TecnoTech
Sistemas

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

Tecnotech Sistemas

Felipe Santos de Andrade / Wanderson Camara dos Santos

Política de uso da internet corporativa

Versão 1.0

Tecnotech Sistemas

Diretoria de Implementação e Projetos

Política criada sob a supervisão de

Romney Dutra / Lucas Diniz - Prolinx

Março de 2023

Abreviaturas e siglas

Confidencialidade: Garantia de que a Informação esteja acessível somente a pessoas com acesso autorizado.

Disponibilidade: Garantia de que os usuários autorizados obtenham acessos à informação e aos ativos correspondentes sempre que necessário.

Integridade: Garantia e salvaguarda da exatidão e completeza da Informação e dos métodos de processamento.

Colaborador: Toda pessoa que trabalha nos negócios da Tecnotech, podendo ser funcionário, estagiário ou terceirizado.

Colaboradores: Realizar suas atividades de forma a evitar incidentes.

Conteúdo

Lista de Tabelas

Capítulo 1

OBJETIVOS

Assegurar à TecnoTech a conformidade da Política de Segurança da Informação com as normas Pertinentes, visando proteger os dados, garantindo que as informações que integram o patrimônio da Tecnotech e aquelas sob sua guarda (dados e informações de clientes), assim como as ferramentas utilizadas para sua obtenção, geração, modificação, armazenagem e disponibilização estejam em conformidade com as leis brasileiras e melhores práticas de segurança da informação. Manter os processos apoiados pelos sistemas informatizados da Tecnotech através da prevenção e solução de eventos de quebra de segurança da Informação. Disseminar boas práticas no uso seguro da Informação na Tecnotech

Capítulo 2

INTRODUÇÃO

Este documento estabelece a PSI – Política de Segurança da Informação da Tecnotech, que é um conjunto das normas, processos e procedimentos necessários à preservação e Segurança das Informações da Tecnotech.

A Informação é um ativo, como qualquer outro ativo importante do negócio, que tem um valor para a Tecnotech e consequentemente necessita ser protegida. A Segurança da Informação visa proteger a Informação de um grande campo de ameaças de forma a garantir a continuidade dos negócios, minimizando os danos ao mesmo e maximizando o retorno dos investimentos e de suas oportunidades.

A Segurança da Informação é aqui caracterizada pela preservação da:

Confidencialidade: que é a garantia de que a Informação esteja acessível somente a pessoas com acesso autorizado.

Integridade: que é a garantia e salvaguarda da exatidão e completeza da Informação e dos métodos de processamento.

Disponibilidade: que é a garantia de que os usuários autorizados obtenham acessos à informação e aos ativos correspondentes sempre que necessário.

Segurança da Informação é alcançada a partir da implantação de uma série de controles, que podem ser políticas, práticas, procedimentos, estruturas organizacionais, instalações, softwares e ferramentas de controles automatizadas. Estes controles são estabelecidos para garantir que os objetivos de segurança da Tecnotech sejam alcançados

Capítulo 3

GESTÃO DE RISCOS

Os riscos típicos que a Política de segurança da informação (PSI) da TecnoTech pretende eliminar, reduzir, tratar e controlar os Incidentes registrados como de Segurança da Informação no sistema de Governança de TI da Empresa e que estiverem em não conformidade com as normas de referência da PSI da Tecnotech conforme avaliação da Gestão de Segurança da Informação da empresa.

Alguns exemplos de riscos que podem ser gerenciados pela Segurança da Informação:

- Revelação de Informações sensíveis.
- Modificações indevidas de dados e programas.
- Perda de dados e programas.
- Destruição ou perda de recursos computacionais e instalações.
- Interdições ou interrupções de serviços essenciais.
- Roubo de propriedade seja qual for.

Capítulo 4

AMEAÇAS

Alguns tipos de ameaças a serem consideradas pela PSI da TecnoTech, em conformidade com o tipo de serviço prestado pela empresa.

Perda Integridade: Ameaças de ambiente, externas ou internas, oriundas de catástrofes, fenômenos da natureza e/ou qualquer evento provocado intencionalmente ou não. Cita-se aqui, como exemplo, fogo, enchentes, tempestades, inundações etc.

Indisponibilidade: Falhas em sistemas e/ou ambientes computacionais da Tecnotech ou de terceiros contratados por ela considerados críticos para o negócio da Empresa.

Divulgação não autorizada da Informação:A divulgação de Informações sensíveis aos Processos de Negócio da Tecnotech e de seus Clientes salvaguardados em seus ambientes, premeditada e/ou acidentalmente.

Alterações não autorizadas: Alterações não autorizadas, premeditadas e/ou acidentais, em sistemas e/ou equipamentos de Tecnologia da Informação ou que suportem os Processos de Negócio da TecnoTech.

Capítulo 5

REGULAMENTAÇÕES

As regulamentações que abrangem a PSI da Tecnotech:

A Tecnotech deve formalizar sua Política de Segurança da Informação e em conjunto com as normas e Procedimentos de Segurança da Informação e privacidade de dados, parte integrante da PSI da TecnoTech, compor um documento ou pasta, impresso ou eletrônico, a ser mantido e atualizado para consultas de todos seus colaboradores e pessoas autorizadas, a fim de praticarem no dia a dia de suas atividades.

Para manter a PSI alinhada com suas estratégias corporativas, deve ser criado um Comitê de Segurança da Informação na Tecnotech, formado por pessoas idôneas e de grau elevado de responsabilidade na Empresa. Aqui formados pela um de seus diretores sócios, um analista de segurança/governança, um analista jurídico e consultorias especializadas tanto sem segurança da informação quanto em privacidade dados.

Para implementar a PSI, devem ser criados mecanismos de controle que assegurem a sua atualização, monitoramento e efetividade. Uma Gestão de Segurança da Informação deve ser criada, cujo responsável deve fazer parte do Comitê de Segurança da Informação. Recomenda-se que esta área esteja ligada diretamente ao um dos sócios proprietários para garantir idoneidade.

A Tecnotech deve fazer conhecer a seus colaboradores, prestadores de serviços, fornecedores, terceiros, parceiros e clientes, que de alguma forma necessitem possuir acessos ao patrimônio de Informações da Empresa, sua PSI e seus Normativos de Segurança e responsabilidades pelo seu acesso a este Patrimônio, evidenciando estas ações, no que lhe concerne.

Todos os colaboradores da Tecnotech assim como seus prestadores de serviços, fornecedores, terceiros, parceiros e clientes que de alguma forma necessitem possuir acessos ao patrimônio de Informações da Empresa são responsáveis pelo conhecimento e cumprimento das normas de Segurança da Informação.

Assim, temos que a Política de Segurança da Informação visa preservar a Confidencialidade, Integridade e Disponibilidade das Informações, recomendando e descrevendo as condutas adequadas para o seu manuseio, controle, proteção e descarte, em conformidade com os demais Gerenciamentos de Processos existentes na Empresa.

Capítulo 6

DECLARAÇÃO DE COMPROMETIMENTO DA DIRETORIA

A Diretoria da Tecnotech declarar-se comprometida com a Segurança da Informação na Empresa, garantindo sua confidencialidade, a integridade e a disponibilidade, sendo replicado este comprometimento a todos os seus Colaboradores. Comprometimento esse declarado por participação ativa no comitê de segurança da empresa.

Capítulo 7

CONTROLES DE SEGURANÇA DA INFORMAÇÃO A SEREM TRATADAS NESSA PSI

7.1 SEGURANÇA FÍSICA

Conceituação: Conjunto de medidas destinadas à proteção e integridade dos ativos da Tecnotech e à continuidade dos seus serviços.
Vulnerabilidades:Recomenda-se a previsão de controles para riscos naturais (inundações, tempestades etc.), riscos acidentais (incêndios, interrupções de abastecimentos diversos etc.), entradas não autorizadas, roubos de patrimônio, dentre outros, em conformidade com os demais Processos de Gerenciamento existentes na Empresa.

7.2 SEGURANÇA LÓGICA

Conceituação: Conjunto de medidas destinadas à proteção de recursos computacionais em nível de sistema operacional e aplicação, contra utilização indevida ou desautorizada, intencional ou não.
Vulnerabilidades:Devem estar previstos acidentes por falhas e/ou sabotagem de hardware, software, aplicativos e procedimentos.

7.3 CONTINUIDADE DO NEGÓCIO

Conceituação: Contemplar as atividades necessárias para a continuidade dos negócios da Tecnotech, quando houver algum tipo de interrupção nos processos, serviços e/ou equipamentos.

considerados críticos à organização e acordados com a diretoria.

Vulnerabilidades:Devem estar previstas interrupções significativas das operações essenciais do negócio causadas pelas vulnerabilidades nas áreas de Segurança da Informação a serem tratadas.

7.4 ESTRUTURA DA SEGURANÇA DA INFORMAÇÃO

A estrutura da Segurança da Informação é constituída, basicamente, por um conjunto de controles, incluindo política, processos, normas e procedimentos de segurança. Objetiva a proteção das informações dos clientes e da empresa, nos seus aspectos de confidencialidade, integridade e disponibilidade. Sendo essa estrutura dívida em.

Estratégico: É o nível relativo às Políticas ou Diretrizes da Organização e descreve "o que deve ser feito". Representando no comitê pela presença do socio diretor.

Tático: É o nível relativo às Normas da Organização. Com base nas Políticas, são criadas as "regras"a serem adotadas. Representada no comitê pelas consultorias especializadas participantes quando necessário.

Operacional: - É o nível relativo aos Procedimentos da Organização. Com base nas Normas, se define "como serão implementadas, as regras". Representada no comitê pelos analistas da empresa responsáveis pelas implantações das normas e procedimentos.

Capítulo 8

ATRIBUIÇÕES E RESPONSABILIDADES

Do ponto de vista da Segurança da Informação, o conhecimento das melhores práticas de Segurança da Informação é de obrigatoriedade nata de todos os colaboradores, prestadores de serviço, terceirizados, parceiros, estagiários e/ou fornecedores que de alguma forma necessitem possuir acessos ao patrimônio de Informações da Empresa.

Em geral, as responsabilidades por executar as normas, processos e procedimentos, relacionados ou não à PSI e à Segurança da Informação, estão indicados nos próprios documentos e conforme algumas definições na Matriz RACI abaixo.

Tabela 8.1: MATRIZ RACI - Processo de Segurança da Informação

Id	Papéis	Governança	Especializadas	Jurídico	Suporte	Humanos	Colaborado
1	incidentes de Segurança	R	C	I	S	I	R
2	Divulgar práticas de Segurança	R	C	R	R	R	R
3	treinamentos de novos colaboradores	A	C			R	
4	Acompanhar tratativa dos incidentes de segurança		R	R	I		
5	Auditar processos controles de segurança	C	R	C		I	C

8.1 Legenda

A (Accountable): Responsável pela garantia da qualidade, eficiência e eficácia do processo. É o nível mais alto de responsabilidade no Processo.

R (Responsible): Responsável pela correta execução da atividade do processo, observadas as determinações do Proprietário do Processo.

S (Supportive): Suporta diretamente uma determinada atividade, apoiando o R na execução da mesma.

C (Consulted): Consultado, para emitir parecer que poderá influenciar na condução da atividade do processo tendo, inclusive, poder de veto.

I (Informed): Informado, sobre o andamento da atividade do processo. Essa informação pode ser feita das seguintes formas:

Ativamente: : Dada certa condição, situação ou status da atividade do processo, o departamento, setor ou área é notificado via e-mail, pop-up, SMS, ou qualquer outra forma mais adequada (a notificação ou não do agente depende de regras que serão definidas posteriormente pelo Projeto).

Passivamente: O departamento, setor ou área tem acesso para consulta aos registros sobre o andamento da atividade do processo. Porém, o departamento, setor ou área não recebe notificação, ficando a seu critério consultar ou não a base de dados para pesquisa.

Capítulo 9

TERMOS

9.1 TERMO DE USO DO SISTEMA DE INFORMAÇÕES TÉCNICAS E ADMINISTRATIVAS

É o documento oficial da Tecnotech que tem o objetivo de regular o acesso e a utilização do SITAC - Sistema de Informações Técnicas e Administrativas do CREA.

9.2 TERMO DE COMPROMISSO E CONFIDENCIALIDADE

Define que as informações e segredos comerciais de cada parte envolvida (incluindo controladas, controladoras ou sociedades sob controle comum) são confidenciais e incluem dados como invenções, dados comerciais, informações técnicas, patentes, projetos, software, processos de fabricação e manutenção, entre outros. O termo é assinado pelo funcionário para garantir a privacidade das informações da Tecnotech Sistemas.

9.3 O TRC - TERMO DE RESPONSABILIDADE E COMPROMISSO TERCEIROS

É o documento oficial da Tecnotech que compromete terceirizados, prestadores de serviços e parceiros, que de alguma forma necessitem possuir acessos ao patrimônio de Informações da Empresa.

9.4 O TA – TERMO DE ADVERTÊNCIA

é o documento oficial da Tecnotech que será aplicado aos colaboradores que descumprirem a política e as normas de segurança vigentes. A validade legal destes Termos somente deve ser reconhecida pela Tecnotech, e por qualquer outro órgão e/ou Empresa, quando devidamente assinados pelos responsáveis legais. O tempo de validação dos termos assinados deve ser exatamente igual ao tempo de prestação de serviço pelo assinante à Tecnotech.

Capítulo 10

CLASSIFICAÇÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

10.1 TERMO DE USO DO SISTEMA DE INFORMAÇÕES TÉCNICAS E ADMINISTRATIVAS

Entende-se como Incidente de Segurança da Informação, qualquer evento em curso ou ocorrido que contrarie a Política de Segurança da Informação e seus Normativos de referência, comprometa a operação do Negócio ou cause danos aos ativos críticos da organização. Estes Incidentes serão identificados através da Gestão de Incidentes (Processo de resposta a incidentes), pelas solicitações abertas na área de service desk e categorizadas como de Segurança da Informação, através de qualquer colaborador da Tecnotech que solicite uma avaliação à Gestão de Segurança da Informação de um Incidente e/ou solicitação e a mesma considere pertinente e solicite a abertura do chamado, os Incidentes relacionados em listagem proposta na IT de Segurança da Informação e, em caso de existência na Empresa, por Auditorias Internas de Segurança da Informação. Nota: Será considerado de Segurança da Informação qualquer Incidente que não esteja em conformidade com a Política de Segurança da Informação da Tecnotech e seus Normativos de referência.

10.2 TREINAMENTO E CONSCIENTIZAÇÃO

Deve ser estabelecido um programa de treinamentos e conscientização, para os colaboradores recém-contratados, em conjunto com a área de Recursos Humanos da Tecnotech, para que a Política e conceitos da Segurança da Informação, sejam semeados e divulgados entre os colaboradores.

10.3 CONTROLES

Para atingirmos os objetivos traçados na política de segurança da informação e nos processos / procedimentos que a cercam, utilizamos um conjunto adequado de controles adequados a realidade da Tecnotech, de forma a alcançarmos a sua eficácia. Os controles são recomendados a serem implementados conforme descrito abaixo:

Capítulo 11

POLÍTICA DE PRIVACIDADE DE DADOS

Sendo a Tecnotech provedora de soluções que manipulam dados de terceiros em nome de controladores em seu próprio nome, estabeleceu uma política de privacidade de dados afim de garantir a conformidade com as lei em relação a tratativa dos mesmos. Nota: O documento detalhado referente ao programa de privacidade de dados estabelecido pela TecnoTech encontra-se em seu diretório corporativo no caminho tecnotech.org/politica-privacidade/.

Capítulo 12

POLÍTICA DE BACKUP

A fim de buscar a garantida de disponibilidade da informação em situações de perda foi estabelecido uma política de backup que permita a recuperação de softwares, sistemas, dados, jobs e documentação, guardados em meio magnético. Recomenda-se que sejam efetuadas simulações periódicas de restauração de alguns dos conteúdos armazenados em backup e auditorias por amostragem, com apresentação de relatório sobre o procedimento executado e os resultados. Nota: O documento detalhado referente ao backup se encontra publicado no diretório corporativo da Tecnotech https://wiki.app.sitac.com.br/books/politica-de-backup-e-restauracao-de-dados-digitais.

Capítulo 13

POLÍTICA DE USO DA INTERNET CORPORATIVA

A utilização da internet deve ser de uso exclusivo para fins corporativos seguindo as normas e regras vigentes de acesso. Nota: O documento detalhado referente a utilização da internet se encontra publicado no diretório corporativo da TecnoTech no caminho https://wiki.app.sitac.com.br/books/politica-de-uso-da-internet-corporativa.

Capítulo 14

POLÍTICA DE CORREIO ELETRÔNICO

A utilização do correio eletrônico deverá ser somente para uso corporativo, sendo expressamente proibido a prática de SPAM ou qualquer conteúdo que comprometa a Tecnotech. Recomenda-se monitoramento e auditorias no processo de envio e recebimento de e-mails corporativos. Nota: O documento detalhado referente à utilização do correio se encontra publicado no diretório corporativo da Tecnotech https://wiki.app.sitac.com.br/book de-correio-eletronico.

Capítulo 15

POLÍTICA DE ACESSO LOGICO

O acesso lógico aos ativos e suas atribuições às dependências da TecnoTech ou armazenados em terceiros, deverá ser restrito e controlado. Aplica-se uma política que determina um conjunto de diretrizes para o gerenciamento de regras para controle do acesso lógico aos ativos de tecnologia da informação da Tecnotech. Nota: O documento que trata as responsabilidades, restrições e métodos relativos ao acesso lógico, bem como o uso, criação e conservação de senhas, encontram-se no diretório corporativo da TecnoTech no campinho https://wiki.app.sitac.com.br/books/politica-de-acesso-logico.

Capítulo 16

POLÍTICA DE CRIAÇÃO E USO DE SENHAS

O uso de credenciais fortes, um processo de gerenciamento eficaz e outros controles combinados. traz maior segurança de integridade as informações salvaguardas pela Tecnotech. Para tal estabeleceu-se uma política de criação e uso de senhas com o objetivo de estabelecer regras para a criação, gerenciamento e uso de senhas seguras, a fim de evitar que pessoas mal-intencionadas descubram suas senhas e acessem sua conta, obtendo acesso não autorizado a informações confidenciais da TecnoTech em seu nome. Nota: O documento que trata as responsabilidades, encontra-se no diretório corporativo da TecnoTech em https://wiki.app.sitac.com.br/books/politica-de-criacao-e-uso-de-senhas

Capítulo 17

POLÍTICA DE ACESSO FÍSICO

O acesso as dependências físicas serão restritas e devidamente autorizadas. Nota: Os documentos que descrevem as regras de acesso físico estão descritos no diretório corporativo da Tecnotech no caminho https://wiki.app.sitac.com.br/books/politica-de-acesso-fisico.

Capítulo 18

COMITÊ DE SEGURANÇA DA INFORMAÇÃO (CSI)

A fim de ter os assuntos de segurança da informação e continuidade do negócio sempre em pauta, a diretoria da Tecnotech estabeleceu um Grupo de Gestão multidisciplinar que agrega várias visões corporativas às soluções de Segurança. Esse grupo é composto por representantes de algumas áreas da Tecnotech, com visões isoladas – sob orientação e coordenação direta da diretoria de projetos da Tecnotech. Além do apoio consultivo pontual conforme contrato das consultorias de Segurança da informação e Privacidade de dados. Recomenda-se que o Comitê ocorra pelo menos trimestralmente ou sob demanda convocado pelo Socio diretor. O documento referente ao Comitê está publicado no diretório público da TecnoTech.

Capítulo 19

REQUISITOS LEGAIS E REGULATÓRIOS

O colaborador da TecnoTech deverá receber documentação, no ato de sua contratação, que delimite e defina claramente quais são as atribuições e responsabilidades dentro da empresa referente ao cumprimento da Política de Segurança da Informação. Não obstante, o colaborador deve estar ciente dos riscos de suas atividades, bem como, a importância da informação e seu devido tratamento. Nota: Responsabilidade dos atos ilícitos praticados pelo colaborador deverão ser tratados em conjunto com o departamento jurídico e de recursos humanos da Tecnotech.

Capítulo 20

CÓDIGO DE CONDUTA E TERMO DE ADVERTÊNCIA

O não cumprimento dos requisitos legais e regulatórios estabelecidos pela Tecnotech assim como do Código de Conduta serão cabíveis de advertência. As obrigações dos requisitos, assim como o Termo de Advertência estão descritos e publicados no diretório da área de Recursos humanos e pode ser solicitado pelos gestores das áreas.

Capítulo 21

ANÁLISE ALTA DIREÇÃO

Semestralmente ou quando convocado pelo Diretor Socio deve se reunir os representantes da Alta direção junto com a gestão do comitê de segurança da informação e seus integrantes, para analisar se as políticas, procedimentos e controles estão adequados a realidade da empresa. Nessa análise são revistos os controles e auditorias bem como seus resultados para analisar a pertinência dos mesmos quanto ao momento da empresa e aos objetivos traçados na política de segurança. Faz-se a análise do semestre passado e as adequações necessárias para próximos semestres.

Capítulo 22

MUDANÇAS NA POLÍTICA

A presente versão 1.0 desta Política de segurança da informação foi atualizada pela última vez em: 07/03/2023. O editor se reserva o direito de modificar, a qualquer momento as presentes normas, especialmente para adaptá-las às evoluções, seja pela disponibilização de novas funcionalidades, seja pela supressão ou modificação daquelas já existentes. Esta Política de segurança da informação poderá ser atualizada em decorrência de eventual atualização normativa, razão pela qual se convida o usuário a consultar periodicamente esta seção.

Capítulo 23

CONTROLE DE VERSÕES

Tabela 23.1: Tabela de versões

Versão	Descrição	Responsável	Publicação
1.0	Versão para divulgação	Wanderson câmara - Felipe Andrade	07/03/2023

Capítulo 24

CONCORDÂNCIA

Eu li e entendi a Política de segurança da informação da TECNOTECH SISTEMAS. Entendo que se eu violar as diretrizes estabelecidas nesta Política, posso enfrentar ações legais e/ou disciplinares de acordo com as leis aplicáveis e as normas internas da TECNOTECH SISTEMAS.

Assinatura do funcionário Data