PONTOTEL

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Sumário

Informações Gerais

Como qualquer outro ativo, a informação também é importante para os negócios e, consequentemente, precisa ser adequadamente protegida especialmente em ambientes de negócios altamente interligados, como nos dias de hoje.

Esta Política de Segurança da Informação busca proteger as informações da Pontotel e de seus clientes de uma ampla gama de ameaças, de maneira a assegurar a continuidade dos negócios, minimizar os riscos e dar suporte à maximização do retorno sobre os investimentos em TI e aproveitamento de novas oportunidades de negócio. Definição, aquisição, operação e melhoria da área de Segurança da Informação são atividades essenciais para se garantir a competitividade, rentabilidade, conformação com requisitos legais e proteção da imagem comercial nos mercados de atuação da empresa.

A presente Política de Segurança da Informação (PSI) é parte integrante e estruturante do Sistema de Gestão de Cibersegurança e Privacidade (SGCP) da Pontotel, descrevendo princípios, requisitos e regras que devem ser comunicados, compreendidos e incorporados nas atividades do dia a dia, por todos os gestores, colaboradores e terceiros.

Objetivo

Esta Política de Segurança da Informação (PSI) descreve princípios, requisitos e regras de proteção de ativos de informação da Pontotel e de seus clientes, definindo as linhas mestras de desenvolvimento e operação seguros de Tecnologia da Informação e Comunicações (TIC) na empresa.

Escopo

Todas as operações de TIC na Pontotel, em todas as áreas de negócio, devem atender aos requisitos estabelecidos nesta Política.

Referências Bibliográficas

- ABNT NBR ISO/IEC 27001:2013 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos
- ABNT NBR ISO/IEC 27005:2011 - Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança da informação
- NIST SP800-53r5:2020 - Security and Privacy Controls for Information Systems and Organizations.

Definições

- ➔ Ação Corretiva: ação para eliminar a causa de uma não-conformidade detectada ou de uma situação indesejável.
- ➔ Ação Preventiva: ação que visa eliminar a causa de uma não-conformidade potencial ou de uma situação indesejável potencial.
- ➔ Aceitação ao Risco: decisão de aceitar o risco.
- ➔ Ameaça: a causa potencial de um incidente indesejado que pode resultar em prejuízo para um sistema ou organização.
- ➔ Análise de Riscos: uso sistemático de informações para identificar fontes de risco e estimá-los.
- ➔ Ativo: qualquer coisa que tenha valor para a organização, que gere uma despesa para a sua recuperação, caso seja perdido.
- ➔ Auditoria: processo sistemático, independente e documentado, usado para se obter evidências e avaliar situações de maneira objetiva, visando determinar se os critérios estabelecidos estão sendo seguidos. Consiste na comparação das práticas e sistemas existentes com os métodos, procedimentos e instruções precisamente definidas. A análise de registros e atividades para verificar sua exatidão é geralmente feita por alguém diferente da pessoa por eles responsável
- ➔ Avaliação de Riscos: todo o processo de análise e avaliação de riscos, ou o processo de comparação entre o risco estimado e os critérios de risco identificados para determinar o significado do risco.
- ➔ Avaliação: verifica o nível relativo de excelência, qualidade, ou utilidade de uma entidade com respeito a uma finalidade específica.
- ➔ Certificação: ação de uma autoridade em executar de maneira documentada uma conformação com requisitos pré-estabelecidos.
- ➔ Cibersegurança: o mesmo que Segurança da Informação.
- ➔ Chief Information Security Officer (CISO): o mesmo que Oficial-Chefe de Segurança da Informação.
- ➔ Cliente: organização ou pessoa que recebe um produto ou para a qual é executado um serviço.
- ➔ Comitê de Segurança da Informação (CSI): formado por gestores representantes das diferentes áreas da organização com objetivo de apoio da Alta Direção no desenvolvimento das atividades de segurança e suporte à tomada de decisões estratégias e táticas.
- ➔ Confidencialidade: assegura que a informação seja acessível somente às pessoas autorizadas.
- ➔ Conformidade: atendimento de um requisito especificado pela qualidade em relação à característica de um produto ou serviço.
- ➔ Controle: equipamentos, softwares, técnicas operacionais e atividades que dão sustentação à segurança de produtos e serviços em relação a requisitos específicos. Tem o mesmo significado quanto ao uso dessas técnicas.

- ➔ Controle de Ativo: envolvem ações para proteção de qualquer tipo de ativo, assegurando o acesso apenas pelas pessoas autorizadas, além de aprovação, armazenamento, revisão, mudança e distribuição adequados, incluindo ativos de TI como sistemas de informação e comunicação, bases de dados e arquivos em geral.
- ➔ Controle de Risco: representa os meios para a redução dos riscos, incluindo políticas, procedimentos, regras norteadoras, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, gerencial ou legal.
- ➔ Evento de Segurança da Informação: ocorrência identificada em um sistema ou no estado da estrutura de serviços que indica uma possível falha na política de Segurança da Informação ou nas proteções implementadas, ou, ainda, de uma situação previamente desconhecida que possa ser relevante para a segurança.
- ➔ Evidência de Conformação: documentos atestando que uma entidade se conforma a determinados requisitos previamente definidos.
- ➔ Fornecedor: usado para subcontratante, vendedor ou locador de produtos e serviços.
- ➔ Garantia de Segurança: todas as atividades e funções relativas à implementação da segurança.
- ➔ Gerenciamento da Segurança: ações de gerenciamento que orientam e controlam a organização com respeito à Segurança da Informação.
- ➔ Gerenciamento de Riscos: consiste nas atividades coordenadas que visam dirigir e controlar uma organização no que diz respeito ao gerenciamento do risco, geralmente incluindo avaliação tratamento, aceitação e divulgação dos riscos.
- ➔ Incidente de Segurança da Informação: consiste em um único ou uma série dos eventos não desejados, ou inesperados, de Segurança da Informação que têm uma probabilidade significativa de comprometer as operações do negócio e a segurança.
- ➔ Infraestrutura de Processamento de Informações: qualquer sistema de processamento de informação, infraestrutura de serviços, ou ambientes físicos onde são abrigados.
- ➔ Integridade: proteção da exatidão e a integralidade das informações e métodos de processamento.
- ➔ Oficial-Chefe de Segurança da Informação (CISO): cabe a liderança dos esforços de Segurança da Informação, dando suporte à tomada de decisões pela Alta Direção e fortalecendo a Cultura de Segurança.
- ➔ Política de Segurança: todas as intenções e orientações com respeito à segurança formalmente expressa pela alta gerência.
- ➔ Produto: resultado de um processo. Pode ser usado como serviço.
- ➔ Programa de Conscientização: empregado para assegurar que todos os profissionais estejam conscientes dos requisitos do SGCP, que todos passem pelo treinamento em conscientização bem como pelo treinamento específico de suas áreas particulares de aplicação.
- ➔ Registros de Segurança: evidências obtidas sobre as características e recursos de um produto ou serviço de segurança e os processos aplicados ao seu desenvolvimento, projeto, produção, instalação, manutenção e eliminação, bem como aos registros sobre avaliações, auditorias, e outras verificações de uma organização para determinar sua capacidade em atender os requisitos de segurança definidos.

- ➔ Requisito: uma necessidade ou expectativa que foi definida, geralmente implícita ou obrigatória.
- ➔ Risco: combinação de probabilidade de ocorrência de um evento com as consequências potenciais, expressa a natureza incerta dos resultados dos processos no ambiente de negócios.
- ➔ Segurança da Informação: diz respeito à preservação da confidencialidade, integridade e disponibilidade da informação, além de outras propriedades tais como autenticidade, contabilidade, não-repúdio, e confiabilidade, que podem ser envolvidas.
- ➔ Segurança: neste contexto, tem o mesmo significado de Segurança da Informação.
- ➔ Segurança Cibernética: o mesmo que Segurança da Informação.
- ➔ Sistema de Gerenciamento: sistema usado no estabelecimento de políticas e objetivos, bem como para se alcançar esses objetivos.
- ➔ Sistema de Gestão de Cibersegurança e Privacidade (SGCP): conjunto formado por princípios, requisitos, políticas, processos, controles, registros, equipamentos, softwares e pessoas capacitadas, com objetivo de assegurar a continuidade dos negócios, minimizar os riscos e dar suporte à maximização do retorno sobre os investimentos em TIC e oportunidades de negócio.
- ➔ Sistema de Segurança: a estrutura organizacional, responsabilidades, atividades, recursos e eventos que juntos oferecem procedimentos e métodos organizados de implementação, garantindo que a organização alcance os requisitos de segurança definidos.
- ➔ Terceiro: aquela pessoa ou grupo reconhecido como sendo independente das partes envolvidas em relação às questões tratadas.
- ➔ Tecnologia da Informação e Comunicações (TIC): compreende todas as operações de coleta, processamento, armazenamento e redes de comunicação de informações digitais.
- ➔ Tratamento do Risco: processo de seleção e implementação de medidas para modificação das características do risco.
- ➔ Validação: confirmação através da apresentação de evidências objetiva que as exigências para um determinado uso ou uma aplicação específica foram cumpridas.
- ➔ Verificação de Sistemas: um processo para assegurar que as funções estão em conformidade com políticas e auditoria.
- ➔ Verificação: inspeção de uma entidade para determinar se há conformação com os requisitos pré-estabelecidos.
- ➔ Vulnerabilidade: uma fraqueza de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

Segurança da Informação

A Era da Informação consolidou a demanda pelo atendimento das obrigações de cibersegurança das empresas, como exigência para a sustentabilidade dos negócios, para empresas nas mais diversas áreas de atuação e tamanho das operações. Paralelo aos ganhos de produtividade e velocidade das operações, decorrência da implantação maciça de recursos digitais, encontramos

o desafio de coordenar pessoas, processos e sistemas tecnológicos visando identificar e mitigar os riscos de segurança associados.

Na medida que sistemas de TIC permeiam todas as áreas, processos e atividades de uma organização, passa a ser imperativo a implementação e operação de um sistema de gestão de segurança da informação que se apoie em conceitos, princípios e regras reconhecidamente eficazes e eficientes, para uma abordagem sistemática de garantia da confidencialidade, integridade, disponibilidade, privacidade, responsabilidade e legalidade das informações.

Política de Segurança da Informação

A presente Política de Segurança da Informação (PSI) define requisitos nas seguintes áreas, que serão apresentados em detalhes nos próximos Capítulos:

- Governança de Segurança da Informação
- Ativos de Informação
- Segurança de Informações
- Gestão da Privacidade
- Identidades e Acessos
- Operações Seguras de TIC
- Segurança de Pessoas
- Segurança de Redes
- Segurança de Extremidade
- Gerenciamento de Criptografia
- Segurança Física
- Gerenciamento de Incidentes
- Gerenciamento de Mudanças
- Gestão da Continuidade de Negócios
- Segurança de Fornecedores
- Auditoria de Segurança
- Desenvolvimento de Software

Governança de Segurança da Informação

A Governança de SI busca o alinhamento entre as ações de garantia da segurança com os objetivos de negócio estabelecidos e as estratégias adotadas. Este alinhamento deve-se dar desde as decisões tomadas ao nível estratégico, até a implementação e operação dos controles do SGCP.

Organização

A SI na Pontotel compreende a seguinte organização:

- Alta Gestão: responsável final pelo acompanhamento das ações de SI na empresa, cujo papel de liderança é fundamental para o sucesso das ações implementadas.

- Comitê de Segurança da Informação: composto por colaboradores de diferentes áreas da Pontotel, é responsável pelo suporte à tomada de decisões e implementação das ações de SI na empresa.

- Equipes de Suporte: formada por colaboradores e consultores externos, responsável pela implementação de controles do SGCP, análises de segurança e suporte ao tratamento de incidentes de SI.

Gerenciamento de Políticas e Processos

Todas as políticas e processos de SI devem ser gerenciados de maneira a garantir a sua integridade, atualidade e pertinência com os objetivos de negócio estabelecidos.

Gerenciamento de Requisitos de SI

Os requisitos legais, contratuais e regulatórios envolvendo SI devem ser gerenciados visando a garantia do atendimento pelos controles do SGCP, comprovado com base em registros operacionais e demais evidências coletadas regularmente.

Requisitos Internos

Todos os controles do SGCP devem atender aos requisitos das políticas e processos internos de SI estabelecidos.

Propriedade Intelectual

Dentre os requisitos legais atendidos pelos controles do SGCP, os de garantia da proteção de propriedade intelectual das informações e aplicações utilizadas na empresa devem também receber atenção, inclusive dos Programas de Capacitação de admissão de novos colaboradores.

Análise Crítica de SI

Todas as ações de TIC envolvendo informações devem ser submetidas a uma análise crítica regular quanto à garantia do atendimento de requisitos de SI a que a empresa esteja submetida.

Responsabilização

Todos os colaboradores nos diferentes níveis administrativos e tecnológicos da Pontotel reconhecem formalmente a sua responsabilidade individual e em grupo pelo atendimento de requisitos de SI, estabelecidos em políticas e processos, em suas atividades na empresa.

Segregação de Funções

Devem ser implementados controles e análises regulares de papéis, funções e responsabilidades dos colaboradores, visando a segregação de funções, com objetivo de dificultar e evidenciar a ocorrência de práticas fraudulentas, corrupção e má-conduta no ambiente de trabalho.

Gerenciamento de Riscos

A identificação, avaliação e mitigação de riscos de SI devem ser regularmente implementadas e acompanhadas pelo Comitê de Segurança da Informação.
Dentre os riscos regularmente avaliados, temos:

- Invasões cibernéticas
- Cadeia de fornecedores
- Redes de computadores
- Humanos
- Operacionais
- Desenvolvimento de software
- Serviços de terceiros
- Privacidade de dados pessoais

A Alta Gestão tem a responsabilidade de apoiar as atividades de mitigação de riscos e utilizar os relatórios de análise de riscos como subsídio à tomada de decisões estratégias e táticas na empresa.

Melhora Contínua

Cabe ao Comitê de Segurança da Informação a implantação e acompanhamento de um Programa de Melhoria Contínua do SGCP, com base no Modelo PDCA:

- Planejar (Plan)
- Executar (Do)
- Verificar (Check)
- Agir (Action)

Cultura de Si

Cabe ao Comitê de Segurança da Informação a implantação e acompanhamento de um Programa de Conscientização em Cibersegurança e Privacidade, com objetivo de incorporar na Cultura Organização os conceitos, princípios e boas práticas de SI.

Rede de Contratos

O Comitê de Segurança da Informação deverá manter atualizada uma lista de contatos-chave de autoridades, especialistas e grupos de apoio de SI, promovendo regularmente atividades conjuntas para o fortalecimento das relações com estes grupos e a consolidação das competências de SI dos colaboradores.

Requisitos de Criptografia

Os requisitos legais, regulatórios e contratuais de criptografia de informações, aos quais a empresa esteja submetida, devem ser gerenciados e regularmente avaliados.

Gerenciamento de Projetos

Projetos internos ou externos devem incluir em todas as fases de concepção e desenvolvimento uma avaliação de requisitos de SI (security by design) e a comprovação final de atendimento desses requisitos, apresentados na entrega dos resultados finais.

Dentre os requisitos de SI previamente estabelecidos existe o de garantia de falha segura (security by default), para que falhas operacionais não venham a comprometer o atendimento de requisitos de segurança.

Informações e Aplicações

Todas as informações e aplicações acessadas por usuários internos e externos devem ser avaliadas frente ao atendimento dos requisitos legais, regulatórios e contratuais de SI.

Titulares de Dados

Devem ser implementados controles e processos para garantia do atendimento dos direitos de Titulares de Dados Pessoais, atendendo, em particular, os requisitos estabelecidos pela Lei Geral de Proteção de Dados Pessoais (LGPD) e pela Autoridade Nacional de Proteção de Dados (ANPD).

Seguros de SI

Sempre que ocorrer situações para as quais os riscos de falha de atendimento de requisitos de SI sejam superiores aos níveis admissíveis, a contratação de seguro contra incidentes de alto impacto deve ser providenciada, como seguro contra invasões cibernéticas ou seguro contra falha de atendimento dos direitos dos Titulares de Dados.

Auditorias de SI

Cabe ao Comitê de Segurança da Informação a implantação de um Plano de Auditoria de SI, acompanhando a identificação de mitigação de não-conformidades de SI, aprovação de Relatórios de Auditoria de SI pela Alta Gestão e divulgação de resultados e Lições Aprendidas entre os gestores de negócio de áreas envolvidas.

Ativos de Informação

Ativos são recursos ou competências para o desenvolvimento das atividades de uma organização, aos quais podemos associar um valor: equivalente àquele que será pago para adquirir um ativo do mesmo tipo em caso de perda do original, ou valor de negócio gerado a partir da utilização do ativo, ou valor que precisa ser investido para desenvolvimento de um novo ativo com as mesmas características.

Gerenciamento de Ativos

O gerenciamento de ativos de informação da Pontotel deve ser implementado com objetivo de reduzir os riscos de prejuízos e garantir o alinhamento com boas práticas reconhecidas de mercado.

Classificação de Ativos

Os ativos de informação de uma organização precisam ser classificados e rotulados em:

- Tangíveis
- Hardware: como roteadores, servidores e storages.
- Dispositivos: pendrives, fitas magnéticas, HD's USB.

- Cabeamento de rede: como cabos, dutos e bandejas de passagem.
- Facilidades: como geradores de energia elétrica, nobreaks, cabos de comunicação.
- Intangíveis
- Softwares: como código-fonte, código executável de aplicações.
- Configurações: como configuração de dispositivos na Nuvem, regras de roteamento, regras de firewalls, configurações de redes sem fio.
- Credenciais: como credenciais de acesso à infraestrutura de Nuvem, identificadores e senhas de contas administrativas e de usuários, chaves públicas e privadas de controle de acesso.
- Dados: como bases de dados, metadados, registros de monitoramento de incidentes.
- Dados pessoais: como nome, RG, endereço, eMail, fotos, currículo, identificadores biométricos, atestados médicos.
- Contratos: como licenças de software e contratos de locação.
- Certificações: como certificações de normas, selos de acreditação e atestados.
- Serviços: como manutenção, monitoração e gerenciamento de projetos.
- Documentação: políticas, planos, processos, procedimentos, relatórios, documentação de softwares, manuais de usuários.
- Conhecimento: como conceitos e princípios da Cultura Organizacional, códigos de bom uso de recursos, medidas antifraude e anticorrupção, Código de Ética, cursos de capacitação e programas de conscientização.

Segurança e Privacidade

Os dados precisam ser classificados de acordo com o nível de segurança da informação e privacidade em:

- Público: com acesso externo à empresa.
- Interno: com acesso apenas por colaboradores da empresa.
- Confidencial: com acesso apenas por pessoas autorizadas.
- Dados pessoais: com acesso interno apenas por pessoas autorizadas.
- Dados pessoais sensíveis: com acesso interno apenas por pessoas autorizadas.

Inventário de Ativos

Deve ser criado e atualizado sistematicamente um Inventário de Ativos de Informação, contendo:

- Hardwares;
- Contas de acesso local e remoto;
- Documentos sigilosos;
- Inventários de mídias e dispositivos
- Sistemas de TIC;
- Softwares;
- Aplicações críticas de negócio;

- Redes e links de comunicação;
- Recursos de Computação em Nuvem;
- Competências-chave;
- Serviços de TIC.

Segurança da Informação

O SGCP deve incorporar os seguintes controles de proteção de ativos de informação:

- Arquitetura funcional e técnica;
- Especificação de requisitos de segurança e privacidade;
- Captura de informações;
- Processamento de informações;
- Armazenamento de informações;
- Transporte de mídias;
- Comunicação de informações;
- Expurgo de informações;
- Descarte de mídias, dispositivos e equipamentos;
- Atendimento de requisitos;
- Encriptação de informações.

Gerenciamento da Privacidade

O SGCP deve incorporar os seguintes controles de garantia da privacidade de dados pessoais e de atendimento dos direitos dos Titulares:

- Papéis, responsabilidades e atividades;
- Requisitos de privacidade;
- Inventário de dados pessoais;
- Mapas e domínios de dados;
- Relatórios de impactos de risco a privacidade;
- Proteções de informações de identificação pessoal (PII);
- Tratamentos de dados pessoais;
- Compartilhamentos de dados pessoais;
- Atendimentos de solicitações de Titulares;
- Armazenamentos e retenções de dados pessoais;
- Registros de tratamento de dados pessoais;
- Anonimizações e pseudonimizações de dados pessoais;
- Incidentes envolvendo dados pessoais;
- Comunicações de incidentes;
- Interoperabilidades de dados pessoais.

Identidades e Acessos

O SGCP deve garantir a segurança de identidades e acessos aos ativos de informação da Pontotel.

Sistema de Autenticação

Deve ser implementado um sistema de autenticação de identidades de sistemas e usuários, tanto internos quanto externos.

Políticas e Processos

Devem ser implantados e periodicamente revisados políticas e processos de gerenciamento de contas de serviços internos e externos, como também de autorização de acesso e de acesso privilegiado aos ativos de informação.

Controles de Identidades e Acessos

O SGCP deve incorporar os seguintes controles de identidades de sistemas e usuários e de acesso aos ativos de informação:

- Controle de senhas;
- Controle de autenticação por duplo fator;
- Entrada e saída seguras nos sistemas;
- Controle de acesso em regimes especiais, como férias e afastamento;
- Registros de acesso;
- Segregação de funções;
- Suspensão automática de acesso;
- Condições de recuperação de acesso.

Operações Seguras De TIC

O SGCP deve garantir a operação segura de TIC na Pontotel, operando controles de segurança de:

- Ambientes de desenvolvimento, qualidade e produção;
- Configuração de ativos de informação (security by design/ by default);
- Sistemas de identificação;
- Acesso aos ativos de informação, local e remoto;
- Softwares operacionais e utilitários privilegiados;
- Aplicações de negócio;
- Licenças de uso de softwares;
- Vulnerabilidades técnicas, operacionais e de configurações;
- Atualizações de hardwares, firmwares e softwares
- Redes de computadores e links de comunicação;

- Trabalho remoto de usuários;
- Serviços de Nuvem;
- Dispositivos móveis;
- Manutenção de ativos;
- Documentação e procedimentos operacionais;
- Registros de incidentes e evidências;
- Testes de penetração e ensaios;
- Suporte à operação e aos usuários.

Segurança de Pessoas

As pessoas são muito importantes na garantia da segurança e privacidade de ativos de informação da Pontotel.

Adesão de Pessoas

Deve ser controlada a adesão obrigatória e formal de todos os colaboradores às políticas de segurança e códigos de conduta definidos pela empresa, incluindo o reconhecimento da responsabilidade individual e coletiva pela garantia da segurança dos ativos de informação.

Ciclo de Vida de Usuários

Ações de capacitação, conscientização e operação de controles de segurança e privacidade do SGCP devem cobrir a todas as etapas do ciclo de vida de usuários de ativos de informação, internos e terceiros:

- Seleção
- Admissão
- Integração
- Acompanhamento
- Desligamento

Aprovação de Acesso

O nível de acesso de colaboradores aos ativos de informação deve ser aprovado pelos respectivos gestores da área de trabalho e revisados periodicamente.

Repreensão De Mau Uso

O mau uso de ativos de informação por parte de usuários poderá levar à repreensão formal e a processos disciplinares, podendo inclusive resultar no cancelamento do acesso e desligamento do colaborador.

Segurança de Redes

O SGCP deve garantir a operação segura ativos de redes de computadores e links de comunicação da Pontotel, operando controles de segurança de:

- Configuração de redes locais;
- Configuração de recursos de Nuvem;
- Configuração de redes wireless;
- Serviços de redes públicas;
- Links de acesso criptografados (VPN's);
- Segregação de tráfegos de rede;
- Serviços de rede;
- Acesso de usuários aos serviços de rede;
- Transferência de informações via redes internas e externas;
- Acordos de transferência de informações;
- Serviços de mensagens eletrônicas;
- Acordos de confidencialidade e não divulgação;
- Acordos de melhores práticas com terceiros.

Segurança de Extremidade

A garantia da segurança de equipamentos dos usuários (end-point security) é fator decisivo para assegurar o atendimento de requisitos de segurança para os negócios.

O SGCP deve operar controles de segurança relativos a:

- Configurações seguras, manuais e automáticas;
- Antimalwares, como worms, cavalos de tróia, spywares e rootkits
- Monitoramento e alarmes;
- Atualizações de softwares e firmwares;
- Armazenamentos autorizados de dados;
- Softwares homologados
- Agentes de monitoração de computadores;
- Cópias de segurança de dados e softwares;
- Recuperação de sistemas comprometidos.

Gerenciamento de Criptografia

O SGCP deve operar controles de gerenciamento de recursos criptográficos relativos a:

- Requisitos de criptografia;
- Configurações de sistemas de criptografia;
- Algoritmos de criptografia autorizados;
- Gerenciamento de chaves criptográficas.

Gerenciamento de Incidentes

O SGCP deve operar controles de gerenciamento de incidentes relacionados a:

- Definição de papéis e responsabilidades;
- Definição de padrões de incidentes;
- Procedimentos de identificação e resposta a incidentes;
- Procedimentos de coleta e proteção de evidências;
- Monitoramento de incidentes
- Suporte à decisão sobre tratamento de incidentes;
- Escalamento de incidentes;
- Resposta a incidentes;
- Registros de eventos;
- Análise crítica de registros de incidentes;
- Análise de vulnerabilidades e ameaças;
- Notificação interna e externa;
- Proteção de registros;
- Controle de causas-raiz;
- Gestão de evidências: identificação, coleta, aquisição e preservação;
- Elaboração de relatórios de Incidentes;
- Elaboração de relatórios de Lições Aprendidas e sugestões de melhorias;
- Sincronização de relógios de sistemas.

Gerenciamento de Mudanças

Deve ser implementado um processo de gerenciamento de mudanças em ativos de informação, que enderece as seguintes áreas:

- Requisitos de negócio sobre mudanças;
- Atualização de políticas, processos e procedimentos sobre mudanças;
- Gerenciamento de riscos de mudanças;
- Funcionalidades de sistemas de TI;
- Plataformas operacionais;
- Pacotes de software;
- Aplicações críticas de negócio;
- Recursos de Nuvem;

- Desenvolvimento de software;
- Capacidade de sistemas.

Gerenciamento da Continuidade

Deve ser implementado um processo de gerenciamento da continuidade de negócios, que enderece as seguintes áreas:

- Requisitos de disponibilidade de áreas de negócio;
- Elaboração e atualização de processos, procedimentos e controles de continuidade;
- Elaboração e implementação do Plano de Continuidade de Negócios;
- Preparação para contingenciamento e continuidade;
- Backups de dados e sistemas;
- Mídias de armazenamento;
- Recursos em Nuvem;
- Definição de cenários de desastres;
- Reação a emergências;
- Treinamentos de colaboradores e terceiros;
- Testes e ensaios de contingenciamento e recuperação;
- Análise de resiliência de sistemas e áreas de negócio;
- Recursos de contingenciamento.

Segurança de Fornecedores

O SGCP deve operar controles de segurança de fornecedores relacionados a:

- Assinatura de acordo de confidencialidade – NDA;
- Avaliação de vulnerabilidades e ameaças;
- Gerenciamento e mitigação de riscos associados;
- Contratação de fornecedores;
- Monitoramento de serviços de fornecedores;
- Mudanças de serviços de terceiros;
- Requisitos de serviços de terceiros;
- Manutenção e suporte de terceiros;
- Softwares de terceiros;
- Capacitação de terceiros;
- Requisitos de contratos;

Auditoria de Segurança

O SGCP deve incorporar processos e procedimentos de auditoria de segurança relacionados a:

- Planejamento;

- Operação;
- Riscos;
- Sistemas;
- Dados;
- Privacidade;
- Cibersegurança;
- Reação a incidentes;
- Qualidade e execução de Planos de Ação;
- Segurança de registros e evidências;
- Tempos de retenção de dados;
- Não-conformidades;
- Reação a incidentes;
- Governança de segurança e privacidade;
- Elaboração de relatórios;
- Análise crítica da conformidade técnico operacional;
- Elaboração de relatórios de auditoria;
- Elaboração de relatórios de Lições Aprendidas e sugestões de melhoria.

Desenvolvimento de Softwares

Deve ser implementado políticas e processos de gerenciamento da segurança de desenvolvimento de software, que enderece as seguintes questões:

- Ambientes de desenvolvimento;
- Codificação segura;
- Proteção de dados de teste;
- Testes estáticos e dinâmicos;
- Testes de aceitação com usuário final;
- Sistemas seguros;
- Desenvolvimento by design/ by default;
- Capacitação de profissionais;
- Implementação e entrega seguras (CI-CD);
- Mudanças de funcionalidades;
- Acessos ao código-fonte de programas;
- Transações em aplicativos;
- Desenvolvimento terceirizado.

Atualização e Validade

Este documento será atualizado sempre que modificações relevantes ocorrerem.

Este documento passa a valer a partir de 08/01/2021.