UNIVERSIDADE FEDERAL DOS VALES DO JEQUITINHONHA E MUCURI
Faculdade de Ciências Exatas (FACET)
Departamento de Computação

Iago Mateus Avila Fernandes
Lucas Alexsander Barbosa Cruz
Mariano Carlos Silva
Mateus Henrique Machado
Rafael Lucas Fernandes Soares

Segurança e Auditoria de Sistemas de Informação:

Contexto e proposta de Política de Segurança da Informação para a empresa de venda de répteis Reptilândia

Diamantina - MG

2024

SUMÁRIO

PARTE I: O contexto da empresa Reptilândia

1. Informações gerais

A Reptilândia é uma empresa de **pequeno porte** que se dedica à **venda legalizada de animais exóticos**, com foco no comércio de répteis. Com uma equipe composta por **20 funcionários**, a empresa estrutura suas atividades em diferentes diretorias e gerências. O organograma a seguir evidencia a estrutura da empresa com base nas funções exercidas por seus membros colaboradores.

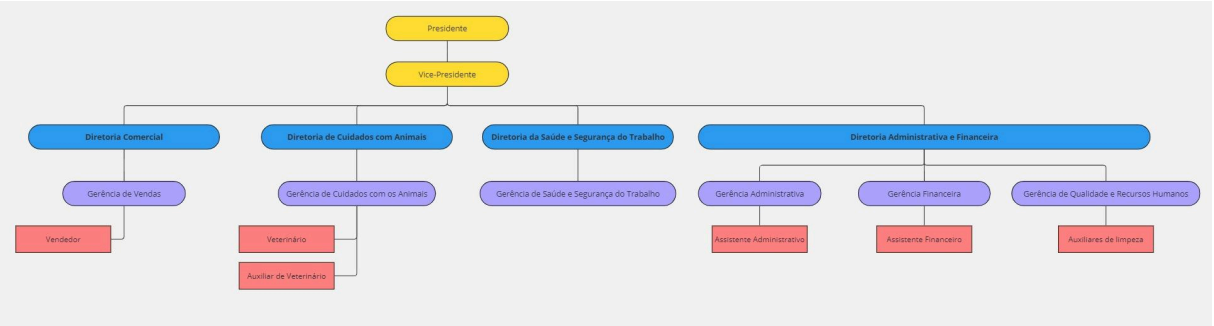

Figura 1: Organograma da Reptilândia

Para a execução de suas atividades, a Repitlândia conta com um sistema de gestão de vendas utilizado somente por seus funcionários. Esse sistema permite o acompanhamento e registro de vendas, dos animais em estoque e dos clientes.

2. Ambiente físico

O ambiente físico da Reptilândia é composto por uma única instalação na qual são realizadas as atividades de venda, cuidado dos animais e funções administrativas. No lobby são concentradas todas as atividades relativas a vendas, sendo a única área de acesso permitido ao cliente. Essa área contém os displays de animais, banheiros e a ilha de caixa onde as compras são efetuadas, que por sua vez, contém os equipamentos necessários para a gestão das vendas.

Já no segundo quadrante do ambiente físico, estão concentradas as atividades relativas à manutenção do negócio e cujo acesso é restrito aos clientes. Nessa área se encontram a enfermaria, a cozinha, banheiros para funcionários, escritório administrativo e sala de servidores. Os funcionários que não lidam com as vendas executam suas funções na

enfermaria e no escritório em um espaço de coworking. Por sua vez, a sala de servidores é acessível somente ao passar pelo escritório. As figuras a seguir ilustram a estrutura física da empresa.

Figura 2: Planta 2D com marcações das regiões do ambiente físico da Reptilândia

Figura 3: Representação 3D da estrutura física da Reptilândia

3. Infraestrutura

A lista a seguir lista os recursos e serviços fundamentais para o funcionamento e desempenho das funções empresariais da Reptilândia.

a. Servidores de rede e backup
b. Computadores
c. Câmeras de segurança
d. Celulares e dispositivos móveis
e. Sistema de ponto eletrônico
f. Sistema de ventilação e refrigeração
g. Aquários e terrários
h. Sistemas de aquecimento e iluminação
i. Instalações de enfermaria veterinária
j. Equipamentos de proteção individual
k. Nobreaks
l. Fechadura de cartão magnético

4. Plano de negócio

4.1. Missão

Fornecer aos nossos clientes uma variedade de répteis de origem legal e saudável, enquanto promovemos a educação sobre o cuidado adequado desses animais únicos. Estamos comprometidos em garantir o bem-estar de todos os nossos animais e fornecer um serviço excepcional e seguro ao cliente.

4.2. Visão

Ser reconhecida como a principal loja de répteis, destacando-se pela qualidade dos nossos animais, pelo nosso compromisso com a educação do cliente e pela nossa contribuição para a conservação de espécies exóticas. Nós nos esforçamos para estabelecer padrões na indústria de animais exóticos, promovendo práticas éticas e sustentáveis.

4.3. Valores

- **Bem-estar animal:** Colocamos o bem-estar dos nossos animais acima de tudo. Nos comprometemos a fornecer a eles o melhor cuidado possível e a educar nossos clientes sobre como fazer o mesmo.
- **Educação**: Acreditamos que a educação é a chave para garantir que nossos clientes possam cuidar adequadamente de seus novos animais de estimação. Oferecemos recursos educacionais e estamos sempre disponíveis para responder a perguntas.
- **Ética**: Operamos de maneira ética em todas as áreas do nosso negócio. Isso inclui garantir que todos os nossos animais possuem chips e sejam adquiridos legalmente e tratados com respeito.
- **Segurança**: Priorizamos a segurança dos nossos animais e clientes. Isso inclui manter instalações seguras e seguir todas as diretrizes de saúde e segurança física e digital.
- **Responsabilidade**: Reconhecemos a responsabilidade que vem com a venda de animais exóticos. Trabalhamos para garantir que cada animal vendido vá para um lar onde será bem cuidado e valorizado. Assim, cada venda é acompanhada de um comprovante e de animais com chips.

5. Vulnerabilidades, ameaças e riscos

A partir do contexto da empresa Reptilândia e do estado atual do sistema, o quadro a seguir lista as vulnerabilidades, ameaças e riscos/impactos associados e identificados.

Quadro 1: Vulnerabilidades, ameaças e riscos no contexto da Reptilândia

Vulnerabilidade	Ameaça	Riscos/Impactos
Falta de um sistema de backup adequado	Perda de dados críticos devido a falhas no sistema, erros humanos ou ataques	Interrupção das operações comerciais, perda de confiança do cliente, custos financeiros para recuperação de dados
Acesso não autorizado aos servidores ou computadores da loja	Roubo de dados, danos ao hardware, instalação de software malicioso	Interrupção das operações, perda de dados, custos de reparação ou substituição de equipamentos
Falta de treinamento em segurança cibernética para os funcionários	Funcionários podem permitir o acesso a sistemas ou informações sensíveis através de phishing ou outras táticas de engenharia social	Violação de dados, perda de confiança do cliente, possíveis multas por violações de privacidade
Sistema web não atualizado regularmente	Exploração de vulnerabilidades conhecidas por hackers	Violação de dados, interrupção do serviço, danos à reputação da empresa
Uso de senhas fracas ou compartilhadas entre os funcionários	Acesso não autorizado aos sistemas da empresa	Violação de dados, perda de confiança e integridade da informação
Falta de criptografia para dados sensíveis	Interceptação e leitura de dados durante a transmissão	Alteração indevida em dados, perda de confiança e danos à imagem da empresa
Falta de um plano de resposta a incidentes de segurança	Inabilidade de responder adequadamente a uma violação de segurança, resultando em maior dano	Perda prolongada de serviço, danos à reputação da empresa, custos financeiros elevados

Vulnerabilidade	Ameaça	Riscos/Impactos
Falta de monitoramento e auditoria regular dos logs do sistema	Atividades suspeitas ou maliciosas podem passar despercebidas	Violação de dados, interrupção do serviço, danos à reputação da empresa
Falta de controle de acesso baseado em função	Funcionários com acesso excessivo podem causar danos (intencionais ou não) aos sistemas ou dados	Violação de dados, interrupção do serviço, confusão operacional
Falta de medidas de segurança adequadas para proteger os dados dos clientes	Violação de dados que resulta na exposição das informações pessoais dos clientes	Perda de confiança do cliente, danos à reputação da loja, possíveis multas por violações de privacidade
Falta de um processo de autenticação forte para o sistema de gestão de vendas	Acesso não autorizado ao sistema	Violação de dados, alterações não autorizadas nos registros de vendas ou estoque, perda de confiança do cliente
Armazenamento inseguro de senhas	Ataque de força bruta	Acesso não autorizado ao sistema
Falta de validação de entrada de dados	Injeção de SQL	Manipulação ou acesso não autorizado aos dados do banco de dados
Configurações padrão inseguras deixadas intactas	Exploração dessas configurações por atores mal-intencionados	Acesso não autorizado ao sistema ou aos dados
Falta de isolamento de rede adequado	Se um sistema for comprometido, o invasor pode ter acesso a outros sistemas na mesma rede	Comprometimento de vários sistemas, perda ou vazamento de dados em larga escala
Falta de procedimentos claros para a remoção segura de dados de dispositivos antigos ou descartados	Recuperação de dados sensíveis de dispositivos descartados	Violação de dados, perda de confiança do cliente, possíveis multas por violações de privacidade

Vulnerabilidade	Ameaça	Riscos/Impactos
Falta de controle sobre o uso de dispositivos pessoais para acessar o sistema da loja	Violação de dados através de dispositivos pessoais infectados ou perdidos	Violação de dados, perda de confiança do cliente, possíveis multas por violações de privacidade
Falta de um sistema de detecção e prevenção de intrusões	Ataques cibernéticos não detectados e não mitigados	Violação de dados, interrupção do serviço, danos à reputação da empresa
Falta de planejamento adequado da rede elétrica	Curtos circuitos provocados por sobrecarga	Interrupção das atividades, corrosão dos dados e servidores, inutilização dos equipamentos

PARTE II: Política de Segurança da Informação

1. Objetivo

Definir diretrizes e normas visando a proteção de informações sob posse da Reptilândia a partir dos pilares de confidencialidade, integridade e disponibilidade. Além disso, busca garantir que qualquer informação, independente do formato ou mecanismo de armazenamento, será protegida de forma adequada contra ameaças de caráter interno, externo, intencional e/ou acidental.

Este documento objetiva definir responsabilidades e fornecer orientações necessárias aos funcionários e parceiros sobre o uso correto e seguro de informações e recursos tecnológicos que fazem parte do exercício da atividade profissional da Reptilândia. Ainda, busca se adequar à legislação vigente e aos contratos aplicáveis à segurança e privacidade da informação, garantindo continuidade do negócio e minimização de danos causados por incidentes de segurança da informação.

Por fim, esta Política de Segurança da Informação atua em conformidade com os interesses estratégicos e empresariais da Reptilândia, em busca de minimizar danos sobre a imagem, participação no mercado, confiança dos clientes e parceiros e continuidade das atividades.

2. Público alvo

Aplica-se a toda e qualquer pessoa que possua acesso às informações e recursos tecnológicos da Reptilândia, incluindo funcionários, prestadores de serviço e/ou terceiros autorizados.

3. Política de Uso Aceitável

Os funcionários devem usar os sistemas e recursos de tecnologias de informação da empresa de maneira responsável e ética. Isso inclui evitar atividades que possam colocar a segurança da rede em risco, como visitar sites inseguros ou baixar software não autorizado.

Qualquer violação da política de uso aceitável será tratada como uma violação série e poderá resultar em ações disciplinares.

4. Responsabilidade

A qualquer pessoa - funcionário, prestador de serviço ou terceiro autorizado -, é atribuída a responsabilidade de adesão e efetivação da Política de Segurança da Informação descrita no presente documento. Essa responsabilidade inclui a obrigação de proteger as informações e os recursos tecnológicos sob posse da Reptilândia e que possui acesso, assim como a de reportar incidentes e violações de segurança assim que forem observados.

O monitoramento, revisão e atualização da política são atividades do Comitê de Segurança da Informação da Reptilândia, que também será responsável pela investigação de violações e respostas aos possíveis incidentes.

Por fim, qualquer violação à política definida neste documento estará sujeita a ações disciplinares conforme a política interna da Reptilândia e da legislação vigente.

5. Diretrizes Gerais

5.1. Classificação e Tratamento da Informação

Todas as informações devem ser produzidas, mantidas e compartilhadas de acordo com os objetivos estratégicos do negócio, suas necessidades e apenas por meio de recursos autorizados.

Todas as informações referentes ao exercício das atividades da Reptilândia devem ser protegidas e ter seu acesso garantido apenas a pessoas autorizadas e nos momentos necessários.

Toda e qualquer informação necessária ao funcionamento da empresa será tratada como sensível e prioritária.

5.2. Controle de Acesso

Serão utilizadas medidas de segurança física e logicamente adequadas para proteger as informações e recursos tecnológicos da Reptilândia.

O acesso às informações e recursos seguirá o princípio do menor privilégio, fornecendo ao usuário somente o absolutamente necessário para o exercício de suas funções.

5.3. Segurança em Recursos Humanos

A Reptilândia se compromete a fornecer o conhecimento necessário sobre segurança da informação para todos os seus funcionários, os tornando aptos a reconhecer falhas e vulnerabilidades.

Todos os funcionários também deverão se tornar cientes desta Política de Segurança da Informação e de todas as suas atualizações ao longo do tempo.

5.4. Monitoramento e Sanções

O uso dos recursos tecnológicos da Reptilândia serão monitorados e quaisquer descumprimento das obrigações ou violações que coloquem em risco a integridade das informações serão tratadas com seriedade, sendo aplicadas sanções conforme a natureza da violação.

5.3. Segurança do Ambiente

A Reptilândia se compromete a garantir que o projeto das áreas de trabalho sejam feitos de forma a minimizar o risco de dano aos equipamentos e ativos, considerando questões da segurança física e garantia da disponibilidade dos recursos a qualquer momento.

6. Diretrizes Específicas

6.1. Tratamento das Informações e Recursos Tecnológicos

6.1.1. Normas Relativas ao Tratamento das Informações e Recursos Tecnológicos

Devem ser definidas categorias de relevância e sensibilidade das informações, que serão utilizadas para a definição dos direitos de acesso para cada funcionário conforme a necessidade.

Devem ser definidas categorias de usuários com base nas responsabilidades e funções exercidas pelos membros da Reptilândia.

Toda e qualquer informação produzida e armazenada na Reptilândia deverá ser utilizada somente para fins que atendam aos objetivos profissionais e estratégicos da empresa.

Toda e qualquer informação utilizada pela Reptilândia para o exercício de suas atividades deve estar acessível quando necessário, sendo aplicados mecanismos de recuperação de informação para casos de perda.

É vedada a transmissão de informações a terceiros, independentemente do meio, bem como reprodução, cópia, utilização ou exploração de informações de posse da Reptilândia sem autorização prévia da presidência e/ou vice-presidência, ou do Comitê de Segurança.

6.1.2. Procedimentos Relativos ao Tratamento das Informações e Recursos Tecnológicos

Todo e qualquer usuário terá acesso somente ao mínimo necessário para a realização de suas atividades, sendo baseado nas suas funções e na sensibilidade das informações.

Toda informação e qualquer informação deverá possuir cópias digitais armazenadas nos servidores principais e de backup, sendo realizado o backup ao início e final do dia.

Toda informação registrada em meio físico como, mas não exclusivamente, notas fiscais e recibos, deverão ser descartadas após um período de dois meses ou armazenadas de forma que as políticas de controle de acesso se façam presentes.

Toda e qualquer informação produzida, coletada e armazenada na Reptilândia deverá possuir ao menos uma cópia em servidores de backup desconectados da internet.

Ao desligamento de um colaborador, suas informações deverão ser anonimizadas após 30 dias do desligamento, incluindo em sistemas de backup.

Durante o desligamento do colaborador, o mesmo deverá retornar todo e qualquer dispositivo disponibilizado pela empresa e que está em sua posse. Esses dispositivos, após realizadas as devidas extrações de informação, deverão ser formatados antes que possam ser reutilizados por outros colaboradores.

6.2. Segurança quanto a Recursos Humanos

6.2.1. Normas Relativas à Segurança quanto a Recursos Humanos

Todo e qualquer membro colaborador da Reptilândia deverá participar dos treinamentos sobre Segurança da Informação fornecidos pela empresa.

Todo e qualquer membro da Reptilândia que possua acesso aos recursos tecnológicos e informações deverá ter apenas uma única identificação, salvo por exceções que forem documentadas e aprovadas pelo Comitê de Segurança.

Todo e qualquer membro colaborador da Reptilândia, no momento de contratação, deverá assinar a Declaração de Responsabilidade Sobre Informações e Recursos Tecnológicos.

Todo e qualquer membro colaborador da Reptilândia deverá ter acesso às possíveis sanções às quais estão sujeitos em caso de violação das políticas estabelecidas por este documento e pelos demais documentos contratuais aqui mencionados.

6.2.2. Procedimentos Relativos à Segurança quanto a Recursos Humanos

Treinamentos sobre Segurança de Informação deverão ser ministrados com uma recorrência semestral a todos os colaboradores da Reptilândia.

O fornecimento de identificações adicionais deverá passar pela avaliação do Comitê de Segurança e deverão ser documentados e armazenados, incluindo cópias para a presidência e para o colaborador que solicitou o acesso.

Cada colaborador terá um prazo de até 7 dias após a publicação deste documento para assinar a Declaração de Responsabilidade Sobre Informações e Recursos Tecnológicos, sob pena de desligamento.

Qualquer candidato à vaga, caso seja escolhido, deverá obrigatoriamente assinar a Declaração de Responsabilidade Sobre Informações e Recursos Tecnológicos antes de receber seus equipamentos e credenciais de acesso.

6.3. Segurança Lógica da Informação e dos Recursos Tecnológicos

6.3.1. Normas Relativas à Segurança Lógica da Informação e dos Recursos Tecnológicos

Todo e qualquer acesso aos serviços e dados deve ser protegido por senhas individuais e intransferíveis.

O compartilhamento de senhas é explicitamente proibido, estando sujeito a sanções que podem variar de acordo com o impacto causado pela ação.

As senhas deverão ser atualizadas periodicamente e deverão seguir o padrão estabelecido pela empresa para senhas fortes.

É dever de cada membro colaborador o armazenamento adequado e seguro de suas senhas.

Em caso de tentativas recorrentes e mal sucedidas de acesso ao sistema, o acesso deverá ser bloqueado imediatamente.

O colaborador jamais deverá deixar sua estação de trabalho desatendida e com a conta logada.

O acesso aos sistemas de informação deverá ocorrer somente através dos dispositivos oficiais da Reptilândia.

Ex-colaboradores deverão ter seus acessos ao sistema completamente bloqueados.

6.3.2. Procedimentos Relativos à Segurança Lógica da Informação e dos Recursos Tecnológicos

As senhas de acesso aos sistemas deverão ser atualizadas a cada, no máximo, 30 dias.

Serão consideradas senhas fortes aquelas que não são triviais ou previsíveis, com um tamanho mínimo de 8 caracteres e formadas a partir da combinação de letras maiúsculas, minúsculas, números e caracteres especiais.

As senhas deverão ser criptografadas e gravadas separadamente dos arquivos de dados, em ambiente de acesso restrito.

Após um máximo de três tentativas de acesso ao sistema sem sucesso, o acesso deverá ser bloqueado até que seja solicitado o desbloqueio pelo colaborador ao Comitê de Segurança.

Somente dispositivos oficiais da empresa serão liberados para o acesso à rede que realiza a transmissão de dados da empresa, ficando expressamente proibida o desbloqueio de dispositivos pessoais para tanto.

Após o desligamento do colaborador, todos os seus acessos devem ser bloqueados imediatamente e senhas alteradas pelo administrador do sistema.

6.3.3. Normas Relativas às Regras de Firewall

As regras de Firewall devem ser configuradas para permitir apenas o tráfego necessário para a operação da empresa.

As portas não utilizadas devem ser fechadas e os IPs devem ser filtrados para garantir que apenas dispositivos confiáveis tenham acesso à rede.

Além disso, pacotes devem ser inspecionados para evitar a entrada de malware ou outros tipos de tráfego malicioso.

6.3.4. Proteção contra Malware

Todos os sistemas devem ter software antivírus instalado e atualizado regularmente.

Medidas devem ser tomadas para proteger contra spyware e outras formas de malware, como implementação de filtros de conteúdo e a educação dos funcionários sobre práticas seguras de navegação na web.

6.4. Segurança Física da Informação e dos Recursos Tecnológicos

6.4.1. Normas Relativas à Segurança Física da Informação e dos Recursos Tecnológicos

Todos os equipamentos e dispositivos tecnológicos utilizados na Reptilândia devem ser armazenados em locais seguros, protegidos contra danos físicos, roubo ou acesso não autorizado.

Em caso de perda, furto ou falha técnica de todo e qualquer dispositivo da Reptilândia, estando incluídos aqueles fornecidos para cada colaborador (quando necessário) deverão ser reportadas imediatamente após o fato para o Comitê de Segurança.

As instalações que abrigam os servidores de rede e de backup devem ser protegidas por controles de acesso físico.

Todos os sistemas da empresa devem contar com dispositivos de energia reserva para casos de emergência.

Nenhum equipamento deverá ser retirado das instalações da Reptilândia sem aprovação explícita e documentada do Comitê de Segurança.

6.4.2. Procedimentos Relativos à Segurança Física da Informação e dos Recursos Tecnológicos

O acesso às áreas onde os equipamentos e dispositivos tecnológicos, especialmente de servidores de rede e armazenamento primário e secundário, deverá ser permitido somente a

usuários autorizados pelo Comitê de Segurança, mediante uso de cartão magnético e/ou biometria.

Situações de perda, furto ou falha técnica deverão ser reportadas ao Comitê de Segurança imediatamente após, salvo por situações extraordinárias, sob pena de aplicação de sanções.

Todos os dispositivos da empresa devem estar conectados a dispositivos de Nobreak com potencial suficiente para garantir a continuidade do funcionamento até que seja desligado de forma adequada e segura em caso de desligamento de rede elétrica.

A retirada de qualquer equipamento das premissas da Reptilândia deverá ser feita mediante solicitação e aprovação do Comitê de Segurança, com devida documentação e assinatura de termos de responsabilidade.

A integridade das câmeras de segurança e fechaduras das instalações deverá ser verificada regularmente, com recorrência semanal.

6.5. Uso dos Recursos Fornecidos pela Empresa

6.5.1. Normas Relativas ao Uso dos Recursos Fornecidos pela Empresa

Contas empresariais fornecidas pela Reptilândia deverão ser acessadas somente por dispositivos credenciados e fornecidos pela empresa e utilizadas somente em função dos objetivos estratégicos e profissionais da Reptilândia.

É vedada a utilização das contas empresariais em aplicativos de redes sociais e derivados, salvo para quando é necessário para a continuidade das atividades da empresa.

Todo e qualquer dispositivo fornecido pela empresa deve ser protegido com senha e criptografia, sendo fortemente recomendado que o armazenamento de informações sensíveis seja minimizado nesses dispositivos.

É proibido o uso dos recursos tecnológicos fornecidos pela Reptilândia para o download de arquivos da internet, especialmente de ambientes suspeitos ou que não possuam relação com o exercício das funções do colaborador e com os objetivos da empresa.

Em nenhuma circunstância será permitido o uso da rede e dos recursos tecnológicos para acesso a conteúdos nocivos como pornografia e plataformas de jogos.

6.5.2. Procedimentos Relativos ao Uso dos Recursos Fornecidos pela Empresa

Qualquer uso de contas empresariais para acesso a redes sociais, quando em função das atividades da empresa, deverá passar pela aprovação do Comitê de Segurança e ser devidamente documentado.

Todos os downloads realizados em dispositivos fornecidos pela empresa deverão ser verificados por um software de antivírus definido pela empresa antes de serem abertos ou executados.

Todos os dispositivos fornecidos pela empresa deverão, obrigatoriamente, bloquear o acesso a recursos, sites e aplicativos conhecidos por serem inseguros e/ou nocivos.

6.6. Acesso por Prestadores de Serviço

6.6.1. Normas Relativas ao Acesso por Prestadores de Serviço

O acesso de recursos tecnológicos e informações da Reptilândia por parte de prestadores de serviços deverá ser feito de forma temporária, com permissões limitadas.

Todo e qualquer prestador de serviço deverá assinar um Termo de Responsabilidade sobre Informações e Recursos Tecnológicos no momento de sua contratação antes que tenha acesso aos recursos disponibilizados pela empresa.

Os prestadores de serviço só poderão acessar os sistemas da Reptilândia por meio de dispositivos fornecidos ou aprovados pela empresa.

6.6.2. Procedimentos Relativos ao Acesso por Prestadores de Serviço

Prestadores de serviço que se recusarem a assinar o Termo de Responsabilidade sobre Informações e Recursos Tecnológicos terão sua contratação revogada.

A concessão de acesso temporário aos sistemas e informações deverá ser realizada pelo Comitê de Segurança, após aprovação da contratação e assinatura do Termo de Responsabilidade sobre Informações e Recursos Tecnológicos.

Todos os dispositivos utilizados pelos prestadores de serviços deverão ser recolhidos após o término das funções e, feita a extração de qualquer informação relevante, deverão ser formatados antes de serem utilizados novamente.

Todos os dispositivos utilizados pelos prestadores de serviço deverão ter acesso mínimo, somente ao absolutamente necessário para execução das atividades.

6.7. Normas de Aquisição, Manutenção e Descarte de Equipamentos e Sistemas

6.7.1. Normas Relativas à Aquisição, Manutenção e Descarte de Equipamentos e Sistemas

Os equipamentos devem ser regularmente inspecionados em busca de vulnerabilidades e falhas físicas ou de sistema.

As instalações de servidores de rede e armazenamento de dados devem ser adequadamente construídas conforme necessidades desses equipamentos, incluindo aspectos como refrigeração, fonte de energia reserva e sistema elétrico.

Os softwares utilizados nos equipamentos e sistemas da Reptilândia devem ser licenciados e atualizados regularmente.

O descarte de equipamentos e sistemas antigos deve ser feito de maneira segura e ambientalmente responsável.

6.7.2. Procedimentos Relativos à Aquisição, Manutenção e Descarte de Equipamentos e Sistemas

A inspeção dos equipamentos deverá ser realizada por uma equipa credenciada e aprovada pelo Comitê de Segurança, que será acompanhada por um dos membros.

O encontro de qualquer irregularidade deverá ser reportado ao Comitê de Segurança imediatamente após a descoberta, para que seja investigada e resolvida o mais brevemente possível.

Os softwares utilizados pela Reptilândia deverão passar por rotinas de atualização com periodicidade no máximo bimestral.

Aspectos relativos a ameaças de incêndio, rede elétrica e controle de temperatura deverão ser considerados na construção das instalações que comportam dispositivos sensíveis.

Todos os equipamentos que forem passíveis de descarte devem passar por rotinas de limpeza dos dados, removendo peças como HD e SSD antes do descarte. Essas peças deverão ser devidamente destruídas.

7. Sanções aplicáveis

O descumprimento de qualquer uma das diretrizes estabelecidas nesta Política de Segurança da Informação e em quaisquer outras que venham a complementar ou modificar oficialmente este documento, será considerado uma violação séria e poderá resultar em ações disciplinares. As sanções aplicáveis dependem da gravidade da violação e podem incluir, além de outras, as consequências a seguir:

1. **Treinamento adicional:** Toda e qualquer violação que não resulte imediatamente no desligamento do funcionário poderá incluir treinamentos adicionais sobre segurança como parte da sanção;
2. **Advertência formal:** Violações menores ou primeiras ofensas que possuem baixíssimo ou nenhum impacto comprovado poderão ser tratadas com a emissão de uma advertência formal;

3. **Suspensão temporária:** Para violações mais graves, a suspensão temporária do funcionário poderá ser imposta, com período a ser determinado de acordo com a natureza e gravidade da violação;
4. **Desligamento:** Em casos de violações graves ou recorrentes, a demissão pode ser uma ação disciplinar apropriada e poderá ocorrer sem aviso prévio;
5. **Ação Legal:** Ações que envolvam atividades ilegais, como roubo ou uso não autorizado de informações, que coloquem em risco a integridade do negócio, incluindo seus colaboradores e clientes, bem como sua imagem, estarão sujeitas a ações legais contra o perpetuador.

A decisão sobre as sanções a serem aplicadas serão tomadas com base na legislação vigente e dos procedimentos internos da Reptilândia. Todos os funcionários possuem o direito de apelar contra qualquer ação disciplinar tomada contra eles, sendo a decisão final crivo da alta administração após a investigação dos fatos e evidências.

8. Gerenciamento de Incidentes de Segurança

Em caso de incidente de segurança, o Comitê de Segurança deve ser notificado imediatamente. O incidente será investigado e medidas serão tomadas para mitigar o impacto.

Após a resolução do incidente, uma análise pós-incidente deve ser realizada para aprender com o evento e melhorar as práticas de segurança.

9. Vigência e Revisão da Política

Esta Política de Segurança da Informação entrará em vigência imediatamente após a sua publicação e disponibilização para todos os funcionários e membros da Reptilândia.

Esta Política de Segurança da Informação será revisada anualmente, ou conforme necessário, pelo Comitê de Segurança para garantir que continue relevante e eficaz no contexto da Reptilândia.

A sua atualização irá considerar quaisquer incidentes de segurança ocorridos, feedbacks dos funcionários, mudanças na legislação ou normas e novas ameaças ou vulnerabilidades identificadas.

Por fim, todas as alterações serão comunicadas a todos os funcionários e partes interessadas relevantes.

Comitê de Segurança - Reptilândia
Política revisada em 26 de maio de 2024