Política de Segurança

UXTECH

Histórico de Alterações

Descrição	Este documento resume a Política de Segurança da Informação	
Responsável		
Setor	Tecnologia da Informação	
Equipe	Segurança da Informação	
Data de Confecção	12/07/2023	
Versão	1.0.0	Versão revisada da Política de Segurança de 10/01/2021
Data Aprovação	14/07/2023	14/07/2023

Sumário

1. Introdução **3**
2. Objetivo **4**
3. Classificação e Tratamento da Informação **4**
3.2. Tratamento da Informação 4
3.3. Rotulagem e Marcação 4
3.4. Armazenamento de Informação 5
3.5. Transmissão de Informação 5
3.6. Descarte Seguro 5
3.7. Tratamento de Informação de Clientes 5
3.8. Compartilhamento Externo de Informação 5
4. Controle de Acesso **5**
4.1. Política de Senhas 5
4.3. Autenticação de Dois Fatores (2FA) 5
4.4. Contas de Usuário Inativas 6
4.5. Controle de Acesso Baseado em Funções (RBAC) 6
4.6. Monitoramento de Acesso 6
4.7. Gerenciamento de Chaves Criptográficas 6
4.8. Auditoria de Acesso 6
4.9. Política de Remoção de Acesso 6
4.10. Acesso a Terceiros 6
4.11. Controle de Acesso Físico 6
5. Diretrizes **7**
5.2. Download de Software 7
5.3. Hardware 7
5.4. Comunicação 7
6. Segurança Física **7**
6.1. Áreas Restritas 7
6.2. Instalações 7
6.3. Equipamentos 7
6.4. Áreas Restritas 8
6.5. Monitoramento de Ambientes 8
6.6. Procedimentos de Manutenção 8
6.7. Política de Acesso às Instalações 8
6.8. Segurança Física de Dispositivos Móveis 8
6.9. Backup e Armazenamento de Dados 8
6.10. Política de Limpeza e Descarte de Materiais 8
6.11. Conscientização sobre Segurança Física 8
6.12. Política da Mesa Limpa 9
7. Política de Retenção de Logs da UXTech **9**
7.1. Escopo 9
7.2. Classificação de Dados 9
7.3. Períodos de Retenção 9
7.4. Cumprimento Legal e Regulatório 9
7.5. Automatização e Gerenciamento 10

7.6. Acesso e Segurança 10
7.7. Monitoramento e Revisão 10
7.8. Descarte Seguro 10
7.9. Treinamento e Conscientização: 10
7.10. Responsabilidade 10
8. Plano de Recuperação de Desastres (PRD) 10
8.1. Avaliação de riscos e impactos 10
8.2. Equipe de resposta a desastres 11
8.3. Backup e armazenamento de dados 11
8.4. Redundância de sistemas e infraestrutura 11
8.5. Procedimentos de emergência 12
8.6. Testes regulares 12
8.7. Treinamento e conscientização 12
8.8. Atualização e revisão contínua 12
8.9. Comunicação com stakeholders 12
9. Plano de Continuidade Operacional (PCO) 12
9.2. Avaliação de riscos e impactos 12
9.3. Equipe de Continuidade Operacional 12
9.4. Backup e Recuperação de Dados 13
9.5. Redundância de sistemas e infraestrutura 13
9.6. Plano de Comunicação 13
9.7. Alternativas de trabalho remoto 13
9.8. Acordos de nível de serviço (SLAs) 14
9.9. Testes e Treinamento 14
9.10. Revisão e Atualização 14
10. Política de Descarte Seguro de Dados da UXTech 14
10.1. Escopo 14
10.2. Classificação de Dados 14
10.3. Procedimentos de Descarte Seguro 14
10.4. Responsabilidade 15
10.5. Conformidade Legal 15
10.6. Monitoramento e Auditoria 15
10.7. Treinamento e Conscientização 15
11. Avaliação e Revisão da Política de Segurança 15
12. Assinaturas 16

1. Introdução

A política de segurança da UX VISION TECH LTDA (abreviada para UXTech neste documento) tem como objetivo garantir a proteção dos ativos de informação, a integridade dos sistemas e a confidencialidade dos dados. Esta política se aplica a todos os funcionários, contratados, parceiros de negócios e usuários autorizados que têm acesso aos recursos da UXTech.

2. Objetivo

Esta política é baseada e tem como objetivo promover os três pilares fundamentais da segurança da informação: confidencialidade, integridade e disponibilidade.

2.1. **Confidencialidade**: restrição de acesso às informações apenas a indivíduos autorizados. As informações confidenciais devem ser mantidas em sigilo e protegidas contra divulgação não autorizada com implementação de medidas de controle de acesso, como autenticação e criptografia, ajudando a garantir que somente pessoas autorizadas possam acessar determinados dados sensíveis.

2.2. **Integridade**: proteção da precisão e da completude dos dados. Isso envolve garantir que as informações não sejam alteradas ou corrompidas de forma não autorizada ou acidental. A integridade dos dados é crucial para garantir a confiabilidade das informações e evitar manipulações que possam comprometer a tomada de decisões, a qualidade dos serviços ou a imagem da organização.

2.3. **Disponibilidade**: garantia de que as informações e os recursos estejam acessíveis quando necessários. Isso implica em manter sistemas, redes e serviços em funcionamento, evitando interrupções não planejadas ou indisponibilidades. A disponibilidade é alcançada por meio da implementação de redundância, backups, planos de recuperação de desastres e medidas de segurança física, além de estratégias para mitigar riscos de falhas técnicas ou ataques cibernéticos. Assegurar a disponibilidade dos dados é essencial para manter a produtividade, a continuidade dos negócios e a satisfação dos usuários e clientes.

3. Classificação e Tratamento da Informação

3.1. Classificação da Informação

Todos os dados e informações da UXTech devem ser classificados de acordo com seu valor e sensibilidade, como confidencial, restrito ou público. A classificação deve ser realizada de acordo com as diretrizes estabelecidas pelo departamento de segurança da informação.

3.2. Tratamento da Informação

A informação classificada como confidencial deve ser protegida de forma adequada, com acesso restrito apenas a pessoas autorizadas. Os dados restritos devem ser compartilhados apenas com pessoas que tenham necessidade de conhecê-los. A informação pública pode ser divulgada livremente.

3.3. Rotulagem e Marcação

Toda informação classificada deve ser rotulada e marcada de forma adequada, indicando sua classificação de segurança. Isso ajuda a garantir que os

funcionários e usuários da empresa identifiquem corretamente a sensibilidade da informação e tomem as medidas apropriadas para protegê-la.

3.4. Armazenamento de Informação

A informação deve ser armazenada em sistemas seguros, de acordo com sua classificação. Medidas de proteção, como criptografia, devem ser aplicadas em dados confidenciais e restritos, tanto em armazenamento físico quanto digital.

3.5. Transmissão de Informação

Ao transmitir informações confidenciais ou restritas, devem ser utilizados mecanismos seguros, como criptografia de dados e protocolos de segurança. É proibido o uso de canais não seguros, como redes públicas ou não autorizadas.

3.6. Descarte Seguro

A informação deve ser descartada de forma segura e adequada, garantindo que não possa ser recuperada por terceiros não autorizados. Isso inclui a destruição física de mídias e o uso de métodos seguros de eliminação de dados digitais.

3.7. Tratamento de Informação de Clientes

A informação de clientes, como dados pessoais e informações financeiras, deve ser protegida de acordo com leis de privacidade aplicáveis e regulamentações governamentais. É necessário obter consentimento explícito dos clientes para a coleta, armazenamento e processamento de suas informações.

3.8. Compartilhamento Externo de Informação

O compartilhamento de informações com terceiros externos à empresa deve ser realizado apenas mediante a assinatura de acordos de confidencialidade e a garantia de que medidas adequadas de segurança estejam em vigor para proteger a informação compartilhada.

4. Controle de Acesso

4.1. Política de Senhas

Os funcionários devem criar senhas fortes e únicas para acessar sistemas e aplicativos da UXTech. As senhas devem ser alteradas regularmente e não devem ser compartilhadas com terceiros.

4.2. Gerenciamento de Identidade e Acesso

O acesso a recursos da UXTech deve ser concedido com base no princípio do menor privilégio, ou seja, cada usuário deve ter apenas os privilégios necessários para realizar suas tarefas. O gerenciamento de identidade e acesso deve ser realizado de acordo com as melhores práticas de segurança.

4.3. Autenticação de Dois Fatores (2FA)

A UXTech deve implementar a autenticação de dois fatores sempre que possível, exigindo que os usuários forneçam uma segunda forma de

autenticação, além da senha, para acessar sistemas e aplicativos. Isso adiciona uma camada adicional de segurança para evitar acesso não autorizado.

4.4. Contas de Usuário Inativas

As contas de usuário inativas devem ser desativadas ou removidas do sistema regularmente. Isso evita que contas não utilizadas sejam comprometidas e usadas como ponto de entrada para ataques maliciosos.

4.5. Controle de Acesso Baseado em Funções (RBAC)

A UXTech deve adotar uma abordagem baseada em funções para conceder acesso aos recursos da UXTech. Os privilégios de acesso devem ser atribuídos com base nas responsabilidades e funções do usuário, garantindo que apenas as permissões necessárias sejam concedidas.

4.6. Monitoramento de Acesso

Deve ser implementado um sistema de monitoramento de acesso para registrar e analisar as atividades dos usuários nos sistemas da UXTech. Isso permite a detecção de comportamentos suspeitos e atividades maliciosas, facilitando uma resposta efetiva a incidentes de segurança.

4.7. Gerenciamento de Chaves Criptográficas

As chaves criptográficas usadas para proteger informações confidenciais devem ser gerenciadas de forma segura. Isso inclui a geração, distribuição, armazenamento e revogação adequados das chaves, garantindo a confidencialidade e a integridade dos dados criptografados.

4.8. Auditoria de Acesso

Deve ser realizada auditoria regular dos registros de acesso para garantir a conformidade com as políticas de segurança da UXTech. Isso inclui revisão e análise dos logs de acesso, identificação de atividades suspeitas e investigação de possíveis violações de segurança.

4.9. Política de Remoção de Acesso

Ao encerrar o emprego ou o relacionamento com a UXTech, o acesso dos funcionários, contratados e parceiros de negócios aos sistemas e recursos da UXTech deve ser prontamente revogado. Isso inclui desativação de contas, revogação de privilégios e retorno de dispositivos de acesso.

4.10. Acesso a Terceiros

O acesso concedido a terceiros, como fornecedores e parceiros, deve ser cuidadosamente gerenciado e limitado apenas ao necessário para a execução de suas atividades autorizadas. Deve haver um processo de avaliação e seleção criterioso para garantir que terceiros cumpram as medidas de segurança necessárias.

4.11. Controle de Acesso Físico

Além do controle de acesso digital, a UXTech deve implementar medidas de controle de acesso físico para restringir o acesso não autorizado às instalações e áreas sensíveis. Isso inclui o uso de crachás de identificação, sistemas de fechaduras e monitoramento por vídeo. Essas seções adicionais fornecem diretrizes mais detalhadas sobre o controle de acesso na UXTech, abordando aspectos como autenticação, monitoramento, gerenciamento de chaves e

acesso a terceiros. É importante adaptar essas diretrizes às necessidades e requisitos específicos da organização, em conformidade com as melhores práticas de segurança.

5. Diretrizes

5.1. Auditoria de Acesso

O uso da Internet por meio dos equipamentos e serviços fornecidos pela UX Tech deve ser restrito exclusivamente à execução de atividades relacionadas ao desempenho das tarefas laborais.

5.2. Download de Software

Os colaboradores não poderão em hipótese alguma utilizar os recursos do UX Tech para fazer o download ou distribuição de software ou dados não oficiais.

5.3. Hardware

É vedada a abertura de computadores para qualquer tipo de atividade pelos colaboradores;

5.4. Comunicação

Qualquer comunicação realizada durante o cumprimento da sua função laboral deve ser através de canal oficial ou ferramenta da empresa, com identificação corporativa criada pela administração nos padrões definidos pela UX Tech.

6. Segurança Física

Essas seções adicionais complementam a política de segurança física, fornecendo orientações sobre áreas restritas, monitoramento ambiental, procedimentos de manutenção, segurança física de dispositivos móveis e políticas de limpeza e descarte de materiais. Além disso, destaca-se a importância da conscientização e treinamento dos funcionários em relação à segurança física da UXTech.

6.1. Áreas Restritas

Certas áreas das instalações podem conter informações sensíveis ou equipamentos críticos. Essas áreas devem ser designadas como restritas e devem ser protegidas por mecanismos adicionais, como leitores de cartão de acesso, biometria ou escolta de segurança. As seções adicionais complementam a política de segurança física, fornecendo orientações sobre áreas restritas, monitoramento ambiental, procedimentos de manutenção, segurança física de dispositivos móveis e políticas de limpeza e descarte de materiais. Além disso, destaca-se a importância da conscientização e treinamento dos funcionários em relação à segurança física da UXTech.

6.2. Instalações

As instalações da UXTech devem ser protegidas adequadamente contra acesso não autorizado. Isso inclui o uso de sistemas de controle de acesso,

monitoramento por vídeo, proteção contra incêndios e outros mecanismos de segurança física.

6.3. Equipamentos

Os equipamentos da UXTech, incluindo computadores, servidores e dispositivos móveis, devem ser protegidos contra roubo, perda ou danos físicos. As medidas de segurança incluem o uso de trancas, alarmes e o registro adequado de ativos.

6.4. Áreas Restritas

Certas áreas das instalações podem conter informações sensíveis ou equipamentos críticos. Essas áreas devem ser designadas como restritas e devem ser protegidas por mecanismos adicionais, como leitores de cartão de acesso, biometria ou escolta de segurança.

6.5. Monitoramento de Ambientes

Deve ser implementado um sistema de monitoramento ambiental para detectar e responder a condições anormais, como temperatura, umidade ou presença de água. Isso ajuda a prevenir danos a equipamentos sensíveis e garante um ambiente adequado para o funcionamento dos sistemas.

6.6. Procedimentos de Manutenção

Procedimentos adequados de manutenção devem ser seguidos para garantir a segurança física dos equipamentos. Isso inclui verificações regulares, manutenção preventiva, substituição de componentes desgastados e descarte seguro de equipamentos obsoletos.

6.7. Política de Acesso às Instalações

Deve existir uma política clara de acesso às instalações da UXTech. O acesso deve ser restrito a pessoas autorizadas e registrado por meio de identificação adequada, como crachás de identificação. Visitantes devem ser acompanhados por um funcionário autorizado durante sua permanência nas instalações.

6.8. Segurança Física de Dispositivos Móveis

Dispositivos móveis utilizados pela UXTech, como laptops e smartphones, devem ser protegidos adequadamente contra roubo ou perda. Isso inclui a utilização de criptografia, senhas de acesso, rastreamento de localização e políticas de bloqueio remoto em caso de incidentes.

6.9. Backup e Armazenamento de Dados

Os dados críticos da empresa devem ser regularmente copiados e armazenados em locais seguros, fora das instalações principais. Isso garante a disponibilidade e recuperação de informações em caso de falhas ou desastres.

6.10. Política de Limpeza e Descarte de Materiais

A empresa deve estabelecer uma política de limpeza e descarte de materiais sensíveis, como documentos impressos e mídias de armazenamento. Esses materiais devem ser adequadamente destruídos antes do descarte, utilizando métodos seguros, como a trituração de papel ou a destruição física de mídias.

6.11. Conscientização sobre Segurança Física

Os funcionários devem receber treinamento e orientação sobre as medidas de segurança física, incluindo a importância de manter as áreas seguras, relatar incidentes de segurança e seguir os procedimentos estabelecidos para proteção dos equipamentos e das instalações.

6.12. Política da Mesa Limpa

Não manter itens expostos ou deixá-los visíveis na mesa de trabalho. Isso se aplica a objetos pessoais, documentos confidenciais ou sensíveis e qualquer informação que possa comprometer segurança ou privacidade. Mantenha seu computador bloqueado (faça logoff) durante as ausências, mesmo que muito pequenas. Ao utilizar recursos compartilhados, como salas de reuniões ou estações de teste, certifique-se de remover todas as informações, sessões ou credenciais utilizadas. Ao se ausentar de seu posto de trabalho, armazene de forma segura as informações impressas. Desligue as estações de trabalho ao final do expediente para reduzir vulnerabilidades a ataques e invasões, além de promover o uso sustentável de energia elétrica. O descarte de mídias deve ser realizado exclusivamente pela equipe de Infraestrutura, assegurando a destruição adequada conforme o tipo e propósito das mídias.

7. Política de Retenção de Logs da UXTech

A Política de Retenção de Logs da UXTech tem como objetivo definir diretrizes para a coleta, armazenamento e descarte adequado dos registros de atividades (logs) gerados em nossos sistemas, aplicativos e infraestrutura. Essa política visa garantir a segurança, conformidade legal e gerenciamento eficiente dos dados de log, além de facilitar a identificação de incidentes, análise de desempenho e detecção de ameaças.

7.1. Escopo

Esta política se aplica a todos os sistemas e dispositivos utilizados pela UXTech que geram e mantêm registros de atividades, incluindo, mas não se limitando, à logs de segurança, logs de aplicativos, logs de sistema, logs de autenticação e logs de firewall.

7.2. Classificação de Dados

Os logs gerados pela UXTech devem ser classificados em termos de sensibilidade e confidencialidade. A classificação de dados deve ser determinada de acordo com as políticas de classificação de dados da empresa.

7.3. Períodos de Retenção

A UXTech estabelece os seguintes períodos de retenção para cada tipo de log, considerando requisitos legais, regulatórios e de conformidade, bem como os objetivos de negócios da empresa:

Logs de Segurança: 12 meses/anos.

Logs de Aplicativos: 12 meses/anos.

Logs de Sistema: 12 meses/anos.

Logs de Autenticação: 12 meses/anos.

Logs de Firewall: 12 meses/anos.

7.4. Cumprimento Legal e Regulatório

A UXTech compromete-se a cumprir todas as leis e regulamentos aplicáveis à retenção de dados e logs, em todas as jurisdições em que a empresa opera. A política deve ser revisada periodicamente para garantir a conformidade com mudanças legais ou regulatórias.

7.5. Automatização e Gerenciamento

A empresa deve implementar soluções de gerenciamento de logs e arquivamento para automatizar o processo de coleta, retenção e descarte dos logs de acordo com os períodos definidos nesta política. A equipe de TI deve ser responsável por monitorar e garantir a integridade dos registros e a eficácia do sistema de retenção de logs.

7.6. Acesso e Segurança

O acesso aos logs retidos deve ser restrito apenas a funcionários autorizados que tenham necessidade legítima de acesso para fins de investigação, segurança ou conformidade. Medidas de segurança, como autenticação multifator e controle de acesso baseado em função, devem ser implementadas para proteger a confidencialidade e a integridade dos dados de log.

7.7. Monitoramento e Revisão

A Política de Retenção de Logs da UXTech deve ser periodicamente revisada para garantir que ela permaneça relevante e alinhada com os objetivos e requisitos da empresa. As revisões devem ser realizadas em intervalos regulares ou sempre que ocorrerem alterações significativas em nosso ambiente operacional ou requisitos regulatórios.

7.8. Descarte Seguro

Ao final do período de retenção especificado para cada tipo de log, os registros devem ser devidamente descartados de forma segura, garantindo que não haja risco de recuperação ou acesso não autorizado.

7.9. Treinamento e Conscientização:

A UXTech deverá fornecer treinamento adequado para os funcionários sobre a importância da política de retenção de logs, sua implementação e conformidade. A conscientização sobre a política deve ser promovida em toda a organização.

7.10. Responsabilidade

A responsabilidade pela implementação e cumprimento desta política deve ser atribuída ao departamento de TI e à equipe de segurança da informação da UXTech.

8. Plano de Recuperação de Desastres (PRD)

8.1. Avaliação de riscos e impactos

Identificação de ameaças e riscos específicos à empresa de desenvolvimento de software.

Análise do impacto potencial de cada cenário de desastre nas operações, sistemas, dados e reputação da empresa.

8.2. Equipe de resposta a desastres

No caso de necessidade de execução do plano de recuperação de desastres, são acionados os profissionais aqui listados.

8.2.1. Gerente de Resposta a Desastres

Lidera a equipe de resposta a desastres e coordena todas as atividades de recuperação.

Mantém comunicação constante com a alta administração e toma decisões críticas durante a emergência.

Supervisiona a implementação do Plano de Recuperação de Desastres e revisa as ações tomadas após o desastre.

8.2.2. Administrador de Sistemas

Responsável por garantir a disponibilidade e integridade dos sistemas de TI.

Faz backups e verifica a eficácia do armazenamento dos dados em locais seguros.

Trabalha na restauração de sistemas e aplicativos após o desastre.

8.2.3. Especialista em Segurança da Informação

Monitora a segurança dos sistemas e redes durante a emergência.

Ajuda a identificar e responder a quaisquer incidentes de segurança cibernética relacionados ao desastre.

Colabora com a equipe de TI para garantir a proteção dos dados e informações críticas.

Realização de treinamentos periódicos para manter a equipe preparada e atualizada.

8.2.4. Especialista em Infraestrutura

Garante a disponibilidade e funcionamento dos servidores, roteadores e outros componentes de infraestrutura.

Implementa medidas de redundância e falha para evitar a interrupção dos serviços críticos.

Trabalha na restauração da infraestrutura após o desastre.

8.3. Backup e armazenamento de dados

Backup regular para todos os dados críticos, incluindo códigos-fonte, documentação e informações do cliente.

Armazenamento dos backups em locais externos seguros, como nuvem ou data centers off-site.

8.4. Redundância de sistemas e infraestrutura

Configuração de sistemas redundantes para evitar pontos únicos de falha.

Distribuição de infraestrutura em locais geograficamente distintos para mitigar riscos regionais.

8.5. Procedimentos de emergência

Todos os serviços, servidores e dados são ativados através de um deploy do último backup disponível em outro servidor idêntico.

A normalização do servidor original é acompanhada pela equipe através de comunicação direta com os contatos disponíveis de cada aplicação/hospedagem utilizada.

8.6. Testes regulares

Realização de testes de simulação de desastres com regularidade para garantir a eficácia e atualidade do PRD.

Revisão das lições aprendidas em cada teste e atualização do plano conforme necessário.

8.7. Treinamento e conscientização

Treinamento contínuo para todos os funcionários sobre as medidas de segurança e o papel de cada um durante a recuperação a cada seis meses.

Promoção de uma cultura de conscientização sobre a importância do PRD em todos os níveis da empresa.

8.8. Atualização e revisão contínua

Revisão e atualização do PRD sempre que houver mudanças significativas nos sistemas, processos ou infraestrutura da empresa.

Acompanhamento das tendências e melhores práticas do setor para manter o PRD alinhado com as últimas ameaças.

8.9. Comunicação com stakeholders

Comunicação proativa e transparente para manter a confiança e a credibilidade da empresa.

9. Plano de Continuidade Operacional (PCO)

9.1. Identificação dos serviços e sistemas críticos

Servidores de hospedagem de aplicativos, banco de dados de produção, controle de versão (como Git), sistemas de suporte ao cliente, sistemas de monitoramento de produção.

9.2. Avaliação de riscos e impactos

Realizar análises regulares de risco para identificar novas ameaças e avaliar o impacto potencial de interrupções nos serviços.

9.3. Equipe de Continuidade Operacional

No caso de necessidade de execução do plano de continuidade operacional, são acionados os profissionais aqui listados.

9.3.1. Gerente de Resposta a Desastres

Lidera a equipe de resposta a desastres e coordena todas as atividades de recuperação.

Mantém comunicação constante com a alta administração e toma decisões críticas durante a emergência.

Supervisiona a implementação do Plano de Recuperação de Desastres e revisa as ações tomadas após o desastre.

9.3.2. Administrador de Sistemas

Responsável por garantir a disponibilidade e integridade dos sistemas de TI.

Faz backups e verifica a eficácia do armazenamento dos dados em locais seguros.

Trabalha na restauração de sistemas e aplicativos após o desastre.

9.3.3. Especialista em Segurança da Informação

Monitora a segurança dos sistemas e redes durante a emergência.

Ajuda a identificar e responder a quaisquer incidentes de segurança cibernética relacionados ao desastre.

Colabora com a equipe de TI para garantir a proteção dos dados e informações críticas.

Realização de treinamentos periódicos para manter a equipe preparada e atualizada.

9.3.4. Especialista em Infraestrutura

Garante a disponibilidade e funcionamento dos servidores, roteadores e outros componentes de infraestrutura.

Implementa medidas de redundância e falha para evitar a interrupção dos serviços críticos.

Trabalha na restauração da infraestrutura após o desastre.

9.4. Backup e Recuperação de Dados

Backup regular para todos os dados críticos, incluindo códigos-fonte, documentação e informações do cliente.

Armazenamento dos backups em locais externos seguros, como nuvem ou data centers off-site.

9.5. Redundância de sistemas e infraestrutura

Configuração de sistemas redundantes para evitar pontos únicos de falha.

Distribuição de infraestrutura em locais geograficamente distintos para mitigar riscos regionais.

9.6. Plano de Comunicação

Sistema de alertas e notificações internas por meio de aplicativos de mensagens, e-mail ou outras ferramentas de comunicação.

9.7. Alternativas de trabalho remoto

Fornecer acesso seguro aos sistemas e dados da empresa por meio de uma VPN (rede virtual privada) ou outras soluções de acesso remoto.

9.8. Acordos de nível de serviço (SLAs)

Em caso de interrupção de serviços, a equipe de suporte entrará em ação em até 1 hora e a recuperação completa será alcançada em até 4 horas.

9.9. Testes e Treinamento

Simulação com regularidade de um ataque cibernético com desligamento dos sistemas críticos para testar a eficácia do plano de resposta a incidentes.

9.10. Revisão e Atualização

Realizar uma revisão após cada teste de continuidade operacional para identificar e corrigir quaisquer deficiências no plano.

10. Política de Descarte Seguro de Dados da UXTech

A Política de Descarte Seguro de Dados da UXTech tem como objetivo estabelecer diretrizes para a eliminação adequada e segura de informações confidenciais, dados pessoais e registros sensíveis que não são mais necessários para as operações comerciais da empresa. Esta política visa garantir a proteção dos dados contra acesso não autorizado, minimizar o risco de violações de segurança e cumprir com as regulamentações aplicáveis.

10.1. Escopo

Esta política se aplica a todos os dados e registros armazenados em sistemas de informação, servidores, dispositivos móveis, documentos impressos, mídias removíveis e quaisquer outras formas de armazenamento utilizadas pela UXTech.

10.2. Classificação de Dados

Os dados a serem descartados deverão ser classificados de acordo com a política de classificação de dados da UXTech. Isso permitirá que os dados sejam tratados com base em sua sensibilidade e importância para a empresa.

10.3. Procedimentos de Descarte Seguro

A UXTech deve seguir os seguintes procedimentos para o descarte seguro de dados:

10.3.1. Métodos de Destruição

Os dados eletrônicos devem ser devidamente apagados ou destruídos por meio de métodos aprovados, como a sobrescrição de dados com padrões seguros ou o uso de ferramentas de destruição de dados.

10.3.2. Descarte de Mídia Física

Documentos impressos e outras mídias físicas devem ser descartados por meio de trituração ou incineração, garantindo que a recuperação dos dados seja impossível.

10.3.3. Desativação de Contas

As contas de usuários e acessos a sistemas devem ser desativadas imediatamente após a cessação do vínculo do usuário com a empresa ou quando não forem mais necessárias para suas funções.

10.3.4. Descarte de Hardware

Antes de descartar equipamentos de TI ou dispositivos contendo dados, a equipe de TI deve executar procedimentos para garantir a remoção completa e segura dos dados armazenados neles.

10.4. Responsabilidade

A equipe de TI e a equipe de segurança da informação devem ser responsáveis por garantir que todos os dados sejam descartados de acordo com os procedimentos estabelecidos nesta política. Eles devem ser responsáveis por supervisionar o processo de destruição e monitorar o cumprimento da política.

10.5. Conformidade Legal

A UXTech deve garantir o cumprimento das leis e regulamentos aplicáveis ao descarte de dados, incluindo, mas não se limitando a, leis de proteção de dados e regulamentos ambientais relacionados ao descarte de equipamentos eletrônicos.

10.6. Monitoramento e Auditoria

A conformidade com a Política de Descarte Seguro de Dados deve ser monitorada regularmente por meio de auditorias internas e externas, para garantir a eficácia e a aderência contínua aos procedimentos de descarte.

10.7. Treinamento e Conscientização

A UXTech deve fornecer treinamento adequado para todos os funcionários sobre a importância do descarte seguro de dados e os procedimentos a serem seguidos. A conscientização sobre a política será promovida em toda a organização.

11. Avaliação e Revisão da Política de Segurança

A política de segurança da UXTech deve ser avaliada e revisada periodicamente para garantir que esteja alinhada com as melhores práticas de segurança e com as necessidades em constante evolução da organização. As atualizações devem ser comunicadas a todos os funcionários e usuários relevantes. Esta política de segurança é um resumo geral das diretrizes e requisitos de segurança da UX Vision Tech. Os detalhes e requisitos adicionais podem ser encontrados em documentos e políticas relacionadas, da área de segurança da informação.

12. Assinaturas

As assinaturas colhidas abaixo representam a aprovação do documento bem como o cumprimento das medidas de segurança aqui descritas, visando a proteção dos ativos de informação e a mitigação de riscos para a empresa.

_____
Diretoria

_____
Segurança da Informação

Política da empresa aprovada em: / /