser implementado um controle de versão e histórico das revisões.

Normas Básicas:

- Acesso à *Internet*;
- Uso Seguro de Redes Sociais;
- Acesso ao Correio Eletrônico;
- *Backup* e Recuperação de Dados;
- Gestão de Ativos;
- Proteção de Código Maliciosos;

- Segurança Física;
- Controle de Acesso Lógico; e
- Uso Dispositivos Móveis.

Normas Adicionais:

- Classificação de Informações;
- Aquisição, Desenvolvimento e Manutenção de Aplicações;
- Gerenciamento de Incidentes;
- Gerenciamento de Riscos;
- Gerenciamento de Continuidade de Negócios;
- Gerenciamento de Mudanças;
- Intercâmbio de Informações;
- Segurança em Terceirização e Prestação de Serviços; e
- Uso da Computação em Nuvem.

6 Declaração de Comprometimento da Direção

A Alta Direção deve aprovar a Política de Segurança da Informação e providenciar sua divulgação, tornando público para toda a empresa o seu comprometimento com a segurança da informação através de veículo de comunicação oficial.

7 Responsabilidades Mínimas pela Segurança da Informação

7.1 Comitê Gestor de Segurança da Informação (CGSI)

O Comitê Gestor de Segurança da Informação (CGSI) é um grupo multidisciplinar que reúne representantes de diversas áreas da empresa,

indicados pelas suas respectivas Gerências e com composição aprovada pela Diretoria, com o intuito de definir e apoiar estratégias necessárias à implantação e manutenção do SGSI.

Compete ao CGSI:

- Propor ajustes, aprimoramentos e modificações na estrutura normativa do SGSI, submetendo à aprovação da Diretoria;
- Redigir o texto das normas e procedimentos de Segurança da Informação, submetendo à aprovação da Diretoria;
- Requisitar informações das demais áreas do CIASC, através das diretorias, gerências e supervisões, com o intuito de verificar o cumprimento da Política, das Normas e Procedimentos de Segurança da Informação;
- Receber, documentar e analisar casos de violação da Política e das Normas e Procedimentos de Segurança da Informação;
- Estabelecer mecanismos de registro e controle de eventos e incidentes de Segurança da Informação, bem como, de não conformidades com a Política, as Normas ou os Procedimentos de Segurança da Informação;
- Notificar as gerências e diretorias quanto a casos de violação da Política e das Normas e Procedimentos de Segurança da Informação;
- Receber sugestões dos gestores da informação para implantação de Normas e Procedimentos de Segurança da Informação;
- Propor projetos e iniciativas relacionadas à melhoria da segurança da informação;
- Acompanhar o andamento dos projetos e iniciativas relacionados à segurança da informação;
- Propor a relação de gestores da informação;
- Monitorar, sistematicamente, a gestão dos ativos da informação;

- Orientar a atualização dos Planos de Continuidade dos Negócios, demandando junto às diversas áreas da empresa e validando-os em intervalos definidos; e
- Orientar e organizar, sistematicamente, a gestão de riscos relacionados à segurança da informação.

7.2 Coordenadoria de Segurança da Informação (COSEI)

Cabe à COSEI:

- Promover a implementação das diretrizes da segurança da informação no âmbito CIASC aprovadas pelo CGSI;
- Implementar e controlar políticas de segurança e controles de acesso lógico;
- Interagir com outros setores da empresa de modo a fomentar a segurança da informação;
- Implementar ferramentas para permitir gerenciamento de rede;
- Implementar e administrar soluções de segurança de rede;
- Identificar, analisar e gerenciar fluxos de tráfego de rede;
- Analisar o desempenho e capacidade de redes;
- Notificar incidentes de segurança da informação, aos responsáveis;
- Indicar treinamentos relativos à segurança da informação;
- Identificar, avaliar e tratar os riscos inerentes às atividades da área de redes;
- Estruturar e manter os controles internos da área de redes; e
- Planejar, coordenar e/ou executar outras atividades correlatas ou quando determinado pela Gerência de Redes.

7.3 Coordenadoria Administrativa (CORAD)

Cabe à CORAD:

- Promover a implementação das diretrizes da segurança da informação no âmbito CIASC aprovadas pelo CGSI;
- Implementar controles de acessos físicos;
- Implementar barreiras físicas para impedir acessos não autorizados;
- Cadastrar e Controlar acessos de visitantes; e
- Coordenar a vigilância Patrimonial.

7.4 Diretoria Executiva

Cabe à Diretoria Executiva:

- Nomear o Representante da Direção para a Proteção de Dados (DPO – *Data Protection Officer*, ou Encarregado de Dados);
- Aprovar a Política e as Normas de Segurança da Informação e suas revisões;
- Aprovar a composição do CGSI;
- Nomear os gestores da informação, conforme as indicações do CGSI; e
- Receber, por intermédio do CGSI, relatórios de violações da política e das normas de segurança da informação, quando aplicável.

7.5 Gestão Operacional de Segurança da Informação:

Cabe às áreas subordinadas à VPT:

- Gerenciar a plataforma de prevenção, detecção e reação a incidentes de segurança;
- Tratar incidentes lógicos de segurança da informação;
- Avaliar vulnerabilidades;

- Implementar mecanismos de proteção (segurança lógica) nas plataformas tecnológicas (Banco de Dados, Sistema Operacional, Rede, armazenamento, etc.) sob a sua responsabilidade;
- Monitorar os serviços de proteção;
- Garantir a implantação de segurança no processo e no código dos sistemas desenvolvidos;
- Implantar mecanismos de segurança lógica e física; e
- Reportar a ocorrência de incidentes e não conformidades de Segurança da Informação à COSEI.

7.6 Gestão de Negócios

Cabe à GECOM:

- Fornecer as diretrizes estratégicas do negócio para orientar as atividades de Segurança da Informação referentes a contratos com clientes;
- Garantir a inclusão de cláusulas contratuais com requisitos relacionados à privacidade e segurança; e
- Reportar a ocorrência de incidentes e não conformidades de Segurança da Informação à área de TIC dos Clientes.

7.7 Gestão de Recursos Humanos (GEREH)

Cabe à GEREH:

- Informar aos responsáveis pelo gerenciamento das credenciais sobre as mudanças nos acessos dos colaboradores em caso de alterações de função ou demissão;
- Indicar necessidade de capacitação em segurança de novos colaboradores; e

- Reportar a ocorrência de incidentes e não conformidades de Segurança da Informação à COSEI.

7.8 Proprietário da Informação

Cabe ao Proprietário da Informação:

- Determinar o nível de relevância e classificação correta das informações utilizadas nos ativos sob sua responsabilidade, de forma a subsidiar as decisões de classificação a serem aplicadas; e
- Reportar a ocorrência de incidentes e não conformidades de Segurança da Informação à COSEI.

7.9 Usuários Internos e Externos

Cabe aos empregados, estagiários, aprendizes e prestadores de serviços do CIASC cumprir com as seguintes obrigações:

- Zelar continuamente pela proteção das informações da organização ou de seus clientes contra acesso, modificação, destruição ou divulgação não autorizada;
- Assegurar que os recursos (computacionais ou não) colocados à sua disposição sejam utilizados apenas para as finalidades estatutárias da organização;
- Garantir que os sistemas e informações sob sua responsabilidade estejam adequadamente protegidos;
- Garantir a continuidade do processamento das informações críticas para os negócios do CIASC;
- Cumprir as leis e normas que regulamentam os aspectos de propriedade intelectual;
- Atender às leis que regulamentam as atividades da organização e seu mercado de atuação;

- Selecionar de maneira coerente os mecanismos de segurança da informação, balanceando fatores de risco, tecnologia e custo; e
- Comunicar imediatamente à COSEI qualquer descumprimento da Política de Segurança da Informação e/ou das Normas de Segurança da Informação.

8 Diretrizes

8.1 Gestão de Ativos

8.1.1 Responsabilidade pelos Ativos

Deve ser definido um proprietário e responsabilidades para proteção dos ativos de informação. O proprietário do ativo, ou custodiante da informação, deve gerenciar os ativos durante todo o do seu ciclo de vida, que compreende: criação, processamento, movimentação, armazenamento e descarte.

8.1.2 Classificação da Informação

Toda informação armazenada ou mantida pela empresa deve ser classificada de acordo com o seu valor, requisitos legais, sensibilidade e criticidade. Definir regras para que os ativos de tecnologia da informação sejam devidamente identificados, inventariados e classificados em função de sua relevância para o processo de negócio a que se destinam.

A guarda, disponibilização, circulação e descarte das informações, devem ser disciplinados por procedimentos, formalmente estabelecidos.

8.1.3 Leis Aplicáveis na Gestão de Ativos

Normas e procedimentos adicionais devem ser elaborados para atender aos requisitos legais da Lei de Acesso Informação (LAI), Lei nº 12.527 de 18 de novembro de 2011, do Marco Civil da *Internet*, Lei nº 12.965, de 23 de abril de

2014 e Lei Geral de Proteção de Dados Pessoais (LPGD), Lei nº 13.709 de 14 de Agosto de 2018.

8.1.4 Política de *Backup*

Devem ser estabelecidos regras e procedimentos para as atividades de *backup*, armazenamento e recuperação de dados. A política de *backup* deve prever o local e a forma de armazenamento, o tempo de retenção, mecanismos de teste de recuperação dos dados, meios para o descarte seguro das mídias do *backup*, dentre outros.

8.2 Segurança em Recursos Humanos

8.2.1 Antes da Contratação

Prever em Edital público e em cláusula contratual, uma seleção criteriosa, especificando a obrigatoriedade da apresentação de cópias de certidões negativas de registros civis, criminais, e assinatura de termo de sigilo.

Realizar avaliação de perfil com a finalidade de detectar incompatibilidades ao cargo proposto e suas atividades.

Toda contratação deverá em seus termos de responsabilidade, contemplar a proteção ao conhecimento sensível através de acordos de confidencialidade, inclusive com as prestadoras de serviços, devendo especificar também os direitos e deveres que o contratado terá referente às informações, assim como à segurança destas.

8.2.2 Durante a Contratação

Deverão ser definidos os requisitos de segurança necessários para exercer cargos e funções de natureza sensível na empresa, assim como, o grau de sensibilidade dos cargos e das funções existentes, no intuito de identificar

formalmente aqueles que, em razão de suas atribuições, tarefas e responsabilidades, possam acessar informações de conhecimento sensível.

As credenciais de acesso, só deverão ser entregues ao(s) contratado(s) quando todos os documentos que descrevem as responsabilidades forem assinados.

Caso a atividade a ser desenvolvida implique a custódia de ativos, estes, assim como as credenciais de acesso, só deverão ser fornecidos após a assinatura de toda documentação pertinente.

8.2.3 Encerramento e Mudança na Contratação

Estes processos deverão contemplar a comunicação com o(s) responsável(is) pelo gerenciamento das credenciais de acesso, objetivando que estas estejam em conformidade com os processos:

- Normatizar procedimentos de desligamento, de forma a interromper o acesso e a vinculação da empresa ao colaborador desligado bem como o procedimento de devolução de ativos sob custódia do(s) contratado(s);
- Realizar a entrevista de desligamento objetivando detectar o grau de satisfação dos colaboradores com a empresa e lembrar a estes da permanência do sigilo de informações as quais tinham acesso durante o vínculo empregatício.

8.2.4 Termo de Confidencialidade e Sigilo

Todos os colaboradores da empresa devem assinar o Acordo de Confidencialidade.

8.3 Controle de Acesso Lógico

8.3.1 Acesso à Rede, Sistema Operacional e Aplicações

O acesso aos recursos computacionais deve ser individual, pessoal e intransferível.

O usuário é responsável pela guarda de sua senha e pelo acesso aos recursos computacionais realizados através da sua credencial de acesso.

O controle de acesso lógico deve ser composto de processos para autenticação, autorização e auditoria.

O acesso lógico à rede deve ser controlado de forma centralizada através de procedimentos formais a partir do perfil de cada usuário, no qual estará definido seu nível de autorização.

Todo serviço de rede não autorizado deve ser bloqueado ou desabilitado.

Todas as transações em rede devem, obrigatoriamente, estar protegidas através de mecanismos de segurança.

O acesso a sistemas e aplicações deve sempre ocorrer através de um procedimento seguro de acesso ao sistema (*login*), projetado para minimizar oportunidades de acessos não autorizados.

O acesso aos ativos deve estar estritamente vinculado à execução do trabalho de cada usuário, e deve ser concedido em conformidade ao princípio do privilégio mínimo.

8.3.2 Uso de Dispositivos Móveis

A política de uso de dispositivos móveis na empresa deve ser regulamentada através de normas e procedimento de segurança. Todo dispositivo móvel somente poderá ser utilizado para acessar à rede e/ou recursos computacionais, caso ofereça suporte para autenticação, mínima de usuário e senha. Procedimentos adicionais devem ser elaborados para assegurar a gestão e monitoramento destes equipamentos.

8.3.3 Trabalho Remoto

Estabelecer norma e procedimento quanto ao uso, gestão, responsabilidades e controle dos acessos efetuados por usuários (internos, clientes e empresas externas), fora das instalações físicas da empresa, para uso da sua rede, sendo chamado de trabalho remoto.

8.3.4 Política de *Logging*

Adotar solução de análise e gestão de *LOGs* que permita a geração de relatórios e emissão automática de alertas de eventos que possam representar riscos para a segurança da infraestrutura tecnológica e dos sistemas de informação.

8.4 Criptografia

8.4.1 Gestão de Chaves Criptográficas

Definir um processo formal para proteger chaves criptográficas, contemplando requisitos referentes ao gerenciamento ao longo de todo o seu ciclo de vida incluindo a geração, a armazenagem, o arquivo, a recuperação, a distribuição, a retirada e a destruição das chaves considerando a geração de registro e auditoria das atividades relacionadas com o gerenciamento destas.

8.5 Segurança Física e do Ambiente

8.5.1 Entrada e Saída de Pessoas

A movimentação de pessoal nos ambientes da empresa deve ser registrada e monitorada, pois caso ocorra incidentes de segurança estes instrumentos poderão ser utilizados para auxiliar na investigação e resolução.

Uma prática comum é utilizar a recepção do ambiente como ponto de registro desta movimentação. Para o monitoramento, poderá ser integrado ao papel do

vigilante a utilização do sistema de vigilância com câmeras de segurança, acompanhando assim a movimentação de pessoal dentro da empresa.

Outro método de proteção às informações é o acompanhamento de visitantes durante o período em que estes permanecem dentro da empresa, pretendendo-se assim evitar que estes visitantes circulem em locais restritos.

8.5.2 Entrada e Saída de Equipamentos

É extremamente importante o registro da tramitação de equipamentos dentro de instituições públicas, uma vez que estes fazem parte do patrimônio do Estado.

Para a segurança das informações, além dessa tramitação, deverão ser registradas informações pertinentes a quem é o proprietário do patrimônio, quem é o responsável por este, e com quem está a sua custodia.

8.5.3 Proteção do Prédio, Equipamentos e Infraestrutura

A proteção da infraestrutura é bastante variável uma vez que diferentes localidades apresentam diferentes requisitos. Por exemplo, ambientes que estão construídos em cidades vulneráveis a catástrofes naturais, deverão tomar cuidados especializados para aquela localidade.

Nos equipamentos, os fabricantes costumam disponibilizar no manual informações pertinentes a proteção física, cabendo assim ao proprietário implementá-las.

Já para a proteção contra ameaças externas vindas do homem, as soluções são mais comuns, visto a diversidade de empresas especializadas neste tipo de proteção, assim a diminuição e até a mitigação da ocorrência destes tipos de incidentes são facilmente solucionadas.

Câmeras de monitoramento por CFTV também são utilizadas para controle de movimentação e para auxiliar na investigação e resolução de problemas envolvendo equipamentos.

8.6 Gerenciamento das Operações

8.6.1 Responsabilidades e Documentação dos Procedimentos de Operação

Os procedimentos operacionais da empresa representam a forma com que são desenvolvidas as atividades da mesma, assim objetivando manter a disponibilidade, integridade e qualidade na execução das tarefas. Documentar estes procedimentos é uma atividade de extrema importância para a empresa.

Estes procedimentos documentados permitem que na ausência do responsável pela execução do procedimento, outro colaborador possa reproduzir a tarefa documentada mantendo assim a disponibilidade da mesma. Além disso, a integridade também é garantida uma vez que ficam descritos os passos necessários para executar a atividade.

É notório que com a manutenção da disponibilidade e integridade do procedimento a empresa atingirá níveis de qualidade nos serviços prestados, já que independente da pessoa que execute o procedimento, o resultado será o mesmo.

No documento que descreve o procedimento, as responsabilidades de quem venha a executá-lo também deverão estar disponíveis, pois facilitará assim a ciência destes por parte do executor.

É importante implantar procedimentos para a Gestão de Mudanças e da Capacidade visando a minimizar os riscos de indisponibilidade.

8.7 Comunicação Segura

8.7.1 Segurança dos Serviços de Rede

Definir requisitos técnicos e procedimentos para implementação do conceito de segurança do tráfego de rede, através da segregação das redes em VLANS, separação dos ambientes computacionais, de acordo com a sua característica e finalidade: desenvolvimento, homologação, testes e produção, além da implementação de recursos de controle de acesso seguro por funcionalidade e monitoramento da rede, para viabilizar a rastreabilidade e auditorias. Adotar

controles e mecanismos de gerenciamento dos serviços de rede em todos os níveis.

8.7.2 Transferência de Informações

Definir as regras e procedimentos de segurança para troca de informações e *softwares* internamente, entre os órgãos e entidades da Administração Pública do Poder Executivo Estadual e/ou com quaisquer entidades externas.

8.8 Aquisição, Desenvolvimento e Manutenção de Sistema da Informação

8.8.1 Requisitos de Segurança de Sistemas da Informação

Garantir que requisitos relacionados com segurança da informação sejam incluídos entre os requisitos para novos sistemas de informação ou melhorias dos sistemas de informação existentes.

Incorporar atividades de segurança no desenvolvimento de sistemas para proteger informações e processos de negócio.

Definir documento ou *framework* para orientar a segurança no desenvolvimento de sistemas e para ser usado como referência no processo de desenvolvimento de sistemas.

Requisitos de segurança devem ser compatíveis com o nível de segurança exigido pelas regras de negócio.

Considerar a proteção em camadas: Segurança da interface do usuário, Segurança da aplicação, Segurança do sistema operacional e Proteção de redes.

8.8.2 Processamento Correto nas Aplicações

Dispor de ambientes segregados para desenvolvimento, homologação, testes e produção de sistemas, para reduzir as oportunidades de uso e modificações indevidas, não autorizadas.

O acesso ao ambiente de Produção deve ser restrito para evitar comprometimento da integridade das informações.

8.8.3 Segurança no Processo de Desenvolvimento e Suporte

Utilizar Metodologia de Desenvolvimento de Sistemas formal que contemple as fases de Concepção, Elaboração, Transição, Operação e Manutenção e desativação para orientar as atividades do desenvolvimento de Sistemas de Informação em todo o seu ciclo de vida.

Contemplar na Metodologia de Desenvolvimento de Sistemas, desde a fase inicial, etapas que apresentem orientações e remetam para verificações e testes de segurança.

A metodologia utilizada para o desenvolvimento de sistemas deve conter atividades e tarefas relativas à segurança da informação no ciclo de vida desenvolvimento do sistema.

É recomendável existir um manual com recomendações para a construção de códigos seguros.

8.8.4 Gestão de Vulnerabilidades Técnicas

Contemplar na Metodologia de Desenvolvimento de Sistemas atividades que identifiquem antecipadamente vulnerabilidades que possam ser eliminadas antes da implantação do sistema em produção.

8.8.5 Testes

Os requisitos de segurança devem ser testados de forma rigorosa por equipe que não esteve envolvida diretamente no desenvolvimento da aplicação.

8.9 Relacionamento com o Fornecedor

8.9.1 Termo de Sigilo do Fornecedor

Todos os colaboradores da empresa envolvidos com a contratação devem assinar o Acordo de Confidencialidade. No caso dos prestadores de serviço, o sigilo deve ser também observado em cláusulas contratuais.

8.9.2 Cláusulas de Segurança na Contratação

Os contratos devem prever os requisitos de segurança pertinentes, regras de conduta internas e externas, responsabilidades das partes durante a execução do contrato e as penalidades aplicáveis em caso de não cumprimento de cláusulas relativas à segurança da informação.

8.9.3 *Cloud Computing* (Computação na Nuvem)

A contratação de serviço em nuvem deve atender aos requisitos da política de segurança da empresa e às normas e legislação brasileiras quanto a confidencialidade e propriedade, localização dos dados armazenados, estes não podem sair do território nacional. A empresa contratada deve assegurar que segue os padrões das normas nacionais e internacionais de segurança em computação na nuvem, através de certificações emitidas por estas entidades.

8.9.4 Gerenciamento de Serviços Terceirizados

Estabelecer diretrizes para implementar e manter o nível apropriado de segurança da informação e de entrega de serviços nos acordos firmados entre a empresa e terceiros.

Os contratos devem prever os requisitos de segurança pertinentes, regras de conduta internas e externas, responsabilidades das partes durante a execução do contrato, acordo de nível de serviço (SLA), e as penalidades aplicáveis em caso de não cumprimento de cláusulas relativas à segurança da informação.

8.10 Gestão de Mudanças

Um processo de gerenciamento de mudanças deve ser estabelecido e implementado a fim de garantir que modificações em recursos de Tecnologia da Informação sejam processadas, levando-se em consideração o grau de importância dos sistemas e processos de negócio envolvidos.

8.11 Gestão de Incidentes de Segurança da Informação

Um processo de gerenciamento de incidentes deve ser estabelecido e implementado. Procedimentos de segurança devem ser elaborados para registro, classificação e tratamento de incidentes de segurança da informação.

8.12 Orientações ao Usuário Final

8.12.1 Uso Aceitável dos Ativos

Estabelecer as diretrizes e responsabilidades para o acesso aos recursos de Tecnologia da Informação disponibilizados pela empresa.

8.12.2 Mesa Limpa e Tela Limpa

Adotar procedimentos de “mesa limpa” ao final do expediente e instalação de armários com dispositivos de segurança para armazenamento de informações sensíveis.

8.12.3 Transferência de Informações

Definir regras e procedimentos para acondicionamento, envio e recebimento de documentos sensíveis em meios físicos e em meios digitais.

8.12.4 Acesso à *Internet* e a Redes Sociais

Estabelecer as diretrizes de proteção relativas ao uso da *Internet* e de outras redes públicas de computadores, com o objetivo de reduzir o risco a que estão expostos os Ativos de Tecnologia da Informação da empresa, tendo em vista que a *Internet* tem sido veículo de muitas ações prejudiciais às organizações, gerando perdas financeiras, perdas de produtividade, danos aos sistemas e à imagem da organização, entre outras consequências. Estabelecer diretrizes de proteção e conduta no uso das Redes Sociais.

8.12.5 Conscientização de Segurança da Informação

Desenvolver programas de capacitação específicos, visando à ampliação da cultura organizacional, quanto à importância da segurança da informação, e seu valor estratégico para a empresa.

8.12.6 Acesso ao Correio e a Ferramentas de Colaboração

Estabelecer regras para utilização de correio eletrônico e ferramentas de colaboração providas pela empresa.

8.12.7 Proteção contra Códigos Maliciosos

Estabelecer regras para a proteção dos recursos de Tecnologia da Informação da empresa contra ação de códigos maliciosos e programas impróprios.

8.13 Gestão de Riscos

8.13.1 Análise, Avaliação e Tratamento de Riscos

Estabelecer regras para implementar um processo sistêmico de gerenciamento de riscos, que adote uma metodologia de gestão de riscos de segurança da informação, contemplando, análise e avaliação, tratamento, aceitação e comunicação de riscos.

8.13.2 Gestão de Continuidade de Negócios

Estabelecer regras e os princípios que regulamentam a Gestão da Continuidade do Negócio - GCN, através de um processo sistêmico para que se construa uma resiliência organizacional que seja capaz de responder efetivamente aos incidentes críticos de segurança e salvaguardar as atividades e a reputação da empresa.

8.14 Monitoramento e Auditoria

Estabelecer regras para criação de um programa de auditoria interna do processo de Gestão de Segurança da Informação, visando a verificar o cumprimento da Política de Segurança da Informação e se controles implementados estão atendendo eficazmente a conformidade dos requisitos.

Deverá ser conduzida uma análise crítica dos resultados da auditoria, com o objetivo de determinar ações preventivas e corretivas para melhoria contínua do processo de Gestão de Segurança da Informação. Um plano de ação deve ser elaborado com base no relatório gerado pela auditoria.

O resultado de auditoria de Segurança da Informação deve ser caracterizado como informação sigilosa, quando esse puder comprometer a segurança dos processos de negócio da empresa.

Todo ativo de informação sob responsabilidade do CIASC é passível de auditoria em data e horários determinados pelo CGSI, podendo esta, também, ocorrer sem aviso prévio.

Na realização de uma auditoria, durante a sua execução, deverão ser resguardados os direitos quanto à privacidade de informações pessoais, desde que estas não estejam dispostas em ambiente físico ou lógico de propriedade do CIASC ou de seus clientes de forma que se misture ou impeça o acesso às informações de propriedade ou sob responsabilidade do CIASC.

Com o objetivo de detectar atividades anômalas de processamento da informação e violações da Política, das Normas ou dos Procedimentos de Segurança da Informação, a COSEI poderá realizar monitoramento e controle proativos, mantendo a confidencialidade do processo e das informações obtidas, sendo que, as informações obtidas poderão servir como indício ou evidência em processo administrativo e/ou legal.

8.15 Gestão de Indicadores de Segurança

Indicadores e métricas devem ser definidos para os processos de segurança da informação, objetivando monitorar, através de uma análise crítica, o desempenho e eficácia dos controles implementados. Os indicadores deverão ser criados baseados nos objetivos estratégicos da empresa.

A análise crítica deve ser realizada em intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia e demonstrem apoio e comprometimento com a Segurança da Informação

9 Penalidades/Processo Disciplinar

Nos casos em que houver violação desta Política ou das normas de segurança da informação, sanções administrativas e/ou legais poderão ser adotadas, podendo culminar com o desligamento e eventuais processos administrativos, cíveis e judiciais cabíveis.

9.1 Violações

São consideradas violações à política, às normas ou aos procedimentos de segurança da informação as seguintes situações, não se limitando às mesmas:

a) Quaisquer ações ou situações que possam expor o CIASC ou seus clientes à perda financeira e de imagem, direta ou indiretamente, potenciais ou reais, comprometendo seus ativos de informação;

b) Utilização indevida de dados corporativos e divulgação não autorizada de informações, segredos comerciais ou outras informações sem a permissão expressa do responsável legal pela informação;

c) Uso de dados, informações, equipamentos, *software*, sistemas ou outros recursos tecnológicos, para propósitos ilícitos, que possam incluir a violação de leis, de regulamentos internos e externos, da ética ou de exigências de organismos reguladores da área de atuação do CIASC ou de seus clientes; e

d) A não comunicação imediata à COSEI de quaisquer descumprimentos da política, de normas ou de procedimentos de Segurança da Informação, que porventura um colaborador, empregado, estagiário, aprendiz ou prestador de serviços venha a tomar conhecimento ou chegue a presenciar.

9.2 Sanções

A violação à política, às normas ou aos procedimentos de segurança da informação ou a não aderência à Política de Segurança da Informação do

CIASC são consideradas faltas graves, podendo ser aplicadas penalidades previstas em normas internas de recursos humanos ou leis vigentes.

10 Atualização

Deve-se estabelecer a periodicidade mínima para a revisão da Política de Segurança da Informação, bem como os demais documentos normativos gerados a partir dela, a fim de que não fiquem ultrapassados ou desatualizados. Não obstante, a política pode ser revisada tempestivamente, a qualquer momento que se fizer necessário.

11 Aprovação

Os documentos integrantes da estrutura normativa da Segurança da Informação do CIASC deverão ser aprovados e revisados conforme critérios descritos abaixo:

11.1 Política

Nível de aprovação: Comitê Gestor e Diretoria do CIASC.

Periodicidade da revisão: Anual.

11.2 Normas Técnicas

Nível de aprovação: Gerentes de áreas, Comitê Gestor e Diretoria do CIASC.

Periodicidade da revisão: Semestral.

11.3 Procedimentos

Nível de aprovação: Coordenadores e Gerentes de áreas.

Periodicidade da revisão: Semestral.

12 Referências Legais

Correlacionam-se com a política, com as diretrizes e com as normas de Segurança da Informação as Leis abaixo relacionadas, mas não se limitando às mesmas:

Decreto-Lei 2.848, de 7 de dezembro de 1940 (Institui o Código Penal);

Lei Federal 3.129, de 14 de outubro de 1982 (Regula a Concessão de Patentes aos Autores de Invenção ou Descoberta Industrial);

Lei Federal 8.159, de 08 de janeiro de 1991 (Dispõe sobre a Política Nacional de Arquivos Públicos e Privados);

Lei Federal 9.279, de 14 de maio de 1996 (Dispõe sobre Marcas e Patentes);

Lei Federal 9.610, de 19 de fevereiro de 1998 (Dispõe sobre o Direito Autoral);

Lei Federal 9.983, de 14 de julho de 2000 (Altera o Decreto-Lei 2.848, de 7 de dezembro de 1940 - Código Penal e dá outras providências).

Lei Federal 10.406, de 10 de janeiro de 2002 (Institui o Código Civil);

Lei Federal 12.737, de 30 de novembro de 2012 (Tipifica os Delitos Informáticos);

Lei Federal 12.965, de 23 de abril de 2014 (Marco Civil);

Lei Federal 13.709, de 14 de agosto de 2018 (LGPD).

13 Referências Normativas (Conformidade)

A gestão de segurança da informação deve atender aos requisitos normativos dos órgãos regulatórios de segurança da informação do Governo Estadual e

Federal, assim como, às normas ABNT de segurança de informação, aplicáveis ao negócio da organização. Deve haver disponível para o conhecimento de todos uma relação de normas e leis relacionados à Segurança da Informação.

Norma Técnica ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização.

Norma ABNT NBR ISO/IEC 27002:2013, que trata de Código de Prática para a Gestão da Segurança da Informação.

Norma Técnica ABNT NBR ISO/IEC 27005:2011, que fornece diretrizes para o processo de gestão de riscos de Segurança da Informação.

Norma Técnica ABNT ISO GUIA 73:2009, que fornece as definições de termos genéricos relativos à gestão de riscos.

Norma Técnica ABNT NBR ISO 31000:2018, que fornece princípios e diretrizes genéricas para a gestão de riscos (item alterado pela Portaria nº 6.493/2019).