Universidade Federal dos Vales Jequitinhonha e Mucuri
Bacharelado em Sistemas de Informação
SEGURANCA E AUDITORIA DE SISTEMAS DE INFORMAÇÃO

Segurança e Auditoria de Sistemas de Informação
Prof Eduardo Pelli
TPI - Política de Segurança da Informação

Douglas Martins Oliveira Silva
Filipe Fernandes Costa
Rafael Dias Rodrigues

Diamantina - MG
2024

Lista de Figuras

Sumário

1 Descrição da Empresa

A ArtSys Tech é uma empresa de tecnologia focada no desenvolvimento de sistemas web distribuídos para atender às necessidades específicas de gestão acadêmica. Com soluções projetadas para otimizar o cadastro e gerenciamento de artigos científicos, a empresa atua como parceira estratégica de departamentos de computação e instituições acadêmicas que buscam excelência e eficiência na organização de suas produções científicas.

1.1 Público-Alvo

Departamentos de Computação, instituições de ensino superior e centros de pesquisa que necessitam de soluções tecnológicas para gerenciar informações acadêmicas de forma ágil e confiável.

1.2 Serviços Oferecidos

Nosso objetivo é proporcionar soluções tecnológicas que otimizem a organização e o gerenciamento de informações acadêmicas, garantindo eficiência e confiabilidade às instituições atendidas.

Abaixo, alguns dos nossos serviços;

- **Desenvolvimento de Sistemas Web Distribuídos:** Soluções personalizadas para o cadastro, organização e busca de artigos acadêmicos.
- **Integração e Suporte Técnico:** Serviços de integração com outras plataformas acadêmicas e suporte técnico contínuo.
- **Análise de Dados Acadêmicos:** Ferramentas para relatórios e métricas que auxiliem na gestão e visualização da produção científica.
- **Consultoria em Transformação Digital Acadêmica:** Assessoria para digitalizar e modernizar processos acadêmicos relacionados à produção científica.

1.3 Diferenciais

- **Foco Acadêmico:** Conhecimento especializado em gestão de dados acadêmicos.
- **Tecnologias de Ponta:** Uso de arquiteturas distribuídas, escaláveis e seguras para garantir alto desempenho.
- **Atendimento Personalizado:** Soluções alinhadas às demandas específicas de cada instituição.

1.4 Localização

ArtSys Tech opera presencialmente na cidade de Diamantina, atendendo instituições em todo o país, com possibilidade de suporte remoto.

1.5 Slogan

Conectando tecnologia à excelência acadêmica.

1.6 Objetivo

O objetivo desta política é estabelecer as principais diretrizes e controles de Segurança da Informação e Segurança Cibernética a serem implementados por fornecedores da ArtSys Tech , bem como as sociedades controladas direta ou indiretamente por ele. É importante observar que o estabelecimento de diretrizes e controles na relação com os fornecedores do grupo não se limita a esta política, podendo ser definidos novos itens e a revisão destes ao longo de toda a relação contratual.

1.7 Visão

Ser referência no desenvolvimento de sistemas web distribuídos que otimizem a gestão acadêmica, contribuindo para a inovação e excelência na organização de artigos e produção científica.

1.8 Missão

Desenvolver soluções tecnológicas eficientes, seguras e escaláveis para gerenciar o cadastro de artigos em Departamentos de Computação, promovendo a organização, a acessibilidade e a integridade das informações acadêmicas.

1.9 Valores

- **Inovação:** Buscamos continuamente aprimorar nossos sistemas, utilizando tecnologias de ponta para atender às demandas acadêmicas de forma eficiente.
- **Excelência:** Garantimos qualidade em cada etapa do desenvolvimento, entregando soluções confiáveis e de alto desempenho.
- **Colaboração:** Valorizamos o trabalho conjunto com o Departamento de Computação, alinhando nossas soluções às suas necessidades específicas.
- **Transparência:** Agimos com clareza e ética em todas as interações e processos.
- **Sustentabilidade:** Priorizamos a criação de sistemas otimizados, reduzindo desperdícios e promovendo o uso responsável de recursos tecnológicos.

2 Ambiente físico

Nossa planta está organizada de forma que cada área da empresa seja identificada claramente, destacando os setores de desenvolvimento, áreas de trabalho colaborativo e áreas de acesso

restrito. O objetivo dessa disposição é garantir que os funcionários tenham ambientes adequados e seguros para realizar suas atividades, ao mesmo tempo em que a circulação de pessoas é monitorada e controlada, preservando dados e equipamentos sensíveis.

2.1 Planta

Abaixo está uma demonstração da local físico da empresa:

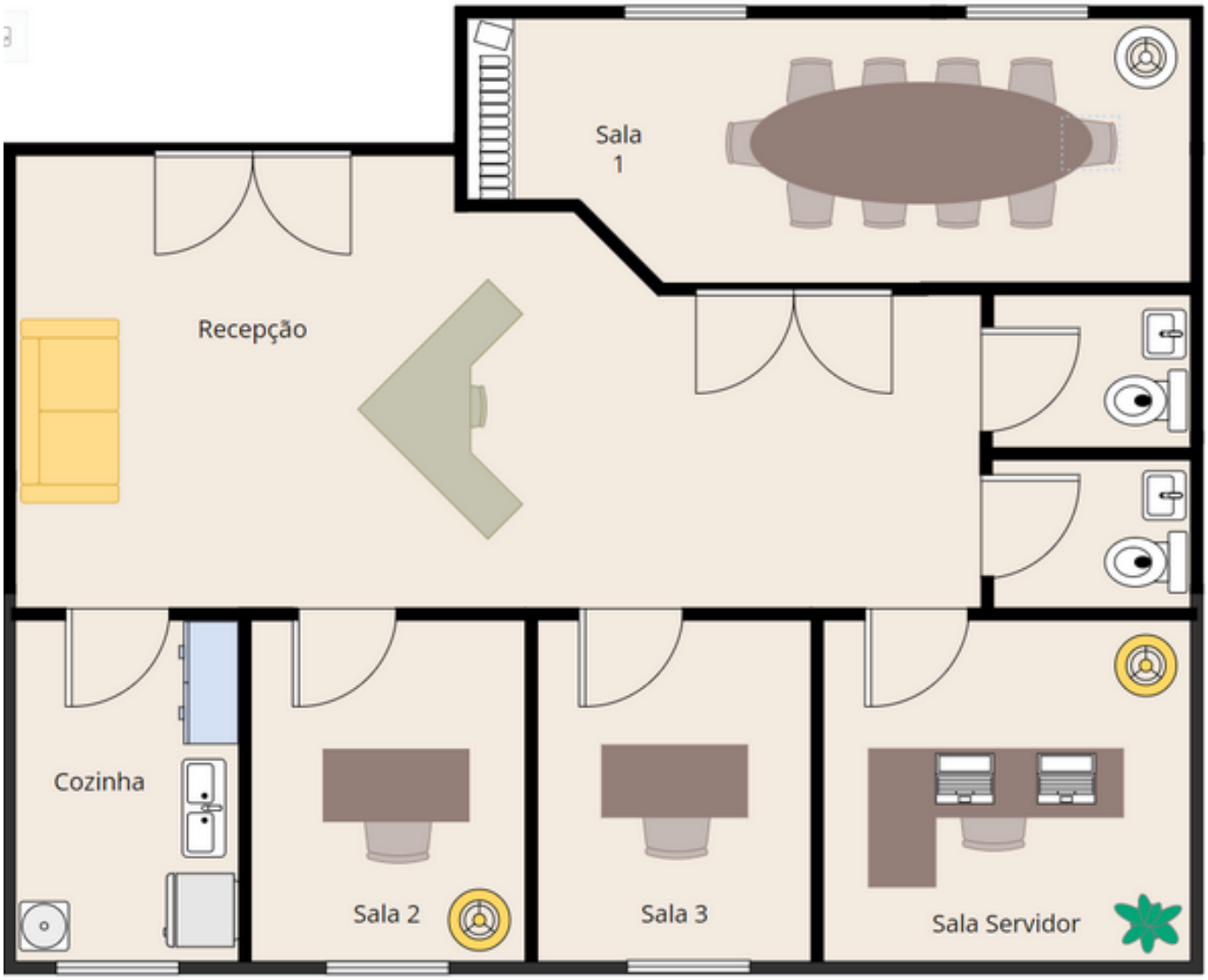

Figura 1: Planta da ArtSys Tech

Ter acesso à planta do ambiente físico permite não apenas uma melhor organização logística e operacional, mas também reforça as políticas de segurança da informação, já que a circulação em áreas críticas pode ser limitada conforme necessário.

3 Vulnerabilidades, principais ameaças, riscos e impactos

Esse tópico é essencial para entender e mitigar os fatores que podem comprometer a segurança da organização.

Ter uma visão clara desses elementos permite que medidas preventivas e reativas sejam adotadas, fortalecendo a resiliência da empresa diante de incidentes de segurança.

3.1 Vulnerabilidades

3.2 Ambiente Físico

3.2.1 Acesso não controlado a instalações:

A ausência de um sistema de controle de entrada eficiente permite que pessoas não autorizadas tenham acesso às áreas internas da empresa, como escritórios e salas de servidores. Sem um mecanismo de autenticação, como crachás, biometria ou registros manuais, o acesso físico fica desprotegido, tornando mais fácil para invasores se infiltrarem. Esses acessos não monitorados podem resultar no roubo de equipamentos ou documentos confidenciais, instalação de dispositivos maliciosos (como keyloggers ou sniffers) ou até mesmo na sabotagem dos sistemas. A falta de registros de entrada e saída também dificulta rastrear atividades suspeitas, prolongando o tempo de resposta em incidentes de segurança.

3.2.2 Equipamentos desprotegidos:

Dispositivos como notebooks, desktops, e periféricos frequentemente contêm informações críticas e podem ser alvos fáceis em um ambiente sem medidas adequadas de proteção. Deixar esses equipamentos expostos em mesas, sem armários ou travas de segurança, aumenta a vulnerabilidade ao roubo ou manipulação indevida. Além disso, em caso de furtos, a ausência de ferramentas de rastreamento ou criptografia nos discos pode levar à exposição de dados sensíveis. Dispositivos móveis, em particular, podem ser levados para fora das instalações e usados em redes inseguras, exacerbando os riscos de comprometimento.

3.2.3 Ausência de monitoramento por câmeras:

A falta de um sistema de vigilância com câmeras em áreas estratégicas, como entradas, saídas, corredores e salas de servidores, impede o registro de atividades suspeitas ou incidentes de segurança. Sem essa vigilância, é impossível identificar quem teve acesso ao local em caso de roubo, vandalismo ou sabotagem. Um sistema de câmeras pode não apenas dissuadir invasores, mas também fornecer evidências para investigações, caso algum incidente ocorra. Sua ausência representa um grande ponto cego na segurança física da empresa.

3.2.4 Falta de backup físico:

Apesar da tendência crescente de armazenar dados na nuvem, os backups físicos ainda são essenciais em casos de falhas catastróficas, como indisponibilidade de servidores remotos ou ataques massivos. A inexistência de um processo de backup físico organizado, utilizando dispositivos como HDs externos ou fitas magnéticas armazenados em cofres ou locais seguros, deixa

os dados expostos a perdas irreparáveis em situações como falhas sistêmicas, desastres naturais ou ataques ransomware.

3.2.5 Desastres naturais não previstos:

Eventos como inundações, incêndios ou tremores podem destruir equipamentos críticos e causar interrupções prolongadas no serviço. A falta de infraestrutura preparada para esses cenários, como sistemas de detecção e combate a incêndios, barreiras contra água ou localização adequada dos servidores, agrava os impactos de tais incidentes. Por exemplo, servidores instalados em andares baixos ficam mais expostos a enchentes, enquanto escritórios sem detectores de fumaça podem ser devastados por incêndios antes que medidas sejam tomadas.

3.2.6 Manutenção inadequada da infraestrutura:

Problemas como cabeamentos desorganizados, refrigeração insuficiente e manutenção elétrica negligenciada podem causar falhas operacionais ou até mesmo acidentes graves. Sistemas de servidores, em particular, exigem condições ambientais controladas, como temperatura e umidade, para operar de forma estável. Sem manutenção adequada, esses fatores podem causar desde quedas intermitentes no serviço até danos permanentes em equipamentos essenciais.

3.2.7 Ambiente físico vulnerável a quedas de energia:

A falta de geradores de emergência ou no-breaks (sistemas de alimentação ininterrupta) deixa a empresa vulnerável a quedas de energia, que podem interromper atividades críticas e causar a perda de dados em dispositivos em uso. Além disso, sistemas desligados de forma abrupta correm o risco de corrupção de arquivos ou danos ao hardware. Esse cenário é agravado em ambientes que dependem de alta disponibilidade para atender a clientes ou realizar operações críticas.

3.3 Ambiente Remoto

3.3.1 Sistemas desatualizados:

Sistemas e aplicativos que não recebem atualizações regulares tornam-se um alvo fácil para atacantes, já que vulnerabilidades conhecidas permanecem expostas. Essas brechas são frequentemente exploradas em ataques automatizados que procuram por sistemas desatualizados na internet. Por exemplo, versões antigas de frameworks de desenvolvimento ou bancos de dados podem conter falhas críticas que permitem a execução de código malicioso ou a extração de dados.

3.3.2 Configurações incorretas de servidores:

Erros de configuração, como permissões excessivas, credenciais padrão ou falta de restrição em portas de comunicação, são uma das principais causas de invasões em sistemas web. Um

servidor mal configurado pode permitir acesso não autorizado a arquivos sensíveis, ou expor interfaces de administração na internet, facilitando ataques. Além disso, logs configurados inadequadamente podem registrar informações confidenciais, expondo ainda mais os dados.

3.3.3 Falta de criptografia robusta:

Sistemas que transmitem dados sem criptografia ou que utilizam métodos frágeis, como SSL desatualizado, tornam informações sensíveis suscetíveis a interceptações. Em redes públicas, por exemplo, um atacante pode capturar senhas, tokens de acesso ou outros dados críticos em trânsito. Isso é particularmente perigoso para aplicações que lidam com informações acadêmicas e pessoais.

3.3.4 Códigos inseguros:

O desenvolvimento de sistemas sem práticas adequadas de segurança, como validação de entradas, é uma porta aberta para ataques como SQL Injection e Cross-Site Scripting (XSS). Um atacante pode explorar essas falhas para acessar ou modificar dados no banco, redirecionar usuários para sites maliciosos ou comprometer a integridade do sistema. A falta de revisão de código ou testes automatizados de segurança agrava essa vulnerabilidade.

3.3.5 Senhas fracas ou padrão:

A utilização de senhas previsíveis, como "admin123" ou "senha", expõe sistemas a ataques de força bruta, nos quais invasores tentam múltiplas combinações até obter acesso. Além disso, o uso de senhas padrão fornecidas por desenvolvedores e não alteradas representa um risco significativo, pois essas credenciais são frequentemente publicadas em listas na internet.

3.3.6 Ausência de monitoramento contínuo:

Sem ferramentas de monitoramento ativo, como SIEM (Security Information and Event Management), as atividades maliciosas podem passar despercebidas. Ataques prolongados, como movimentação lateral dentro da rede ou exploração de vulnerabilidades desconhecidas, só são detectados após causarem danos significativos. Logs de atividades, se não analisados regularmente, tornam-se inúteis em identificar incidentes.

3.4 Ameaças

3.5 Ambiente Físico

3.5.1 Roubo de equipamentos e dados sensíveis:

O furto de dispositivos como servidores, computadores e dispositivos móveis representa uma ameaça significativa à continuidade dos serviços da ArtSys Tech. Equipamentos de TI geralmente armazenam informações críticas, como credenciais, registros acadêmicos e até mesmo

dados financeiros de instituições parceiras. Além disso, o roubo pode comprometer backups físicos, caso não estejam devidamente armazenados. Essa ameaça é ampliada em ambientes sem controle de acesso adequado e pode levar ao vazamento de dados sensíveis, prejudicando a confiança dos clientes e ocasionando possíveis ações legais contra a empresa.

3.5.2 Acesso físico indevido por terceiros:

Pessoas não autorizadas, como visitantes ou prestadores de serviços, podem aproveitar a falta de controle rigoroso para acessar áreas restritas. Esses indivíduos podem obter informações confidenciais, conectar dispositivos de espionagem ou até mesmo comprometer a segurança de sistemas por meio de ações como instalação de malwares em máquinas desprotegidas. Além disso, sem câmeras de vigilância ou registros de entrada e saída, é impossível rastrear a origem de tais incidentes.

3.5.3 Ataques direcionados à infraestrutura:

Indivíduos ou grupos podem direcionar ataques físicos contra a empresa, como cortes intencionais de energia, destruição de cabeamentos ou interrupções de serviços de internet. Esses ataques podem ser realizados por concorrentes desleais, ex-funcionários ou até mesmo por ativistas contrários ao modelo de negócio da empresa. Sem redundância de infraestrutura ou planos de contingência, essas ações podem resultar em paralisação prolongada dos serviços.

3.5.4 Funcionários desatentos:

A negligência de colaboradores em proteger o ambiente físico representa uma ameaça recorrente. Por exemplo, deixar portas destrancadas, esquecer dispositivos eletrônicos expostos ou compartilhar senhas escritas em papéis são comportamentos que aumentam as chances de intrusões. Sem treinamentos regulares de conscientização, esse tipo de comportamento pode comprometer a segurança da empresa de forma contínua.

3.6 Ambiente Remoto

3.6.1 Ataques de phishing direcionados:

E-mails fraudulentos projetados para enganar colaboradores são uma das maiores ameaças digitais. Esses e-mails frequentemente se disfarçam de comunicações legítimas de parceiros ou superiores hierárquicos, solicitando credenciais de acesso ou informações confidenciais. Quando bem elaborados, podem comprometer sistemas inteiros ao induzir usuários a clicarem em links maliciosos ou baixarem arquivos infectados.

3.6.2 Ransomware:

O ransomware é uma ameaça crescente que pode criptografar todos os dados da empresa e exigir um resgate para liberar o acesso. Esse tipo de ataque não apenas paralisa as operações

da empresa, mas também pode levar ao vazamento de informações confidenciais se os dados forem copiados antes da criptografia. Empresas de tecnologia, como a ArtSys Tech, são alvos preferenciais devido à criticidade dos dados que armazenam e à dependência de serviços contínuos.

3.6.3 Exploração de vulnerabilidades de software:

Sistemas com falhas conhecidas podem ser explorados por invasores para obter acesso não autorizado, comprometer dados ou controlar remotamente servidores da empresa. Ataques como SQL Injection e Cross-Site Scripting (XSS) exploram essas vulnerabilidades em aplicativos web, permitindo desde o roubo de informações confidenciais até a interrupção total dos serviços.

3.6.4 Ataques de força bruta:

Tentativas sistemáticas de adivinhar senhas para acessar sistemas críticos representam uma ameaça constante. Essas tentativas podem ser automatizadas e direcionadas a contas administrativas mal protegidas. Uma vez que os invasores obtenham acesso, podem alterar configurações, roubar dados ou implantar malwares, comprometendo a integridade do sistema.

3.6.5 Ataques DDoS (Distributed Denial of Service):

Esse tipo de ataque visa sobrecarregar os servidores da ArtSys Tech, tornando os sistemas indisponíveis para os clientes. Um ataque DDoS bem-sucedido pode prejudicar gravemente a reputação da empresa, especialmente se os clientes perceberem a falha como um reflexo de uma infraestrutura inadequada. Empresas que oferecem serviços de alto desempenho, como a ArtSys Tech, frequentemente se tornam alvos desse tipo de ameaça.

3.6.6 Interceptação de comunicações:

Sem o uso de criptografia robusta, como HTTPS ou VPNs, os dados transmitidos entre usuários e servidores podem ser interceptados por atacantes. Isso inclui credenciais de login, dados pessoais e informações confidenciais dos artigos científicos gerenciados pela empresa. Esse tipo de interceptação pode levar ao vazamento de informações ou à manipulação de dados em trânsito.

3.7 Riscos

3.8 Ambiente Físico

3.8.1 Interrupção das operações devido ao roubo de equipamentos:

O roubo de equipamentos essenciais, como servidores ou dispositivos de armazenamento, pode interromper completamente as atividades da ArtSys Tech. Esse tipo de incidente não apenas paralisa a empresa, mas também gera custos elevados para a reposição de equipamentos e

recuperação de dados. A falta de backups atualizados ou redundância no armazenamento de informações pode agravar o impacto, levando a atrasos significativos na prestação de serviços aos clientes. Além disso, a incapacidade de cumprir prazos pode comprometer relações comerciais com instituições acadêmicas.

3.8.2 Exposição de dados devido ao acesso físico indevido:

O risco de exposição de informações confidenciais aumenta significativamente quando pessoas não autorizadas conseguem acessar áreas restritas. Isso pode incluir acesso a documentos impressos, dispositivos conectados à rede ou até mesmo backups físicos armazenados em locais vulneráveis. A exposição de informações sensíveis, como dados acadêmicos ou credenciais de acesso, pode levar a ações legais contra a empresa e ao comprometimento da privacidade de clientes e parceiros.

3.8.3 Aumento de riscos devido à negligência de funcionários:

Colaboradores que não seguem boas práticas de segurança física aumentam os riscos de incidentes, como roubo de equipamentos ou vazamento de informações. Por exemplo, deixar dispositivos móveis ou laptops desprotegidos em locais públicos ou esquecer portas destrancadas pode resultar em acessos não autorizados. Esse comportamento negligente também pode refletir uma falta de cultura de segurança organizacional, expondo a ArtSys Tech a riscos recorrentes.

3.8.4 Custos de recuperação por vandalismo ou intrusão:

Os danos causados por atos de vandalismo ou intrusão em horários de menor vigilância podem ser significativos. Além dos custos de reparo ou substituição de equipamentos, a empresa pode enfrentar gastos adicionais com reforço de segurança ou contratação de sistemas de monitoramento mais avançados. Esses custos, somados à interrupção das operações, representam um impacto financeiro que pode prejudicar investimentos futuros em inovação e crescimento.

3.9 Ambiente Remoto

3.9.1 Paralisação dos serviços devido a ataques de ransomware:

Os ataques de ransomware podem comprometer completamente os sistemas da ArtSys Tech, tornando todos os dados inacessíveis até que um resgate seja realizado. O risco inclui não apenas a paralisação das operações, mas também a possibilidade de vazamento de informações confidenciais, caso os dados sejam copiados antes da criptografia. Além disso, mesmo após o pagamento do resgate, não há garantia de que os dados serão recuperados, ampliando as perdas financeiras e operacionais.

3.9.2 Vazamento de dados sensíveis por phishing:

Os ataques de phishing representam um risco elevado de comprometimento de informações confidenciais, como credenciais de acesso e dados de clientes. Caso um colaborador caia em uma armadilha, os invasores podem obter acesso aos sistemas internos, roubar informações ou instalar malwares. Isso pode levar a ações judiciais por violação de privacidade e danos à reputação da empresa, além de custos significativos para remediação do incidente.

3.9.3 Perda de confiança devido à exploração de vulnerabilidades de software:

A exploração de falhas em sistemas web, como SQL Injection ou XSS, pode resultar no roubo de informações ou na manipulação de dados críticos. O impacto vai além dos danos financeiros, afetando diretamente a imagem da ArtSys Tech como uma empresa confiável. Instituições acadêmicas, principais clientes da empresa, podem optar por encerrar contratos devido à percepção de insegurança nos serviços oferecidos.

3.9.4 Interrupção do serviço devido a ataques DDoS:

Ataques DDoS podem tornar os sistemas da ArtSys Tech indisponíveis para os clientes, causando insatisfação e possíveis perdas contratuais. Esses ataques frequentemente exigem recursos adicionais para mitigação, como serviços especializados de proteção contra DDoS. A repetição desse tipo de incidente pode prejudicar severamente a reputação da empresa, especialmente entre clientes que dependem de acesso contínuo aos sistemas para gerenciar suas produções científicas.

3.9.5 Exposição de dados por interceptação de comunicações:

Sem a implementação de protocolos seguros, como HTTPS ou criptografia de ponta a ponta, as comunicações entre sistemas e usuários podem ser interceptadas. Isso expõe credenciais de login, dados pessoais e informações acadêmicas sensíveis. O vazamento desses dados pode levar a ações legais contra a ArtSys Tech e comprometer relações comerciais com parceiros estratégicos, além de prejudicar a privacidade dos clientes.

3.9.6 Infecções sistêmicas devido a dispositivos pessoais comprometidos:

Dispositivos pessoais infectados com malwares podem introduzir ameaças diretamente na rede corporativa da ArtSys Tech. Isso inclui a instalação de ransomwares, keyloggers ou outras ferramentas de espionagem. O impacto vai além do comprometimento imediato de sistemas, podendo exigir auditorias completas e a reformulação de políticas de segurança, gerando custos elevados e interrupções prolongadas nas operações.

3.10 Impactos

3.11 Ambiente Físico

3.11.1 Perda financeira direta por roubo ou vandalismo:

A subtração de equipamentos, como servidores, computadores e dispositivos de armazenamento, representa uma perda financeira imediata para a ArtSys Tech. Além dos custos de reposição, a empresa pode enfrentar interrupções nas operações enquanto novos dispositivos são adquiridos e configurados. Se os equipamentos roubados contiverem dados sensíveis ou confidenciais, há o risco de exposição de informações críticas, o que pode gerar penalidades legais e danificar a reputação da empresa no mercado de tecnologia acadêmica.

3.11.2 Interrupção prolongada das operações por desastres naturais:

Incidentes como incêndios, enchentes ou quedas de energia causadas por tempestades podem inutilizar completamente a infraestrutura física da empresa. O impacto não se limita à substituição de equipamentos, mas também afeta a continuidade dos serviços, prejudicando clientes que dependem das soluções da ArtSys Tech. A ausência de um plano de recuperação de desastres pode prolongar os períodos de inatividade, resultando na perda de contratos importantes e na redução da confiança dos clientes.

3.11.3 Comprometimento da reputação por negligência na segurança física:

A falta de controle de acesso a áreas sensíveis pode resultar em incidentes que afetam a imagem da empresa. Por exemplo, invasões físicas ou acessos não autorizados podem expor falhas na política de segurança da ArtSys Tech. Clientes podem questionar a capacidade da empresa de proteger seus próprios ativos e, consequentemente, suas informações acadêmicas, levando à perda de contratos e à redução da base de clientes.

3.11.4 Custos elevados com medidas corretivas pós-incidentes físicos:

Após um incidente físico, como roubo ou vandalismo, a ArtSys Tech pode ser obrigada a investir em reforços de segurança, como câmeras, fechaduras digitais ou vigilância 24 horas. Esses custos adicionais, somados à reposição de equipamentos danificados ou roubados, representam um impacto financeiro significativo. Além disso, a empresa pode precisar alocar recursos humanos para investigar e mitigar os problemas, desviando atenção de atividades estratégicas.

3.11.5 Comprometimento de informações sensíveis em backups físicos:

Se os backups físicos forem armazenados em locais vulneráveis, há o risco de perda ou acesso não autorizado aos dados. Isso pode gerar consequências legais, como multas por não conformidade com regulamentações de proteção de dados, além de prejuízos para os clientes que dependem dessas informações para suas atividades acadêmicas. O impacto na confiabilidade da empresa pode ser duradouro, dificultando a captação de novos clientes no futuro.

3.11.6 Prejuízos relacionados à saúde e segurança dos colaboradores:

Em casos de sabotagem ou vandalismo, os colaboradores podem enfrentar riscos físicos, como ferimentos. Isso não apenas gera impactos éticos, mas também obriga a empresa a lidar com possíveis ações trabalhistas, custos médicos e a necessidade de implementar medidas adicionais de segurança. Colaboradores que se sentem inseguros em seus ambientes de trabalho podem ter sua produtividade reduzida ou até mesmo optar por deixar a empresa, dificultando a retenção de talentos.

3.12 Ambiente Remoto

3.12.1 Prejuízo operacional por credenciais comprometidas:

O comprometimento de credenciais administrativas pode permitir que invasores assumam o controle de sistemas críticos, causando danos à infraestrutura ou acessando dados confidenciais. O impacto imediato é a interrupção das operações, mas as consequências a longo prazo podem incluir custos elevados de mitigação, auditorias de segurança e implementação de novas políticas para evitar incidentes futuros.

3.12.2 Comprometimento de integridade de dados por ataques a vulnerabilidades:

Explorações de vulnerabilidades em sistemas web, como SQL Injection, podem permitir que invasores alterem ou excluam informações críticas armazenadas nos bancos de dados da ArtSys Tech. O impacto inclui não apenas a perda de dados, mas também a necessidade de auditorias e reconciliação de informações, o que pode ser demorado e custoso. Clientes podem perder confiança na integridade dos serviços da empresa, levando à rescisão de contratos.

3.13 Custos elevados com recuperação após infecções por malware:

A introdução de malwares na rede corporativa pode causar danos significativos, desde a corrupção de dados até o comprometimento de sistemas críticos. Os custos para detectar, remover e recuperar sistemas infectados podem ser altos, incluindo horas de trabalho adicionais para equipes de TI e a necessidade de contratar especialistas externos. Esse impacto financeiro pode comprometer investimentos planejados em inovação ou expansão.

4 Diretrizes

A informação constitui-se ativo valioso de extrema importância para a companhia e fundamental para o sucesso do negócio, merecendo, portanto, proteção adequada.

A segurança da informação consiste na adoção de medidas para proteger a propriedade, confidencialidade, disponibilidade e integridade da informação, em qualquer forma e suporte que

se apresente física ou digital, das diversas ameaças existentes, a fim de evitar seu uso indevido, inadequado, ilegal ou em desconformidade com as políticas e os procedimentos internos.

4.1 Segurança em Recursos Humanos

Os programas de conscientização e treinamento devem ser realizados de forma a garantir que todos os colaboradores ("Equipe de Trabalho") assimilem e se comprometam com os princípios e a cultura de Segurança da Informação da ArtSys Tech. A aderência da instituição e de sua Equipe de Trabalho à presente política e às demais normas derivadas deve ser assegurada. A instituição também deve se responsabilizar pelas ações de sua Equipe de Trabalho no uso de dispositivos tecnológicos (ex.: computadores, celulares etc.) e pelo acesso às informações relacionadas a ArtSys Tech, garantindo a segurança das informações durante todo o ciclo contratual.

4.2 Gestão de ativos

Definir categorias para efeitos de classificação da informação e proteção através de controles e diretrizes adequados a cada categoria. A companhia adota quatro categorias:

- Público: É uma informação da ArtSys Tech ou de seus clientes com linguagem e formato dedicado à divulgação ao público em geral, sendo seu caráter informativo, comercial ou promocional. É destinada ao público externo ou ocorre devido ao cumprimento de legislação vigente que exija publicidade da mesma.

- Interno: É uma informação da ArtSys Tech que ela não tem interesse em divulgar, onde o acesso por parte de indivíduos externos à empresa deve ser evitado. Caso esta informação seja acessada indevidamente, poderá causar danos à imagem da Organização, porém, não com a mesma magnitude de uma informação confidencial. Pode ser acessada sem restrições por todos os empregados e prestadores de serviços da TArtSys Tech.

- Confidencial: É uma informação crítica para os negócios da ArtSys Tech ou de seus clientes. A divulgação não autorizada dessa informação pode causar impactos de ordem financeira, de imagem, operacional ou, ainda, sanções administrativas, civis e criminais à ArtSys Tech ou aos seus clientes. É sempre restrita a um grupo específico de pessoas, podendo ser este composto por empregados, clientes e/ou fornecedores.

- Restrita: É toda informação que pode ser acessada somente por usuários da ArtSys Tech explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização.

4.3 Treinamento

A unidades organizacionais da ArtSys Tech devem promover ações de treinamento e conscientização para que os seus colaboradores entendam suas responsabilidades e procedimentos

voltados à segurança da informação e à proteção de dados.

- Parágrafo único: A conscientização, capacitação e sensibilização em segurança da informação devem ser adaptadas aos papéis e responsabilidades dos colaboradores e realizadas trimestralmente.

4.4 Boas práticas de comunicação verbal dentro e fora da empresa

Cuidado ao tratar de assuntos da empresa dentro e fora do ambiente de trabalho, em locais públicos, ou próximos a visitantes, seja ao telefone ou com algum colega, ou mesmo fornecedor.

Evite nomes e tratativas de assuntos confidenciais, nestas situações, fora da empresa ou próximos a pessoas desconhecidas.

Caso seja extremamente necessária a comunicação de assuntos sigilosos em ambientes públicos, ficar atento as pessoas à sua volta que poderão usar as informações com o intuito de prejudicar a imagem da empresa.

4.5 Controle de Acesso Físico

Todos os funcionários receberão crachás específicos de acordo com seu cargo e função na organização, facilitando a identificação e garantindo níveis adequados de acesso físico às dependências da empresa. Cada crachá terá uma distinção visual correspondente ao nível de acesso permitido, refletindo a necessidade de segurança e controle de acesso em áreas restritas.

Será de total responsabilidade dos colaboradores portar seus crachás de forma visível durante todo o período em que estiverem nas instalações, sendo o uso obrigatório como parte das diretrizes de segurança estabelecidas na Política de Segurança da Informação (PSI).

4.6 Monitoramento e Auditoria do Ambiente

A rede, os sistemas, as informações e os serviços utilizados pelos usuários são de exclusiva propriedade da ArtSys Tech, não podendo ser interpretados como de uso pessoal. Todos os empregados da ArtSys Tech devem ter ciência de que o uso da rede, das informações e dos sistemas de informação da ArtSys Tech pode ser monitorado, e que os registros assim obtidos poderão ser utilizados para detecção de violações da Política e dos Enunciados Normativos de Segurança da Informação e, conforme o caso, servir como evidência em processos administrativos e/ou legais.

A qualquer momento, podem ser realizadas inspeções físicas nos equipamentos pertencentes à instituição. Além disso, devem ser instalados sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

4.7 Firewall

O uso de firewalls na rede deve seguir as diretrizes de segurança da informação, garantindo que apenas o tráfego autorizado tenha permissão para acessar os recursos internos. É fundamental que o firewall seja configurado, mantido e monitorado regularmente, registrando os acessos e incidentes para análise.

5 Normas

As normas buscam estabelecer obrigações e procedimentos devem ser definidos de acordo com as diretrizes da Política, estabelecendo regras a serem seguidas em diversas situações em que as informações são tratadas.

5.1 Autenticação e Controle de Acesso

Todos os usuários da empresa devem possuir uma identificação única e pessoal para acessar os sistemas internos, tanto para a versão física quanto para a online. A autenticação multifatorial (MFA) é obrigatória para todos os acessos remotos, garantindo que o processo de login seja seguro.

A Gerência de Segurança da Informação será responsável por gerenciar os acessos, garantindo que apenas funcionários autorizados tenham permissões para determinadas funções e sistemas. O não cumprimento dessa norma poderá resultar em sanções disciplinares.

5.2 Controle de Acesso Lógico (Baseado em senhas)

Todo usuário deve ter uma identificação única, pessoal e intransferível, qualificando-o como responsável por qualquer atividade desenvolvida sob esta identificação. O titular assume a responsabilidade quanto ao sigilo da sua senha pessoal.

5.3 Controle de Acesso Físico

O acesso às instalações físicas da empresa será restrito a colaboradores e prestadores de serviços autorizados. A entrada nas dependências será monitorada por sistemas de controle de acesso, como crachás ou biometria, que registrarão a hora de entrada e saída de cada indivíduo. Os visitantes deverão ser acompanhados por um colaborador durante todo o período de permanência nas dependências da empresa. A manipulação e cópia dos sistemas de controle de acesso será tratada como uma violação grave da política de segurança.

5.4 Proteção de Dados Sensíveis

A empresa deve garantir que todos os dados sensíveis, como informações financeiras, dados de clientes e informações de empregados, sejam armazenados apenas em sistemas seguros e cripto-

grafados. O acesso a esses dados será restrito a colaboradores autorizados, de acordo com suas funções específicas.

O vazamento ou manipulação indevida desses dados, por qualquer colaborador, resultará em medidas disciplinares severas, conforme a gravidade do incidente.

5.5 Uso de Dispositivos Móveis

Todos os dispositivos móveis corporativos, incluindo notebooks, tablets e smartphones, devem ter criptografia de disco ativada para proteger os dados em caso de roubo ou perda do equipamento.

A equipe de Gerência de Infraestrutura e Suporte da ArtSys Tech, será responsável por garantir que a criptografia seja configurada corretamente, e todos os dispositivos devem ser rastreáveis. Além disso, os colaboradores devem manter os dispositivos protegidos com senhas ou biometria e não devem deixar os dispositivos desacompanhados em locais públicos ou inseguros.

Os colaboradores e prestadores de serviços devem notificar o departamento técnico sobre qualquer dispositivo desconhecido ou não autorizado conectado ao seu computador;

É proibido alterar ou abrir manuais dos equipamentos de informática sem a presença ou permissão do responsável.

5.6 Uso da Rede

Arquivos pessoais que não estejam relacionados ao trabalho da ArtSys Tech, como fotos, vídeos e músicas, não devem ser salvos ou transferidos para a rede, para evitar sobrecarga no sistema de armazenamento.Caso esses arquivos sejam identificados, serão deletados sem aviso prévio.

Diretórios ou pastas de acesso público não devem ser utilizados para armazenar documentos que contenham informações confidenciais ou de caráter específico. Apenas dados de interesse geral podem ser guardados nesses locais.

Documentos essenciais para as atividades dos colaboradores da ArtSys Tech devem ser salvos na rede. Os arquivos que são mantidos localmente em computadores (como no disco C:) não têm garantia de backup e podem ser perdidos em caso de falha do equipamento, sendo de inteira responsabilidade do usuário.

Colaboradores e prestadores de serviços da ArtSys Tech, especialmente aqueles com contas privilegiadas, estão proibidos de executar comandos que possam sobrecarregar os serviços de rede da empresa, a menos que previamente solicitados e autorizados pela Gerência de Infraes-

trutura e Suporte.

5.7 Uso da Internet

A Internet corporativa deve ser utilizada exclusivamente para fins corporativos, enriquecimento intelectual ou como ferramenta de busca por informações, enfim, tudo que possa vir a contribuir para o desenvolvimento de atividades relacionadas à empresa. O uso da internet para assuntos pessoais (home banking, lojas virtuais e afins) é permitido, com limitações, desde que com bom senso e respeitando as demais diretivas corporativa.

Não é permitido os acessos a sites impróprios na Internet, incluindo, mas não se limitando a: jogos, mensagens de corrente, troca ou armazenamento de conteúdo ilícito, obsceno, pornográfico, violento, discriminatório, racista, político, religioso, difamatório ou que desrespeite qualquer indivíduo ou entidades, de acordo com as Leis nº 8.069 (Estatuto da Criança e do Adolescente) e nº 12.965 (Marco Civil da Internet).

Os acessos a internet corporativa são monitorados através de identificação do usuário, podendo ser bloqueados a qualquer momento, sem aviso prévio, pela equipe de tecnologia ou segurança da informação, quando for identificado alguma irregularidade ou risco ao ambiente.;

5.8 Datacenter

Toda entrada no Datacenter, via sistema de autenticação, deve ser registrada, incluindo o usuário, a data e a hora, utilizando um software apropriado para esse controle.

O acesso por chave física só será permitido em casos de emergência, quando houver comprometimento da segurança do Datacenter, como em situações de incêndio, inundação ou danos estruturais, ou se o sistema de autenticação estiver indisponível.

5.9 Backup (Cópia de Segurança)

A empresa deve realizar backup completo de todos os dados corporativos, incluindo sistemas, bases de dados e arquivos essenciais, uma vez por semana. Esses backups devem ser armazenados em local seguro, com acesso restrito apenas a pessoas autorizadas. Além disso, testes de recuperação de dados devem ser realizados trimestralmente para garantir que a integridade dos backups seja validada.

A recuperação de dados somente será possível mediante a solicitação formal e aprovação do dono da informação ou gestor imediato.

A responsabilidade pela execução desses procedimentos fica a cargo da equipe de Tecnologia da Informação, que deve seguir os procedimentos documentados.

5.10 Criptografia

Deve haver um processo de criptografia de disco em todos os notebooks e dispositivos móveis corporativos, para proteger quanto a confidencialidade das informações e possíveis vazamentos de dados derivados de perda ou roubo dos equipamentos. Toda aplicação que contenha informações da empresa e esteja hospedada em ambiente externo deve suportar comunicação com protocolo seguro (https) e criptografia forte no tráfego dos dados;

5.11 Uso de Firewalls e Segurança de Rede

Todos os sistemas da empresa, sejam físicos ou online, devem ser protegidos por firewalls configurados de acordo com as diretrizes de segurança. A configuração do firewall deve ser revisada regularmente para garantir que apenas o tráfego autorizado tenha permissão para acessar recursos internos. A equipe de TI será responsável pela manutenção e monitoramento desses firewalls, garantindo a detecção e bloqueio de acessos não autorizados ou suspeitos.

5.12 Segurança em Ambiente Online

Todas as aplicações web da empresa, tanto internas quanto voltadas para o cliente, devem ser configuradas para usar criptografia SSL/TLS (HTTPS), garantindo a segurança da comunicação de dados entre o servidor e os usuários. A equipe de TI deve garantir que todas as conexões sejam feitas por meio de protocolos seguros e que as chaves de criptografia sejam mantidas em segredo. Qualquer aplicativo que não suporte comunicação segura será bloqueado.

6 Procedimento

Instrumentalizam o disposto nas Normas e na Política, permitindo sua aplicação direta nas atividades da organização.

6.1 Procedimento de Criação de Senha

- Utilizar senha com pelo menos oito caracteres contendo números, letras maiúsculas e minúsculas e caracteres especiais, e não deverá utilizar informações pessoais fáceis de serem obtidas como, o nome, o número de telefone ou data de nascimento como senha.
- Não incluir senhas em processos automáticos de acesso ao sistema, por exemplo,armazenadas em macros ou teclas de função.
- A distribuição de senhas aos usuários de TI (inicial ou não) deve ser feita de forma segura. A senha inicial, quando gerada pelo sistema, deve ser trocada, pelo usuário de TI no primeiro acesso.

6.2 Procedimento de Backup

O procedimento de backup envolve o uso de ferramentas automatizadas para realizar cópias de segurança de todos os sistemas e dados críticos todas as noites. A equipe de TI é responsável por agendar os backups para a madrugada, quando a carga nos servidores está menor. Após cada backup, a equipe deve verificar os logs para garantir que não houve falhas. Além disso, uma vez por mês, a equipe realiza um teste de recuperação de dados em uma estação de trabalho separada para garantir que o backup é funcional.

6.3 Procedimento de Recuperação de Dados

Quando uma falha no sistema resulta na perda de dados importantes, a equipe de TI deve verificar a última cópia de segurança para garantir que os dados possam ser restaurados. Se a recuperação for necessária, a equipe segue um passo a passo, começando pela identificação do sistema afetado, seguida pela localização do backup relevante. Os dados são restaurados em um servidor de testes para garantir que estão íntegros, antes de serem movidos para o ambiente de produção.

6.4 Procedimento de Acesso ao Datacenter

O acesso ao Datacenter deve ser acessado apenas por meio de sistemas de autenticação, como biometria ou cartões magnéticos de controle de acesso.

6.5 Procedimento de Gestão de Incidentes de Segurança

Caso um incidente de segurança seja identificado (como um vazamento de dados ou ataque cibernético), o colaborador que detectar a ameaça deve imediatamente comunicar à equipe de segurança de TI. A equipe irá iniciar o processo de contenção, que pode envolver a desconexão de dispositivos comprometidos, isolando áreas da rede e bloqueando contas suspeitas. A equipe documenta cada etapa tomada e realiza uma análise de causa raiz após a contenção do incidente, para evitar que se repita.

6.6 Procedimento Criação de Novos Usuários

Deve ocorrer uma solicitação formal feita pelo gestor ao departamento de TI, contendo dados do colaborador, função e nível de acesso necessário. Após aprovação, o TI realiza o cadastro, atribuindo login e senha inicial, configurados segundo o princípio do menor privilégio.

As credenciais são entregues de forma segura, e o usuário deve alterar a senha no primeiro acesso, seguindo as diretrizes de segurança. Antes de usar os sistemas, é necessário participar de um treinamento básico sobre segurança e assinar um termo de responsabilidade. Todas as etapas do processo são documentadas para auditoria e conformidade.

6.7 Procedimento Exclusão de Usuários

Deve ser feita uma solicitação formal do gestor responsável ao departamento de TI, justificando a necessidade da remoção e indicando os sistemas ou serviços que devem ser desativados. Após validação da solicitação, o TI deve revogar imediatamente o acesso do usuário, garantindo que ele não possa mais acessar os recursos da empresa.

As credenciais e permissões atribuídas ao usuário devem ser removidas de todos os sistemas e registros, incluindo e-mails, ferramentas corporativas e acessos físicos, se aplicável. Caso o usuário tenha arquivos ou informações importantes armazenados, o gestor ou responsável deve solicitar previamente sua transferência ou backup.

Todas as etapas da exclusão devem ser registradas e arquivadas para auditoria, garantindo conformidade com a Política de Segurança da Informação

6.8 Procedimento de Controle de Acesso Físico

Quando um colaborador precisa acessar áreas restritas, como o data center, ele deve passar pela portaria onde será verificado o seu cartão de identificação. Caso o cartão seja válido, a portaria autoriza o acesso. O colaborador deve se registrar no livro de visitantes e acompanhar um responsável do setor até a área restrita. Em caso de falha no sistema de controle de acesso, o responsável pelo setor deve ser contatado para autorizar manualmente o acesso.

6.9 Procedimento de Controle de Acesso Remoto

Para garantir que o acesso remoto à rede corporativa seja feito de maneira segura, o colaborador deve utilizar uma VPN (Rede Privada Virtual) configurada pela equipe de TI. Antes de acessar a rede, o colaborador deve verificar que seu dispositivo está atualizado com patches de segurança. Quando o acesso remoto for necessário, o colaborador deve autenticar-se utilizando um código de autenticação multifatorial. Após o término da tarefa, o colaborador deve desconectar-se da rede e apagar qualquer dado sensível armazenado temporariamente no dispositivo.

Todos os sites e serviços corporativos devem ser configurados para utilizar certificados SSL/TLS válidos, garantindo a transmissão criptografada de informações. O servidor deve ser configurado para forçar o uso de HTTPS e desabilitar protocolos antigos e inseguros. A validade dos certificados será monitorada e renovada conforme necessário para evitar falhas de segurança.

6.10 Procedimento de Monitoramento de Rede

Para monitorar a segurança da rede, a equipe de TI deve usar um software de monitoramento contínuo, que registrará todas as tentativas de acesso, tentativas de login e qualquer tráfego

anômalo. Quando uma atividade suspeita for detectada, o sistema enviará uma notificação imediata à equipe de segurança. A equipe deverá então investigar o incidente, realizando a análise forense e, caso necessário, bloqueando IPs ou usuários suspeitos de atividades maliciosas.

6.11 Procedimento de Atualizações de Software

A equipe de TI deve garantir que todos os sistemas e aplicativos da empresa sejam atualizados com as últimas correções de segurança (patches) dentro de 72 horas após a liberação pelo fornecedor. Isso inclui sistemas operacionais, software de segurança e aplicativos críticos utilizados pela empresa. As atualizações devem ser testadas em um ambiente controlado antes de serem implementadas em produção para evitar possíveis falhas. Caso uma atualização falhe ou cause problemas, a equipe de TI deve ser capaz de reverter para uma versão anterior do software sem comprometer a segurança.

7 Sanções

O não cumprimento das normas e diretrizes estabelecidas neste documento, bem como em suas normas complementares, será considerado uma falta grave. Em caso de infrações, a Terracap adotará as medidas cabíveis nos âmbitos administrativo, civil e judicial, de acordo com a gravidade e as circunstâncias do incidente.

As seguintes ações são consideradas contrárias à Política de Segurança da Informação da Terracap, sujeitando os responsáveis às sanções apropriadas:

1. **Ações Irregulares com Intenção de Obter Vantagem Indevida:** Praticar qualquer ato que cause prejuízo à Terracap ou que tenha como objetivo obter lucro ou vantagem, seja para o próprio colaborador ou para terceiros, constitui violação grave. Isso inclui abusos de confiança, erros ou prejuízos sem justificativa razoável, uso indevido de senhas ou processos de identificação de terceiros, bem como o uso de meios fraudulentos.

2. **Manejo Indevido de Informações e Sistemas:** Qualquer comportamento que envolva omissão ou falha no tratamento adequado de informações, documentos físicos, sistemas e redes de dados será tratado como infração. A violação das normas de segurança em relação à guarda e manipulação de informações sensíveis prejudica diretamente a Terracap e seus colaboradores.

3. **Uso Indevido dos Recursos da Empresa:** O uso de recursos da Terracap, como sistemas, equipamentos ou redes, para fins exclusivamente pessoais é uma violação da política interna. Esses recursos devem ser utilizados única e exclusivamente para as atividades profissionais relacionadas à função de cada colaborador.

4. **Destruição ou Modificação Indevida de Dados:** Apagar, destruir ou modificar dados, programas de computador ou documentos físicos sem a devida autorização constitui

uma infração grave. Isso inclui a inutilização total ou parcial de informações ou sistemas, comprometendo a integridade e a operação dos mesmos.

5. **Acesso Indevido a Sistemas e Informações:** Obter ou manter acesso não autorizado a dados, computadores, redes ou meios de identificação, como crachás e senhas, é um ato de infração. A entrega de acesso indevido a terceiros ou a manutenção de credenciais não autorizadas também são infrações graves.

6. **Obtenção Indevida de Informações Sigilosas:** O acesso não autorizado a segredos, informações confidenciais ou dados para os quais o colaborador não tenha permissão de acesso é uma violação significativa. Isso inclui informações armazenadas em sistemas digitais, bem como documentos físicos, que pertencem à Terracap.

7. **Criação ou Inserção de Dados Maliciosos:** Qualquer ação que envolva a criação ou inserção de programas ou dados com a intenção de modificar, destruir ou inutilizar informações em sistemas da Terracap é considerada uma violação severa. Isso inclui a introdução de códigos maliciosos ou de qualquer outra forma que prejudique a funcionalidade dos sistemas.

8. **Download ou Upload de Conteúdos Inapropriados:** Realizar o download ou upload de jogos, filmes, conteúdos pornográficos ou qualquer outro material que não tenha relação com as atividades da Terracap é proibido. O uso de recursos corporativos para atender interesses pessoais que não estejam alinhados com as atividades da empresa constitui uma infração.

9. **Distribuição Não Autorizada de Conteúdo da Empresa:** Distribuir cópias não autorizadas de arquivos, informações ou software da Terracap é uma violação grave da política interna, comprometendo a segurança e os direitos de propriedade intelectual da empresa.

10. **Envio de Mensagens Inapropriadas por Correio Eletrônico:** Utilizar os serviços de correio eletrônico da empresa para enviar mensagens de teor político, racista, preconceituoso, comercial, pornográfico, pejorativo ou publicitário é estritamente proibido. Essas ações comprometem a imagem da Terracap e violam as normas de conduta.

11. **Fraude ou Tentativa de Burlar os Sistemas de Segurança:** Qualquer tentativa de fraudar ou burlar os sistemas de segurança da informação implementados pela Terracap, seja para obter acesso não autorizado ou para prejudicar a operação dos mesmos, é considerada uma infração gravíssima.

12. **Desvio de Conduta em Relação aos Padrões de Uso dos Recursos de Rede:** Agir em desacordo com os padrões e procedimentos específicos estabelecidos para o uso dos recursos e serviços de rede corporativa também configura uma violação. Isso inclui desrespeitar as regras sobre acessos, transferências de dados ou comportamentos que afetem a segurança da rede.

7.1 Aplicação das Sanções

As sanções aplicáveis aos comportamentos listados acima podem variar dependendo da gravidade da infração, podendo incluir advertências, suspensão, demissão, e até mesmo medidas legais, se necessário. A Terracap se reserva o direito de adotar as ações corretivas e disciplinares de acordo com as circunstâncias e a legislação vigente.

Essas medidas visam proteger a integridade, confidencialidade e disponibilidade das informações e recursos da Terracap, além de garantir que todos os colaboradores atuem em conformidade com as diretrizes estabelecidas na Política de Segurança da Informação.

8 Vigência e validade

A presente política passa a vigorar a partir da data de sua homologação e publicação, sendo válida por tempo indeterminado.