
 Cred Uai	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
		Versão: 1.1
	Classificação: Pública	Última revisão: 10/06/2024

Política de Segurança da Informação (PSI) CredUai

1. INTRODUÇÃO	02
1.1. Escopo:	03
2. COMITÊ DE SEGURANÇA DA INFORMAÇÃO	03
2.1 Composição	03
2.2 Atribuições	03
3. DIRETRIZES GERAIS	03
3.1 Confidencialidade	03
3.2 Integridade	04
3.3 Disponibilidade	04
3.4 Conformidade	05
4. Normas Táticas	05
4.1 Gestão de Acessos e Criação de contas de usuários	05
4.2 Configuração das Redes das agências da CredUai (DHCP)	05
4.3 Proteção de Dados	05
4.4 Gerenciamento de Incidentes	05
4.5. Responsabilidades	06
4.5.1 Comitê de Segurança da Informação - CSI	06
4.5.2 Gestão Executiva/Diretoria	06
4.5.3 Gerente de TI	06
4.5.4 Colaboradores	06
4.6 Treinamento e Conscientização	06
4.7. Monitoramento e Auditoria	07
4.8. Resposta a Incidentes	07
4.9. Penalidades	07
4.9.1. Descrição das Penalidades	07
4.9.2. Critérios para Aplicação	07
4.10. Conformidade Legal	07
4.11. Revisão e Atualização	08
5. Glossário	08
Apêndice	10

 Cred Uai	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Classificação: Pública	Versão: 1.1
		Última revisão: 10/06/2024


1. INTRODUÇÃO

A CredUai não é apenas um banco; é o lar de uma comunidade que valoriza a segurança, a união e o progresso. Juntos, avançamos seguros, com a certeza de que cada passo que damos é protegido pela mais alta dedicação à segurança da informação.

Nossa missão é proteger as informações da CredUai e de seus associados, assegurando a confidencialidade, integridade e disponibilidade dos dados, e garantindo a conformidade com as legislações e regulamentações aplicáveis. Promovemos uma cultura de segurança da informação que suporte nossos objetivos estratégicos e fortaleça nossos relacionamentos. Esta missão agrega valor ao banco ao minimizar riscos operacionais, evitar perdas financeiras e legais e fortalecer a confiança dos stakeholders.

Valorizamos a confidencialidade, garantindo que as informações sejam acessadas apenas por pessoas autorizadas; a integridade, assegurando que as informações estejam completas e precisas, protegidas contra modificações não autorizadas; e a disponibilidade, garantindo que as informações estejam disponíveis para uso quando necessário. Cumprimos todas as leis, regulamentos e normas aplicáveis, incluindo a Lei Geral de Proteção de Dados (LGPD), e demonstramos comprometimento ao alinhar as ações da alta gestão com os objetivos estratégicos da empresa, promovendo a segurança da informação. Também enfatizamos a importância da conscientização, promovendo a educação sobre a segurança da informação entre todos os colaboradores.

Esta política estabelece diretrizes aderentes ao comprometimento da alta gestão, alinhadas com os objetivos estratégicos da empresa para aplicar os princípios de proteção da informação aos seus clientes, parceiros, terceiros, profissionais ou qualquer pessoa ou empresa que mantenha um relacionamento com a CredUai. Além disso, a política tem como objetivo proteger os ativos de informação contra ameaças internas e externas de acessos não autorizados e promover a conscientização sobre a importância da segurança da informação entre todos os colaboradores. Essas ações trarão valor ao banco ao criar um ambiente mais seguro e confiável, essencial para a sustentabilidade e crescimento contínuo da CredUai.

 Cred Uai	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Classificação: Pública	Versão: 1.1
		Última revisão: 10/06/2024

1.1. Escopo

Esta política se aplica a todos os funcionários, prestadores de serviços, parceiros e terceirizados que tenham acesso às informações das cooperativas bancárias, incluindo sistemas, redes, dispositivos e quaisquer outros meios de armazenamento de dados.

2. COMITÊ DE SEGURANÇA DA INFORMAÇÃO

2.1 Composição

O Comitê de Segurança da Informação (CSI) será composto por representantes das áreas de Tecnologia da Informação, Auditoria Interna, Jurídico, Recursos Humanos e Operações.

2.2 Atribuições

- Definir e revisar periodicamente a Política de Segurança da Informação.
- Monitorar e avaliar a conformidade com a política.
- Analisar e responder a incidentes de segurança.
- Promover a conscientização e treinamento sobre segurança da informação.


3. DIRETRIZES GERAIS

3.1 Confidencialidade

Garantir que as informações sensíveis sejam acessadas apenas por pessoas autorizadas.

- **Controle de Acesso:** O acesso às informações deve ser restrito apenas aos indivíduos autorizados, com base nas suas funções e responsabilidades. Todos os acessos dos colaboradores devem ser identificáveis e únicos, garantindo assim a qualificação de cada um como responsável pelas atividades realizadas.
- **Classificação da Informação:** As informações devem ser classificadas de acordo com seu grau de sensibilidade e importância, e tratadas conforme as normas estabelecidas para cada categoria.

Documentos que forem relacionados aos clientes, bem como informações confidenciais, serão classificados como PRIVADOS, onde somente pessoal autorizado terá acesso e não deverá ser divulgado publicamente.

 Cred Uai	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Classificação: Pública	Versão: 1.1
		Última revisão: 10/06/2024

Documentos relacionados a informações críticas, estratégicas e financeiras, documentos de compliance e auditoria, planos de segurança da informação e recuperação de desastres, detalhes sobre novos produtos e serviços antes do lançamento, informações sobre a infraestrutura de T.I e segurança, serão classificados como RESTRITOS, onde somente executivos de alto nível e membros do conselho e funcionários de departamentos específicos e de auditoria.

Documentos de cunho informativo, bem como esta Política da Segurança da Informação, serão classificados como PÚBLICOS e todos terão acesso.

Independente da categoria de confidencialidade, todos os documentos e suas informações deverão ser utilizados apenas para fins profissionais e institucionais.

3.2 Integridade


Assegurar que as informações estejam completas, precisas e protegidas contra modificações não autorizadas.

- **Controle de Alterações:** Qualquer modificação nas informações deve ser registrada e auditável para garantir a rastreabilidade.
- **Proteção contra Malware:** Todos os sistemas e dispositivos devem estar protegidos contra vírus, malware e outras ameaças que possam comprometer a integridade das informações.

3.3 Disponibilidade

Garantir que as informações estejam disponíveis para uso quando necessário.

- **Plano de Continuidade de Negócios:** Deve ser mantido um plano de continuidade de negócios para garantir que as operações possam ser retomadas rapidamente em caso de interrupção.
- **Backup:** As informações críticas devem ser regularmente copiadas e armazenadas em locais seguros para garantir a recuperação em caso de perda de dados.

 Cred Uai	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Classificação: Pública	Versão: 1.1
		Última revisão: 10/06/2024

3.4 Conformidade

Cumprir todas as leis, regulamentos e normas aplicáveis relacionadas à segurança da informação e à Lei Geral de Proteção de Dados (LGPD).

4. Normas Táticas

4.1 Gestão de Acessos e Criação de contas de usuários

- Definir perfis de acesso com base nas necessidades de trabalho, garantindo que apenas pessoas autorizadas tenham acesso às informações conforme sua função.
- Revisar e atualizar regularmente os direitos de acesso dos usuários para assegurar que estão alinhados com as mudanças nas funções e responsabilidades.
- Implementar autenticação multifator para acesso a sistemas críticos, reforçando a proteção contra acessos não autorizados.

4.2 Configuração das Redes das agências da CredUai (DHCP)

Procedimento de endereçamento de IP


- Atribuir automaticamente IP aos clientes DHCP IPv4 de cada agência, respeitando os intervalos de IP especificados para cada área dentro de cada agência.

4.3 Proteção de Dados

- Criptografar dados sensíveis tanto em trânsito quanto em repouso para garantir a confidencialidade e integridade das informações.
- Realizar backups periódicos e armazená-los em locais seguros para assegurar a disponibilidade e recuperação dos dados em caso de incidentes.

4.4 Gerenciamento de Incidentes

- Estabelecer um plano de resposta a incidentes para assegurar uma resposta rápida e eficaz a qualquer ameaça à segurança da informação.
- Registrar e analisar todos os incidentes de segurança para identificar causas, impactos e medidas corretivas.

 Cred Uai	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Classificação: Pública	Versão: 1.1
		Última revisão: 10/06/2024

- Realizar exercícios periódicos de simulação de incidentes para testar e aprimorar a eficácia dos planos de resposta a incidentes.

4.5. Responsabilidades

4.5.1 Comitê de Segurança da Informação - CSI

- Definir e manter a Política de Segurança da Informação.
- Monitorar a conformidade e a eficácia das medidas de segurança.

4.5.2 Gestão Executiva/Diretoria:

- Responsável por aprovar e revisar a política de segurança da informação.
- Garantir recursos necessários para a implementação da política.
- Apoiar iniciativas de segurança da informação.

4.5.3 Gerente de TI:


- Responsável por implementar e manter os controles de segurança, bem como pela conformidade com esta política.
- Monitorar e responder a eventos de segurança.

4.5.4 Colaboradores:

- Todos os funcionários têm a responsabilidade de seguir as diretrizes desta política.
- Reportar quaisquer incidentes de segurança ao CSI.

4.6 Treinamento e Conscientização

- Todo colaborador deve receber a Cartilha de Boas Práticas de Acesso Seguro ao ingressar na CredUai.
- Todos os colaboradores devem receber treinamento regular sobre segurança da informação e boas práticas.
- Devem ser realizadas campanhas de conscientização para reforçar a importância da segurança da informação.

 Cred Uai	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Classificação: Pública	Versão: 1.1
		Última revisão: 10/06/2024

4.7. Monitoramento e Auditoria

- Devem ser realizadas auditorias periódicas para garantir a conformidade com esta política e identificar possíveis vulnerabilidades.
- Sistemas e atividades devem ser monitorados continuamente para detectar e responder a incidentes de segurança em tempo hábil.

4.8. Resposta a Incidentes

- **Plano de Resposta a Incidentes:** Deve ser estabelecido um plano de resposta a incidentes que define os procedimentos para identificação, contenção, erradicação e recuperação de incidentes de segurança.
- **Relato de Incidentes:** Todos os incidentes de segurança devem ser imediatamente relatados ao responsável designado para permitir uma resposta rápida e adequada.

4.9. Penalidades

4.9.1. Descrição das Penalidades


- Advertência verbal ou escrita.
- Suspensão temporária de atividades.
- Rescisão do contrato de trabalho.
- Ação judicial, se aplicável.

4.9.2. Critérios para Aplicação

- Gravidade da infração cometida.
- Reincidência da conduta.
- Impacto da infração na segurança da informação.

4.10. Conformidade Legal

A cooperativa deve assegurar que suas práticas de segurança da informação estejam em conformidade com as leis e regulamentações aplicáveis, como a Lei Geral de Proteção de Dados (LGPD).

 Cred Uai	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Classificação: Pública	Versão: 1.1
		Última revisão: 10/06/2024

4.11. Revisão e Atualização

Esta política deve ser revisada periodicamente e atualizada conforme necessário para refletir mudanças nas ameaças de segurança, requisitos legais e necessidades operacionais.

5. Glossário

AD: Active Directory.

AWS: Amazon Web Services.

Autenticação Multifator: Método de verificação de identidade que utiliza duas ou mais formas de autenticação.

Backup: Cópia de segurança de dados para recuperação em caso de perda ou corrupção.

CAU: Centro de Autorização de Usuário.

Confidencialidade: Propriedade de manter a informação acessível apenas a pessoas autorizadas.

CSI: Comitê de Segurança da Informação.

DHCP: Dynamic Host Configuration Protocol. (Protocolo de Configuração Dinâmica de Host).

Disponibilidade: Propriedade de assegurar que a informação esteja disponível quando necessário.


Filezilla: Softwares capazes de conectar máquinas e transferir arquivos usando o FTP.

FTP: File Transfer Protocol é um protocolo de rede para a transmissão de arquivos entre computadores.

IP: Internet Protocol. (Protocolo de Rede). O IP é a identificação individual de cada um dos dispositivos conectados à internet ou a redes privadas.

Integridade: Propriedade de assegurar que a informação não seja alterada de maneira não autorizada.

LGPD: Lei Geral de Proteção de Dados.

 Cred Uai	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Classificação: Pública	Versão: 1.1
		Última revisão: 10/06/2024

PSI: Política de Segurança da Informação.

TI: Tecnologia da Informação

HTTPS: (Hypertext Transfer Protocol Secure) - Protocolo de comunicação utilizado na internet para transferir dados de forma segura, protegendo a integridade e confidencialidade das informações transmitidas.

SSL: (Secure Sockets Layer) - Tecnologia de segurança que estabelece uma conexão criptografada entre um navegador web e um servidor, garantindo a segurança das informações transmitidas.


TLS: (Transport Layer Security) - Versão mais recente do SSL, utilizado para fornecer segurança na comunicação entre aplicativos em rede, como sites e servidores.

MITM: (Man-in-the-Middle) - Tipo de ataque cibernético em que um invasor intercepta e monitora a comunicação entre duas partes, muitas vezes sem o conhecimento das partes envolvidas.

AES: (Advanced Encryption Standard) - Algoritmo de criptografia amplamente utilizado para proteger dados sensíveis, oferecendo um alto nível de segurança e desempenho.

2FA: (Two-Factor Authentication) - Método de autenticação que requer duas formas diferentes de verificação de identidade antes de conceder acesso a uma conta ou sistema.

HSMs: (Hardware Security Modules) - Dispositivos de hardware dedicados que fornecem segurança adicional para chaves criptográficas e operações sensíveis de criptografia.

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
		Versão: 1.1
	Classificação: Interna	Última revisão: 10/06/2024

Apêndice

Procedimentos Operacionais

Criador destes procedimentos: Sr. Renato Araújo – Gerente Técnico

Revisor destes procedimentos: Sra. Fátima Silva – Coordenadora técnica


1. Procedimento para Gestão de Acessos e Criação de Contas de Usuário e Email

Para a criação de uma nova conta de usuário, é necessário que a demanda seja comunicada por meio do preenchimento do Cadastro de Acesso de Usuário (CAU), que está disponível na plataforma de gestão interna. O cadastro deve ser completo, contendo informações como nome, departamento, agência, cargo e o nível de acesso necessário para o novo funcionário. Após o preenchimento, o cadastro deve ser enviado eletronicamente ao gestor responsável, que deverá aprovar a solicitação, garantindo que os níveis de acesso estejam alinhados com as funções do funcionário.

Com a aprovação do gestor, a solicitação é encaminhada ao setor de Tecnologia da Informação (TI), que configura a conta no Active Directory (AD), definindo os perfis de acesso conforme as diretrizes corporativas e as necessidades do cargo. Em seguida, o TI gera credenciais temporárias de acesso e as envia de forma segura ao departamento de Recursos Humanos. O RH, por sua vez, entra em contato com o novo funcionário para informar sobre o e-mail corporativo e a senha temporária.

No primeiro acesso ao sistema, o usuário deve inserir seu e-mail corporativo e a senha temporária, sendo então solicitado a criar uma nova senha permanente e pessoal. É fundamental que a nova senha seja forte e única, e que não seja compartilhada ou anotada em locais inseguros. O usuário deve confirmar com o RH que conseguiu acessar o sistema e alterar a senha com sucesso. Se houver problemas, o suporte de TI está disponível para assistência imediata.

Além disso, se um funcionário recém-contratado precisar de permissões de acesso além das inicialmente definidas, o gestor deve formalizar essa necessidade no CAU, especificando o nível

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
		Versão: 1.1
	Classificação: Interna	Última revisão: 10/06/2024

de acesso adicional e justificando a necessidade em relação às responsabilidades do funcionário. O TI avalia a solicitação para garantir a conformidade com as políticas de segurança e, após aprovação, implementa as permissões adicionais, notificando o funcionário e o gestor sobre a atualização do perfil de acesso.

Esses procedimentos são cuidadosamente projetados para reforçar a segurança da informação e otimizar a integração de novos colaboradores, equipando cada funcionário com os recursos tecnológicos necessários e alinhados com as políticas de segurança e melhores práticas. Nosso compromisso é com uma transição segura e eficiente para todos os membros da equipe, promovendo um ambiente de trabalho produtivo e protegido desde o início.

2. Procedimento para Configuração das Redes das agências da CredUai (DHCP)

Procedimento de endereçamento de IP

Nas configurações de Rede e Internet, a máquina cliente é configurada para receber endereço de IP de forma automática (DHCP), respeitando os intervalos de IP especificados para cada área dentro de cada agência. Isso evita a sobreposição de endereços IP e garante que cada cliente DHCP receba um endereço IP único.

O endereçamento do cliente é feito de forma automática na rede, através de um servidor DHCP autorizado no Active Directory.

O servidor DHCP é configurado para reconhecer os intervalos de IP de cada área. Ele é capaz de atribuir automaticamente um endereço IP dentro do intervalo correto, com base na localização do cliente DHCP, conforme especificações abaixo.

Estrutura da Sede

Router: endereço IP: 192.168.0.1/29

Servidor DHCP (Service): endereço IP: 192.168.0.2/29

Servidor de arquivo (Service): endereço IP: 192.168.0.2/29

Servidor de e-mail (Service): endereço IP: 192.168.0.3/29

Servidor DNS (Service): endereço IP: 192.168.0.4/29


 Cred Uai	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
		Versão: 1.1
	Classificação: Interna	Última revisão: 10/06/2024

Tabela de endereçamento de IP da Filial-Sede:

Departamento	Rede	Primeiro IP	Último IP	Broadcast	Máscara	Prefixo
Dispositivos de rede (4)	192.168.0.0	192.168.0.1	192.168.0.6	192.168.0.7	255.255.255.248	/29
Gerência (4)	192.168.0.8	192.168.0.9	192.168.0.2	192.168.0.2	255.255.255.240	/28
Tesouraria (1)	192.168.0.2	192.168.0.2	192.168.0.3	192.168.0.3	255.255.255.248	/29
Atendimento (6)	192.168.0.3	192.168.0.3	192.168.0.6	192.168.0.6	255.255.255.224	/27
Clientes (?)	92.168.0.64	92.168.0.65	92.168.0.93	92.168.0.94	255.255.255.224	/27


Estrutura da Filial 1

Router: endereço IP: 192.168.1.1/29

Servidor DHCP (Service): endereço IP: 192.168.1.2/29

Tabela de endereçamento de IP da Filial-1:

Departamento	Rede	Primeiro IP	Último IP	Broadcast	Máscara	Prefixo
Dispositivos de rede (4)	192.168.1.0	192.168.1.1	192.168.1.6	192.168.1.7	255.255.255.248	/29
Gerência (4)	192.168.1.8	192.168.1.9	192.168.1.22	92.168.1.23	255.255.255.240	/28
Tesouraria (1)	92.168.1.24	92.168.1.25	92.168.1.30	92.168.1.31	255.255.255.248	/29

 Cred Uai	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO		PSI-001-2024
			Versão: 1.1
	Classificação: Interna		Última revisão: 10/06/2024

Atendimento (6)	92.168.1.32	92.168.1.33	92.168.1.62	92.168.1.63	255.255.255.224	/27
Clientes (?)	92.168.1.64	92.168.1.65	92.168.1.93	92.168.1.94	255.255.255.224	/27


Estrutura da Filial 2

Router: endereço IP: 192.168.2.1/29

Servidor DHCP (Service): endereço IP: 192.168.2.2/29

Tabela de endereçamento de IP da Filial-2:

Departamento	Rede	Primeiro IP	Último IP	Broadcast	Máscara	Prefixo
Dispositivos de rede (4)	192.168.2.0	192.168.2.1	192.168.2.6	192.168.2.7	255.255.255.248	/29
Gerência (4)	192.168.2.8	192.168.2.9	92.168.2.22	92.168.2.23	255.255.255.240	/28
Tesouraria (1)	92.168.3.24	92.168.2.25	92.168.2.30	92.168.2.31	255.255.255.248	/29
Atendimento (6)	92.168.4.32	92.168.2.33	92.168.2.62	92.168.2.63	255.255.255.224	/27
Clientes (?)	92.168.5.64	92.168.2.65	92.168.2.93	92.168.2.94	255.255.255.224	/27

 Cred Uai	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
		Versão: 1.1
	Classificação: Interna	Última revisão: 10/06/2024

Estrutura da Filial 3

Router: endereço IP: 192.168.3.1/29

Servidor DHCP (Service): endereço IP: 192.168.3.2/29

Tabela de endereçamento de IP da Filial-3:

Departamento	Rede	Primeiro IP	Último IP	Broadcast	Máscara	Prefixo
Dispositivos de rede (4)	192.168.3.0	192.168.3.1	192.168.3.6	192.168.3.7	255.255.255.248	/29
Gerência (4)	192.168.3.8	192.168.3.9	192.168.3.22	192.168.3.23	255.255.255.240	/28
Tesouraria (1)	192.168.3.24	192.168.3.25	192.168.3.30	192.168.3.31	255.255.255.248	/29
Atendimento (6)	192.168.3.32	192.168.3.33	192.168.3.62	192.168.3.63	255.255.255.224	/27
Clientes (?)	192.168.3.64	192.168.3.65	192.168.3.93	192.168.3.94	255.255.255.224	/27


Estrutura da Filial 4

Router: endereço IP: 192.168.4.1/29

Servidor DHCP (Service): endereço IP: 192.168.4.2/29

Tabela de endereçamento de IP da Filial-4:

Departamento	Rede	Primeiro IP	Último IP	Broadcast	Máscara	Prefixo
Dispositivos de rede (4)	192.168.4.0	192.168.4.1	192.168.4.6	192.168.4.7	255.255.255.248	/29
Gerência (4)	192.168.4.8	192.168.4.9	192.168.4.22	192.168.4.23	255.255.255.240	/28

 Cred Uai	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO				PSI-001-2024
					Versão: 1.1
	Classificação: Interna				Última revisão: 10/06/2024

Tesouraria (1)	92.168.4.24	92.168.4.25	92.168.4.30	92.168.4.31	255.255.255.248	/29
Atendimento (6)	92.168.4.32	92.168.4.33	92.168.4.62	92.168.4.63	255.255.255.224	/27
Clientes (?)	92.168.4.64	92.168.4.65	92.168.4.93	92.168.4.94	255.255.255.224	/27

Estrutura da Filial 5

Router: endereço IP: 192.168.4.1/29

Servidor DHCP (Service): endereço IP: 192.168.4.2/29


Tabela de endereçamento de IP da Filial-5:

Departamento	Rede	Primeiro IP	Último IP	Broadcast	Máscara	Prefixo
Dispositivos de rede (4)	192.168.5.0	192.168.5.1	192.168.5.6	192.168.5.7	255.255.255.248	/29
Gerência (4)	192.168.5.8	192.168.5.9	192.168.5.22	192.168.5.23	255.255.255.240	/28
Tesouraria (1)	192.168.5.24	192.168.5.25	192.168.5.30	192.168.5.31	255.255.255.248	/29
Atendimento (6)	192.168.5.32	192.168.5.33	192.168.5.62	192.168.5.63	255.255.255.224	/27
Clientes (?)	192.168.5.64	192.168.5.65	192.168.5.93	192.168.5.94	255.255.255.224	/27

3. Procedimento para Proteção de Dados

3.1.Procedimentos para criptografar dados em trânsito:


- **Utilizar protocolos seguros de comunicação:** Certifique-se de que todas as comunicações entre os clientes e os servidores da cooperativa bancária são protegidas por protocolos seguros, como HTTPS, SSL/TLS.

 Cred Uai	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
		Versão: 1.1
	Classificação: Interna	Última revisão: 10/06/2024

- **Implementar certificados SSL/TLS confiáveis:** Adquirir e configurar certificados SSL/TLS emitidos por autoridades certificadoras confiáveis para garantir a autenticidade dos servidores e proteger contra ataques MITM (Man-in-the-Middle).
- **Utilizar chaves de criptografia fortes:** Utilizar algoritmos de criptografia robustos, como AES (Advanced Encryption Standard), e chaves de criptografia longas o suficiente para resistir a ataques de força bruta.
- **Implementar autenticação de dois fatores:** Adicionar camadas de autenticação, como autenticação de dois fatores 2FA (Two-Factor Authentication), para garantir que apenas usuários autorizados tenham acesso aos sistemas e dados da cooperativa bancária.
- **Monitorar e registrar o tráfego de rede:** Utilizar ferramentas de monitoramento de rede para identificar e investigar quaisquer atividades suspeitas ou tentativas de acesso não autorizado aos dados em trânsito.

3.2. Procedimentos de criptografar dados em repouso:

- **Utilizar algoritmos de criptografia forte:** Criptografar todos os dados sensíveis armazenados em bancos de dados ou dispositivos de armazenamento usando algoritmos de criptografia forte, como AES (Advanced Encryption Standard) .
- **Gerenciar chaves de criptografia de forma segura:** Implementar práticas de gestão de chaves robustas, como o uso de HSMs (Hardware Security Modules), para proteger e gerenciar as chaves de criptografia usadas para criptografar e descriptografar os dados em repouso.
- **Aplicar controle de acesso rigoroso:** Além da criptografia, implementar políticas de controle de acesso para garantir que apenas usuários autorizados tenham permissão para acessar e manipular os dados sensíveis armazenados.
- **Realizar auditorias de segurança regulares:** Realizar auditorias de segurança periódicas para garantir a conformidade com os padrões de segurança e identificar possíveis vulnerabilidades nos sistemas de armazenamento de dados.
- **Fazer backup dos dados criptografados de forma segura:** Certificar-se de que os backups dos dados criptografados são realizados regularmente e armazenados de forma segura, de preferência em locais externos e protegidos por criptografia adicional.

 Cred Uai	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
		Versão: 1.1
	Classificação: Interna	Última revisão: 10/06/2024

3.3. Procedimento de Backup

Para garantir a segurança e a integridade dos dados críticos da empresa, implementamos um processo meticuloso de backup diário. Os dados são automaticamente protegidos através de um sistema de backup automatizado, que opera com confiabilidade e precisão. Utilizamos um servidor de arquivos FTP seguro para armazenar esses backups, e empregamos ferramentas como o Filezilla para a transferência segura dos dados, assegurando que a integridade dos mesmos seja mantida.

A consistência e a confiabilidade dos backups são verificadas regularmente por meio de scripts de checagem automatizados. Essa etapa é crucial para manter a integridade dos dados e para a pronta disponibilidade em caso de necessidade de restauração. Além disso, para uma proteção ainda mais robusta, armazenamos cópias de segurança em locais geograficamente dispersos, incluindo a infraestrutura de nuvem da Amazon Web Services (AWS). Essa estratégia de redundância é essencial para a recuperação de dados em caso de desastres naturais ou falhas sistêmicas.

Para completar nosso compromisso com a segurança dos dados, realizamos testes periódicos de restauração dos backups. Esses testes são fundamentais para confirmar a eficácia do nosso processo de backup e para garantir que, quando necessário, os dados estarão disponíveis e íntegros para uso. Através dessas medidas, reforçamos nosso objetivo de manter um ambiente de trabalho produtivo e seguro, onde a informação é tratada como um ativo valioso e protegido com o máximo rigor.

4. Procedimento de Gerenciamento e Resposta a Incidentes

Quando um incidente de segurança for identificado, ele deve ser imediatamente registrado no sistema de gerenciamento de incidentes. A comunicação imediata ao Comitê de Segurança da Informação (CSI) é essencial para iniciar a resposta. O incidente será contido e mitigado utilizando medidas apropriadas, como isolamento de sistemas afetados e aplicação de patches de segurança. A análise de causa raiz será conduzida para identificar as origens do incidente e aplicar medidas corretivas para evitar recorrências. Um relatório final será elaborado, documentando todas as ações tomadas e quaisquer atualizações necessárias nas políticas e procedimentos, garantindo que as lições aprendidas sejam incorporadas na gestão de segurança da informação.